РАСШИРЕНИЕ ПРОФИЛЯ ОПЕРАЦИОННОГО РИСКА В БАНКАХ ПРИ ВОЗРАСТАНИИ DDoS-УГРОЗ[1]

Ревенков П.В.[2], Бердюгин А.А.[3]

Актуальность тематики обусловлена отсутствием глубокой научно–практической проработки вопросов обеспечения кибербезопасности в условиях применения систем дистанционного банковского обслуживания (ДБО) и Интернета вещей. Операционный риск (ОР) является банковским риском, уровень которого может повышаться в связи с использованием ДБО кредитной организацией. Сюда же можно отнести правовой и стратегический риски, риск ликвидности и риск потери деловой репутации (репутационный риск). Согласно названию, в статье характеризуются проявления операционного риска в банках и факторы его реализации в организациях кредитно–финансовой сферы.

Приводится закон Роберта Меткалфа о ценности телекоммуникационной сети и по нему рассчитывается полезность Интернета вещей. Ботнеты обеспечивают распределённую платформу для многих видов незаконной деятельности, таких как запуск DDoS–атак на важные объекты, массовое распространение вредоносных программ, фишинг и кража конфиденциальных данных. В статье описываются возможности ботнетов для реализации DDoS–атак на кредитные организации.

Приведены подходы к обеспечению кибербезопасности в условиях Интернета вещей и систем ДБО. Делаются попытки представить киберпространство Интернета вещей с помощью математической теории графов. Определены основные направления регулирования операционного риска в условиях возрастания DDoS–угроз. Перечислены факторы, повышающие уровень воздействия кибератак. Анализируются способы защиты информации на устройствах Интернета вещей. Обращается внимание на роль регулирующих органов в области обеспечения кибербезопасности банков в условиях применения систем ДБО и развития Интернета вещей.

***Ключевые слова**: дистанционное банковское обслуживание, Интернет вещей, DDoS–атака, информационная безопасность, ботнет*

DOI: 10.21681/2311-3456-2017-3-16-23

Операционный риск в кредитных организациях

Особое внимание к операционному риску (ОР) в кредитно-финансовой сфере стало уделяться после выхода ряда рекомендаций Базельского комитета по банковскому надзору (БКБН). БКБН не устанавливает обязательных правил, но многие государства стараются следовать его рекомендациям при организации банковского регулирования и надзора.

В отношении ОР рекомендации по стандартам изложены БКБН в основном документе «Международная конвергенция измерения капитала и стандартов капитала: новые подходы» (известном как Базель II)[4]. В соответствии с положениями данного документа, регулирование ОР включает:

- поддержание собственного капитала для покрытия ОР;
- создание внутренних процедур для оценки и управления ОР, которые позволяли бы удерживать его на допустимом уровне;
- раскрытие информации по ОР.

БКБН рекомендует три группы подходов для расчёта величины ОР и, соответственно, определения капитала, необходимого для покрытия этого риска:

- подход на основе базового индикатора (Basic Indicator Approach, BIA);
- стандартизированный подход (The Standardized Approach, TSA);
- усовершенствованные (продвинутые) подходы (Advanced Measurement Approaches, AMA).

Регулятор в каждой стране самостоятельно принимает решение, какие подходы разрешается использовать работающим в стране банкам. Подходы различаются по:

1 Статья подготовлена по результатам исследований, выполненных за счёт бюджетных средств по государственному заданию Финуниверситета 2017 года.

2 Ревенков Павел Владимирович, доктор экономических наук, профессор кафедры «Информационная безопасность», Финансовый университет при Правительстве РФ, Москва, Российская Федерация. E-mail: pavel.revenkov@mail.ru

3 Бердюгин Александр Александрович, аспирант кафедры «Информационная безопасность», Финансовый университет при Правительстве РФ, Москва, Российская Федерация. E-mail: a40546b@gmail.com

4 На этом же документе, как отмечает БКБН, основывается и Базель III. Базель III вносит изменения по количеству и качеству капитала, а также ряд других изменений, которые, однако, не коснулись операционных рисков.

- сложности внедрения, расчётов и поддержания методологии и инфраструктуры расчётов в актуальном состоянии;
- чувствительности к профилю ОР банка;
- чувствительности к уровню контроля ОР банка;
- требованиям к банкам, применяющим тот или иной подход (квалификационным требованиям);
- ряду других параметров.

