Александр А. Бердюгин
Финансовый университет при Правительстве Российской Федерации,
Щербаковская ул., 38, г. Москва, 105187, Россия
e-mail: brdgn@bk.ru, https://orcid.org/0000-0003-2301-1776

РАЗРАБОТКА АЛГОРИТМА ОЦЕНКИ РИСКА ВОЗДЕЙСТВИЯ КИБЕРАТАК В УСЛОВИЯХ ЭЛЕКТРОННОГО БАНКИНГА

DOI: http://dx.doi.org/10.26583/bit.2019.2.06

Аннотация. Основная задача банковского риск-менеджмента состоит в оптимизации банковских бизнес-процессов. Актуальность выбранной темы обусловлена необходимостью проработки оценки риска воздействия кибератак (РВКа) на системы электронного банкинга (СЭБ). Цель статьи – формализация алгоритма оценки РВКа в организациях кредитно-финансовой сферы. Решаемые в работе задачи направлены на развитие оценки риска для решения существующих и потенциальных проблем и с учётом новых систем и инноваций, которые уже проникли в нашу жизнь и которые ожидают нас в будущем. Сформулировано определение РВКа на СЭБ. Внимание уделяется необходимости использования математических моделей оценки показателей эффективности системы менеджмента информационной безопасности (СМИБ). Обсуждены некоторые методы оценки риска, в том числе с учётом постоянно растущих вычислительных возможностей и доступности кибератак. Анализируется расчёт требований к капиталу, резервируемому для покрытия потерь в ходе операционной деятельности банка, предлагаемый соглашением Базельского комитета по банковскому надзору (Basel II). Рассмотрены варианты количественной оценки риска разными экспертами. Подробно описывается количественная оценка эффективности кибероружия, которая зависит от обстоятельств, отягчающих ответственность взломщика. Цель оценки риска заключается в представлении объективной информации, необходимой для принятия решения об обработке риска. Делаются выводы об избыточных функциях безопасности, которые снижают качество безопасности. Приведены примеры рудиментарных компонентов СМИБ. Подчёркнуты различия между неэмбоссированной пластиковой картой «Золотая корона» и картами других платёжных систем. В заключении говорится о построении структуры управления РВКа. Результаты работы могут быть использованы для более детальных исследований РВКа на СЭБ.

Ключевые слова: киберпространство, кибербезопасность, кибератаки, электронный банкинг, оценка риска, Базельский комитет по банковскому надзору.

Для цитирования: БЕРДЮГИН, Александр А. РАЗРАБОТКА АЛГОРИТМА ОЦЕНКИ РИСКА ВОЗДЕЙСТВИЯ КИБЕРАТАК В УСЛОВИЯХ ЭЛЕКТРОННОГО БАНКИНГА. Безопасность информационных технологий, [S.l.], v. 26, n. 2, p. 86-94, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1201>. Дата доступа: 31 may 2019. doi:http://dx.doi.org/10.26583/bit.2019.2.06.

Alexander A. Berdyugin
Financial University under the Government of the Russian Federation,
Scherbakovskaya Street, 38, Moscow, 105187, Russia
e-mail: brdgn@bk.ru, https://orcid.org/0000-0003-2301-1776

Development of algorithm for assessment risk of cyber attacks in electronic banking

DOI: http://dx.doi.org/10.26583/bit.2019.2.06

Abstract. The main task of bank risk management is to streamline banking business processes. This subject arises from the need to study assessment of risk of cyberattacks impact on e-banking systems. The purpose of this paper is to formalize the algorithm for assessing risk of cyberattacks impact in organizations of credit and financial sphere. The problems solved in this work are aimed at improving the development of risk assessment for addressing of existing and potential challenges and considering the new systems and innovations that have already arrived in our lives as well as those are coming. The

definition of risk of cyberattacks impact on e-banking systems is formulated. Attention is given to employ mathematical models for evaluating the effectiveness of information security management system (ISMS). Some methods of risk assessment are discussed, also considering the ever-increasing computational capabilities and cyberattacks accessibility. The paper analyzes the calculation of capital requirements reserved to cover losses in the course of the Bank's operations, proposed by the agreement of the Basel Committee on banking supervision (Basel II). The options of quantitative risk assessment by different experts are considered. It describes in detail the quantitative assessment of the effectiveness of cyber weapons, which depends on the circumstances aggravating the responsibility of the attacker. The purpose of risk assessment is to provide objective information necessary to make a decision on risk treatment. Conclusions are drawn about redundant safety features, which reduce the quality of safety. Examples of rudimentary components of ISMS are given. The differences between the non-embossed plastic card "The Golden crown" and the cards of other payment systems are emphasized. In conclusion, it is said about the construction of the management structure. The results of the work can be used for more detailed studies of the risk of cyberattacks impact inherent in electronic banking.
Keywords: cyberspace, cybersecurity, cyberattacks, electronic banking, risk assessment, Basel Committee on Banking Supervision.
For citation: BERDYUGIN, Alexander A. Development of algorithm for assessment risk