Размер операционного риска в общем случае рассчитывается по формуле

$$ОР = 0{,}15 \times \frac{\sum_{i=1}^{n} Д_i}{n} \quad (1)$$

где Д – доход за -й год для целей расчёта капитала на покрытие операционного риска и n – количество лет, предшествующих дате расчёта размера операционного риска (не должно превышать трёх лет).

Предложенные БКБН подходы образуют гибкую систему, построенную по принципу «от простого к сложному». Сложность расчётов и требования к уровню управления ОР банка возрастают от подхода на основе базового индикатора к продвинутым подходам. Такая система подходов позволяет банкам постепенно переходить от более простых методов к более сложным и чувствительным, по мере того, как улучшается их система управления рисками и растут ресурсы, которые банк может себе позволить вложить в разработку методов оценки операционных рисков. Предпосылки и стимулы для такого перехода заложены в коэффициентах формул расчёта в подходе на основе базового индикатора и стандартизированном подходе. Первый даёт самое высокое расчётное значение капитала под операционные риски, которое, как полагал БКБН, должно снижаться с переходом на стандартизированный подход, а использование усовершенствованных подходов, скорее всего, даст еще меньшую расчётную величину требований к капиталу.

В подходе на основе базового индикатора ОР рассчитывается на годовом интервале для всего банка в целом. Индикатором ОР является валовой доход (Gross Income) банка, который усредняется за три прошедших года. Умножив среднее значение на коэффициент альфа, получаем величину ОР. Коэффициент альфа в настоящее время установлен БКБН в размере 15%. Такой расчёт рекомендуется производить один раз в год.

Предлагая данный подход, БКБН ориентировался на то, что при его использовании суммарные операционные риски всех банков (банковского сектора) как с высоким, так и с низким уровнем контроля ОР, будут покрыты капиталом, причём с запасом. В целом, по банковскому сектору доля капитала под операционные риски при применении подхода на основе базового индикатора должна составлять 12%.

Банк России также уделяет особое внимание ОР. После выхода документа БКБН «Принципы надлежащего управления операционным риском»[5] (июнь 2011 г.) регулятор направил для использования в рамках анализа деятельности кредитных организаций неофициальный перевод данного документа (Письмо Банка России от 16.05.2012 № 69-Т)[6]. Затем вышло Указание Банка России от 25.06.2012 № 2840-У «О требованиях к управлению операционным риском небанковскими кредитными организациями, имеющими право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций» в котором определил, что ОР возникает в результате нарушения законодательства Российской Федерации (в том числе несоответствия внутренних документов организации), отказов и (или) нарушений в работе автоматизированных информационных систем и технических средств, ненадлежащего уровня квалификации сотрудников, а также воздействия иных факторов ОР.

Предмет анализа ОР заключается в понимании причин или факторов его возникновения, а также потенциальных последствий его реализации. Вообще, любой риск представляет собой комбинацию вероятности и последствий наступления неблагоприятных событий:

$$\text{Риск} = \text{Вероятность} \times \text{Последствия} \quad (2)$$

То есть риск – это вероятность. Значение вероятности неблагоприятного события позволяет определить вероятность благоприятного события по формуле:

$$P_+ = 1 - P_- \quad (3)$$

Обстоятельства, которые влияют на вероятность реализации риска, являются его факторами. Эти обстоятельства сами по себе могут и не стать причиной наступления события ОР, но способствуют его реализации или рассматриваются как его дополнительный фактор, увеличивая вероятность возникновения риска или усугубляя по-

5 Документ на английском языке (Basel Committee on Banking Supervision, «Principles for the Sound Management of Operational Risk», June 2011) доступен на web-сайте Банка международных расчётов www.bis.org.

6 Ранее Банк России выпустил письмо «О Методических рекомендациях по организации кредитными организациями внутренних процедур оценки достаточности капитала» (от 29.06.2011 № 96-Т).

следствия реализации ОР. Основными факторами реализации ОР являются:

- факторы бизнес-процессов – наличие несовершенных процессов (например, ручной обработки данных или слабо выстроенной системы обмена информацией и взаимодействия между подразделениями), которые могут привести к реализации ОР, например, к ошибке при обработке данных или к неправильным действиям со стороны одного подразделения по причине несвоевременного получения информации от другого подразделения;

- факторы действий персонала – данные обстоятельства определяются уровнем профессионализма сотрудников, их опытом, а также их намерениями. ОР, например, может реализоваться как из-за некомпетентности сотрудника, так и из-за осознанного злоупотребления своими должностными обязанностями;

- факторы IT-систем – в случае, если используемые технологии устарели и IT-системы работают нестабильно, это может стать причиной реализации ОР, связанной с простоем систем или некорректным отражением тех или иных операций;

- факторы внешних событий – те обстоятельства, на которые сам банк не имеет прямого влияния. В основном в данную категорию относятся чрезвычайные ситуации, в том числе природного и техногенного характера, а также риски противоправных действий третьих лиц по отношению к банку [7].

Боевой червь опаснее боевого слона

В связи с активным внедрением в финансовый бизнес информационных и телекоммуникационных технологий, распространением систем дистанционного банковского обслуживания (ДБО), факторы реализации ОР стали во многом зависеть от надёжности аппаратно-программных средств, используемых в организациях кредитно-финансовой сферы, способности систем безопасности противостоять компьютерным атакам, профессиональной подготовки сотрудников, в чьи функции входит обеспечение информационной безопасности.

В рамках данной статьи нас будут интересовать только те факторы реализации ОР, которые связаны с DDoS-атаками. Аббревиатура DDoS образована от английского словосочетания Distributed Denial of Service, что буквально переводится как «распределённая атака типа “отказ в обслуживании”». DDoS-атака представляет собой злоумышленную попытку вызвать сбой в работе сервера или сетевого ресурса, сделав его недоступным для пользователей. Как правило, это достигается путем прерывания или временного сбоя работы хоста, подключённого к сети Интернет. Для организации DDoS-атаки участвующие в ней компьютеры часто предварительно заражаются специальными программами-«червями».

В отличие от обычной атаки типа «отказ в обслуживании» (DoS-атака), где для переполнения пакетами целевого ресурса используется один компьютер и одно интернет-соединение, DDoS-атака осуществляется с использованием множества компьютеров и интернет-соединений, которые зачастую глобально распределены в рамках системы под названием «ботнет[7]». По результатам исследования «Информационная безопасность бизнеса», которое было проведено «Лабораторией Касперского» совместно с компанией B2B International в 2016 году, 7 из 10 российских организаций неоднократно подвергались этим атакам. То есть российские предприятия плохо понимают, как нужно защищаться от DDoS-атак.

DDoS-атаки вызывают временную остановку действия сайта и, как следствие, нарушение привычного функционирования организации. Подобные перерывы могут приводить к срыву важных операций, вызывать сбои в различных процессах и наносить урон репутации. Отметим, что существенный урон DDoS-атаки наносят системам дистанционного финансово-сервисного обслуживания, которые за последние 15 лет получили широкое распространение среди клиентов кредитных организаций.

Попробуем разобраться – почему DDoS-атаки становятся мощнее, а их последствия необходимо учитывать при построении системы управления ОР в кредитных организациях. Вспомним несколько, получивших известность, законов в области применения информационных технологий.

Закон Гордона Мура[8]: «Вычислительная мощь микропроцессоров и плотность микросхем удваивается примерно каждые 18 месяцев при неизменной цене». Что говорит о темпах прогресса.

---

7 Ботнет (англ. botnet произошло от слов robot и network) – компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей ботмастеру выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

8 Данный закон оставался верным последние 40 лет и, вероятно, останется неизменным еще, по меньшей мере, в течение 15 лет [2].

Таблица 1.
Ценность сети

n	1	2	3	4	5
$Ц_n = (n-1)\cdot c$	0	1c	2c	3c	4c
$P_n = n(n-1)\cdot c$	0	2c	6c	12c	20c

Таблица 2.
Ценность Интернета вещей с 2012 по 2020 годы (условных единиц)

Год	2012	2013	2014	2015	2016	2017	2018	2019	2020
$n \cdot 10^9$	8,7	11,2	14,4	18,2	22,9	28,4	34,8	42,1	50,1
P_n	$8{,}7^2/2 \approx 37{,}8$	$11{,}2^2/2 \approx 62{,}7$	$14{,}4^2/2 \approx 103{,}7$	$18{,}2^2/2 \approx 165{,}6$	$22{,}9^2/2 \approx 262{,}2$	$28{,}4^2/2 \approx 403{,}3$	$34{,}8^2/2 \approx 605{,}5$	$42{,}1^2/2 \approx 886{,}2$	$50{,}1^2/2 \approx 1255{,}0$

Роберт Меткалф углубился в исследования и пришел к выводу, что полезность системы (ценность $Ц_n$ сети) растёт пропорционально квадрату числа компонентов n^2. При этом

$$Ц_n = (n-1)\cdot c \quad (4)$$

где $c = const$ – оценка возможности вести переговоры с одним абонентом.

Общая ценность сети P_n, состоящей из n узлов для всех её абонентов может быть вычислена по формуле

$$P_n = n(n-1)\cdot c \quad (5)$$

Как видим, ценность сети тем выше, чем выше число её компонентов n. Другими словами, сети способны генерировать новую ценность [2].

Возьмём упрощённую формулировку закона $P_n = n^2/2$, чтобы определить темпы роста ценности Интернета вещей9 с 2012 по 2020 годы10 в условных единицах.

Таким образом, за девять лет количество устройств увеличится в $50{,}1/8{,}7 \approx 5{,}8$ раз, при этом ценность Интернета вещей возрастёт в $1255{,}0/37{,}8 \approx 33{,}2$ раза и более половины всех новых бизнес-процессов и систем будут включать в себя IoT-элементы. Далее в квадратичной зависимости (ведь $\sqrt{33{,}2} \approx 5{,}76$ и $5{,}76^2 \approx 33{,}2$).

Закон распространяется и на ботнеты. Надо отметить, что чем больше устройств входит в состав ботнета, тем больший урон он может нанести (и как следствие, большую стоимость он имеет у хакеров).

В состав ботнета попадают заражённые вредоносным программным обеспечением компьютеры. Учитывая, что «умные кофеварки» или «умные холодильники» являются по своей сути компьютерами – они также могут входить в состав ботнета для организации DDoS-атак, технически напоминающих видеоигру Space Invaders. Поэтому развитие Интернета вещей может приводить не только к улучшению качества жизни людей, но и возрастанию угроз.

Возможности Интернета вещей позволят злоумышленникам удалённо управлять городским транспортом, персональными медицинскими системами или «внести разнообразие» в меню киберповара. Вспомним атаку на Иран в 2010 году, которая остановила обогащение урана и отбросила национальную ядерную программу Ирана на два года назад. Вирус Stuxnet, запущенный на smart-устройствах ядерного комплекса был использован для дистанционной агрессии одного государства против другого. Единственный способ защитить все устройства, объединённые интернет-сетью, – это надёжная защита единого центра управления Интернетом вещей еще на этапе разработки протоколов и устройств.

Мы можем представить всё киберпространство Интернета вещей, как совокупность множеств и взаимодействий его основных участников Поль-

9 Совокупность устройств, взаимодействующих посредством сети Интернет называется Интернетом вещей. Интернет вещей (англ. Internet of Things, IoT) представляет собой сетевую взаимосвязь физических объектов («вещей»), организация которой способна перестроить экономические и общественные процессы, увеличить повсеместное распространение Интернета и улучшить качество нашей жизни посредством уменьшения участия человека в определённых действиях и операциях.

10 Рассчитано и составлено авторами по данным сайта statista.com, статья «Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020» (дата обращения: 27.01.2017).

зователь (P), Сервер (S), Техника (T). По существу, мы имеем

$$P = \{p_1, p_2, \ldots, p_L\} \quad (6)$$

$$S = \{s_1, s_2, \ldots, s_M\} \quad (7)$$

$$T = \{t_1, t_2, \ldots, t_N\} \quad (8)$$

Где $M<<L<<N$, поскольку серверов гораздо меньше, чем пользователей и людей гораздо меньше, чем устройств в развивающемся мире Интернета вещей.

Решение проблем безопасности и конфиденциальности направлено на обеспечение безопасности вершин следующих графов:

$G_p = \{P, E_p\}$, где $E_p = \{(p_i, p_j)\}$, причём $i, j = 1, 2, \ldots, L$ (9)

$G_S = \{S, E_S\}$, где $E_S = \{(s_i, s_j)\}$, причём $i, j = 1, 2, \ldots, M$ (10)

Граф Техника («Вещи») можно опустить, поскольку ботмастеру целесообразно атаковать сервер целиком (это подтверждает анализ Spamhaus о том, что за 2016 год было выявлено более семи тысяч управляющих серверов, операторы которых использовали свои ботнеты для банковских махинаций, кражи учётных данных и DDoS-атак):

$G_S = \{T, E_T\}$, где $E_T = \{(t_i, t_j)\}$, причём $i, j = 1, 2, \ldots, N$ (11)

Смешанные графы, выражающие отношения Человек-Сервер и Человек-Техника, представлены ниже:

$G_{PS} = \{P, S, E_{PS}\}$, где $E_{PS} = \{(p_i, s_j)\}$, причём $i = 1, 2, \ldots, L; j = 1, 2, \ldots, M$ (12)

$G_{PT} = \{P, T, E_{PT}\}$, где $E_{PT} = \{(s_i, s_j)\}$, причём $i = 1, 2, \ldots, L; j = 1, 2, \ldots, N$ (13)

$G_{ST} = \{S, T, E_{ST}\}$, где $E_{ST} = \{(t_i, t_j)\}$, причём $i = 1, 2, \ldots, M; j = 1, 2, \ldots, N$ (14)

С ростом количества взаимосвязанных устройств, графы G_{PT} и G_{ST} приобретают особое значение. Внимание специалистов по информационной безопасности в ближайшем будущем будет сосредоточено на защите вершин именно этих графов [1].

По результатам анализа основных киберугроз, с которыми столкнулся мир в 2016 г, проведённого специалистами «Лаборатории Касперского», появились огромные ботнеты из устройств, подключённых к Интернету вещей, атаки на клиентские счета в банках сменились атаками на сами финансовые учреждения, участились атаки на критически важные системы [9].

Самый известный случай использования Интернета вещей в преступных целях в России – это двухдневная хакерская атака в ноябре 2016 г. на сайты восьми крупнейших банков и Банка России. Целью атак было нарушение работы сервисов. В атаке были задействованы преимущественно интернет-видеокамеры и роутеры. На очереди бытовая техника.

Кибербезопасность в условиях развития Интернета вещей

Кибербезопасность является составной частью безопасности национальной любого государства. Она оказывает постоянное влияние на состояние и защищённость национальных интересов страны. Это положение находит подтверждение в Доктрине информационной безопасности Российской Федерации, которая развивает Концепцию национальной безопасности страны применительно к информационной сфере.

Финансовым организациям понадобятся серьёзные технологии защиты от хакерских атак и непосредственного физического взлома приспособлений. Проблема усугубляется тем, что большинство smart-устройств создаются с применением простейших операционных систем и процессоров, которые не поддерживают сложные средства защиты, что немаловажно в том случае, когда IoT-решения направлены на снижение затрат потребителей. Именно поэтому специально для «вещей» создана принципиально новая операционная система с говорящим названием – KasperskyOS. Система выстроена на основе принципа Default Deny, исключающего совершение программными компонентами каких-либо несанкционированных действий[11].

Стоит признать, что киберпреступники всегда на шаг впереди, они нападают внезапно и могут использовать нешаблонные способы атак. В связи с этим производители средств защиты вынуждены постоянно обороняться, т.е. искать защиту в условиях жёсткого лимита времени, поскольку самый большой вред исходит именно от атак «нулевого дня» (когда «противоядие» ещё не найдено). В некоторых случаях защищаться приходится от того, о чём есть крайне поверхностное понимание: отсутствуют данные о количестве подобных атак, которые уже направлялись на банки, каким способом непосредственно производилось заражение программного обеспечения, как действовали злоумышленники в определённых ситуациях и т.п.

11 Операционка KasperskyOS начала экспансию на мировой рынок. URL: http://tadviser.ru/a/258426 (дата обращения 27.02.2017).

Таблица 3.
Основные направления регулирования ОР в кредитно-финансовой сфере в условиях возрастания DDoS-угроз. Составлено авторами

Направления регулирования	Что надо сделать РЕГУЛЯТОРУ	Что должны сделать БАНКИ
Установление требований для создания достаточных резервов под ОР	Разработать нормативные документы, содержащие требования для создания резервов под ОР	В соответствии с рекомендациями регулятора создать необходимые резервы под ОР
Совершенствование методов дистанционного и контактного надзора за ОР в банках	Разработать и внедрить методы дистанционного и контактного надзора для проверки качества управления ОР в банках (включая методики проверки инспекционными подразделениями вопроса качества управления ОР)	Выполнить рекомендации регулятора по созданию системы управления ОР и быть готовыми пройти проверку инспекционных подразделений регулятора без серьёзных замечаний
Повышение уровня обеспечения ИБ до приемлемого (включая своевременное выявление угроз ИБ и оперативное информирование регулятора)	Разработать и внедрить нормативные документы по обеспечению приемлемого уровня ИБ в банках (включая разработку схемы оперативного информирование регулятора об инцидентах ИБ и компьютеных атаках на информационные ресурсы банков)	Выполнить рекомендации регулятора по обеспечению приемлемого уровня ИБ (включая внедрения схемы реагирования на инциденты ИБ и компьютерные атаки на информационные ресурсы банка
Повышение качества подготовки персонала, в чьи функции входит управление ОР	Разработать стандарты (или другие нормативные документы, содержащие аналогичные рекомендации) в соответствии с которыми в банках должны быть специалисты в области управления ОР	Принять на работу или подготовить собственных специалистов в области управления ОР в соответствии с рекомендациями регулятора

При отсутствии взаимодействия противостояние осуществляется практически вслепую. Это всё равно, что вести войну, не имея сведений о численности и дислокации врага, используемом им вооружении и источниках подкреплений.

Кибербезопасность в кредитных организациях должна базироваться на готовности подразделений безопасности противостоять новым кибератакам, понимании всего спектра угроз для организации в целом и распределении приоритетов между активами организации и их защитой[12].

К факторам, повышающим уровень воздействия кибератак, можно отнести:

- отсутствие отлаженного правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области кибербезопасности (в том числе в условиях применения smart-технологий);

- высокая латентность (от лат. latentis – скрытый, невидимый) киберпреступлений и недостаточное осознание органами государственной власти на федеральном и особенно региональном уровнях, возможных политических, экономических, моральных и юридических последствий компьютерных преступлений [3];

- амбициозный прагматический характер противоправных действий в киберпространстве (достижения глобального экономического превосходства в течение одного поколения страны);

- высокий уровень технологичности и результативности компьютерных атак в плане проникновения с целью сбора информации (кибератаки мало касаются технологий прошлого века, как-то: атаки хакеров-одиночек или подмена контента) [4];

- несовершенство системы единого учёта правонарушений, совершаемых с использованием средств информатизации;

- слабая координация действий правоохранительных органов, суда и прокуратуры в борьбе с киберпреступлениями, недостаточная подготовка их кадрового состава к эффективному предупреждению, выявлению и расследованию таких действий;

- существенное отставание отечественной индустрии средств и технологий информатизации и кибербезопасности от мирового уровня;

- ограниченные возможности бюджетного финансирования научно-исследовательских и опытно-конструкторских работ по созданию правовой, организационной и технической баз кибербезопасности.

Учитывая, что кредитно-финансовая сфера становится одной из самых привлекательных зон интересов киберпреступников (о чём свидетельствует значительный рост числа киберпреступлений и целевых атак на банки), а также оптимизацию финансовых решений в условиях Интернета вещей,

12 Результаты мониторинга кибербезопасности кредитной организации рекомендовано оценивать не реже, чем раз в квартал. Причина такого решения – увеличение числа кибератак на системы финансовых организаций и рост финансовых потерь клиентов из-за хакерских программ (Письмо Банка России от 24.03.2014 № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»).

необходимо оперативно принять меры к обеспечению повышенного уровня кибербезопасности (особое внимание должно быть обращено на ДБО) [5]. Ведь мир, где всё соединено со всем и буквально всё может взаимодействовать и участвовать в торговле предоставляет огромные возможности не только для банков, но и для киберпреступников.

Описанные направления, по мнению авторов, представляют далеко не полный перечень мероприятий, которые необходимо выполнить в рамках обеспечения кибербезопасности в условиях применения Интернета вещей. Ведь в реальной практике каждое направление будет содержать гораздо больше задач, направленных на достижение цели. В перспективе нужно стремиться создать не только систему надзора в виртуальном пространстве, но и поднять культуру поведения в нём всех участников информационного обмена.

Выводы:

- учитывая, что ОР становится одним из самых значимых рисков в банковской деятельности по причине высокой зависимости непрерывности бизнеса от надёжности и защищённости используемых ИКТ в банках, необходимо принять меры по совершенстованию подходов к управлению ОР по причине возрастания DDoS-угроз. Очевидно, что структуру управления ОР необходимо строить на основании рекомендаций регулятора, а также с учётом потребностей и масштабов бизнеса и приоритетных процессов, обеспечивая эффективное распределение зон ответственности за управление теми или иными составляющими ОР;

- необходимо в ближайшее время разработать требования для банков по повышению уровня обеспечения ИБ до приемлемого. Одновременно разработать требования по резервированию ОР, тем самым поставив в прямую зависимость объёмы резервов под ОР от качества обеспечения ИБ (включая оценку качества подготовки персонала подразделений по управлению ОР и обеспечения ИБ);

- взаимодействие между разработчиками IoT-технологий и банками возможно лишь при условии обеспечения приемлемого уровня обеспечения ИБ. В противном случае IoT-устройства могут использоваться злоумышленниками в мошеннических целях (например, для организации DDoS-атак с последующим требованием выкупа от организаций и физических лиц);

- будущее в условиях Интернета вещей должно быть обязательно осознано и исследовано с разных точек зрения: социальной, психологической, политологической, военной и экономической. Множество нестандартных (а зачастую конфликтных) ситуаций в мире, подключённом к единой Интернет-системе, основанном на принципах сотрудничества и существующем за счет возобновляемых источников энергии, требует повышенного внимания. Регулирующим органам необходимо заранее учитывать темпы равития IoT-технологий и корректировать нормативные документы для снижения сопутствующих рисков;

- регулирующие органы должны создать работоспособную систему обеспечения кибербезопасности в кредитно-финансовой сфере, в том числе специальные надзорные подразделения. Продолжением политики регулятора в этой области должны быть рекомендации для организаций кредитно-финансовой сферы, выполнение которых позволит минимизировать возможные последствия кибератак;

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

***Рецензент**: Алексей Сергеевич Марков, доктор технических наук, профессор кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, старший научный сотрудник. E-mail: a.markov@npo-echelon.ru*

Литература:

1. Adel S. Elmaghraby, Michael M. Losavio. Cyber security challenges in Smart Cities: Safety, security and privacy // Journal of Advanced Research. July 2014. Volume 5, Issue 4. Pages 491-497.
2. Информационные системы и технологии в экономике и управлении: учебник / под ред. проф. В.В. Трофимова. 2-е изд., перераб. и доп. М.: Высшее образование, 2007. 480 с.
3. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: «Onebook.ru», 2012. 420 с.: ил.
4. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства // Вопросы кибербезопасности. 2016. №1(14). С. 68-74.
5. Международное и зарубежное финансовое регулирование: институты, сделки, инфраструктура: монография / под ред. А.В. Шамраева : в 2 ч. – Часть вторая. М.: КНОРУС: ЦИПСиР, 2014. 640 с.

6. Рогозин Д.О., Шеремет И.А., Гарбук С.В., Губинский А.М. Высокие технологии в США: опыт министерства обороны и других ведомств. М.: Изд-во МГУ, 2013. 384 с.
7. Ревенков П.В. Управление рисками в условиях электронного банкинга: Монография. М.: Издательский дом «Экономическая газета», 2011. 168 с.
8. Ревенков П.В., Бердюгин А.А. Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. № 11 (344). С. 158-169.
9. Киберпреступность становится организованнее и сложнее // Банковские технологии. 2016. № 11/12. С. 76-79.
10. Кинг Бретт. Банк 3.0. Почему сегодня банк – это не то, куда вы ходите, а то, что вы делаете. – М.: ЗАО «Олимп – Бизнес», 2014. 520 с.
11. Лямин Л.В. Применение технологий электронного банкинга: риск-ориентированный подход. М.: КНОРУС: ЦИПСиР, 2011. 336 с.
12. Интернет-технологии в банковском бизнесе: перспективы и риски: учебно-практическое пособие / Ю.Н. Юденков, Н.А. Тысячникова, И.В. Сандалов, С.Л. Ермаков. – 2-е изд., стер. – М.: КНОРУС, 2014. 318 с.

EXPANSION OF THE OPERATIONAL RISK PROFILE IN BANKS UNDER INCREASE OF DDoS-THREATS

P. Revenkov[13], A. Berdyugin[14]

The need in this research arises since cybersecurity has not been elaborated and studied scientifically and practically, considering the Internet of Things and remote banking service (RBS). Operational risk (OR) is a banking risk, the level of that may increase in connection with using RBS by the credit institution. Its also includes legal and strategic risks, liquidity risk and risk of business reputation loss (reputation risk). As the title implies the article is characterizes displays of operational risk in banks and factors of its implementation in organizations of credit and financial sector.

Robert Metcalfe›s law is given about the value of a telecommunications network and it is calculated the usefulness of the Internet of Things. Botnets provides distributed platform for many kinds of illegal activities, such as launching DDoS–attacks on important targets, the mass distribution of malware, phishing and identity theft. This article describes the botnets capabilities for implementation of DDoS–attacks on credit institutions.

Approaches are given to ensuring cybersecurity in the Internet of Things and systems RBS. Attempts are made to present cyberspace of the Internet of Things with mathematical Graph Theory. We determined the key areas for regulation of operational risk in the context increasing of DDoS–threats. Factors that step–up level of impact cyberattacks are listed. It is analyzed the ways of information protection on the Internet of Things devices. Attention is drawn to the role of regulators in ensuring cybersecurity of banks in the context of RBS and the Internet of Things.

***Keywords**: remote banking service, Internet of Things, DDoS–attack, information security, botnet*

References:

1. Adel S. Elmaghraby, Michael M. Losavio. Cyber security challenges in Smart Cities: Safety, security and privacy // Journal of Advanced Research. July 2014. Volume 5, Issue 4. Pages 491-497.
2. Informatsionnye sistemy i tekhnologii v ekonomike i upravlenii: uchebnik / pod red. prof. V.V. Trofimova. 2-e izd., pererab. i dop. M.: Vysshee obrazovanie, 2007. 480 s.
3. Fedotov N.N. Forenzika – komp'yuternaya kriminalistika. M.: «Onebook.ru», 2012. 420 s.: il.
4. Markov A.S. Letopisi kibervoin i velichaishego v istorii pereraspredeleniya bogatstva // Voprosy kiberbezopasnosti. 2016. №1(14). C. 68-74.
5. Mezhdunarodnoe i zarubezhnoe finansovoe regulirovanie: instituty, sdelki, infrastruktura: monografiya / pod red. A.V. Shamraeva : v 2 ch. – Chast' vtoraya. M.: KNORUS: TsIPSiR, 2014. 640 s.
6. Rogozin D.O., Sheremet I.A., Garbuk S.V., Gubinskii A.M. Vysokie tekhnologii v SShA: opyt ministerstva oborony i drugikh vedomstv. M.: Izd-vo MGU, 2013. 384 s.
7. Revenkov P.V. Upravlenie riskami v usloviyakh elektronnogo bankinga: Monografiya. M.: Izdatel'skii dom «Ekonomicheskaya gazeta», 2011. 168 s.
8. Revenkov P.V., Berdyugin A.A. Kiberbezopasnost' v usloviyakh Interneta veshchei i elektronnogo bankinga // Natsional'nye interesy: prioritety i bezopasnost'. 2016. № 11 (344). S. 158-169.
9. Kiberprestupnost' stanovitsya organizovannee i slozhnee // Bankovskie tekhnologii. 2016. № 11/12. S. 76-79.
10. King Brett. Bank 3.0. Pochemu segodnya bank – eto ne to, kuda vy khodite, a to, chto vy delaete. – M.: ZAO «Olimp – Biznes», 2014. 520 s.
11. Lyamin L.V. Primenenie tekhnologii elektronnogo bankinga: risk-orientirovannyi podkhod. M.: KNORUS: TsIPSiR, 2011. 336 s.
12. Internet-tekhnologii v bankovskom biznese: perspektivy i riski: uchebno-prakticheskoe posobie / Yu.N. Yudenkov, N.A. Tysyachnikova, I.V. Sandalov, S.L. Ermakov. – 2-e izd., ster. – M.: KNORUS, 2014. 318 s.

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

14 Alexandr Berdyugin, graduate student of the Department «Information Security», Financial University under the Government of the Russia. E-mail: a40546b@gmail.com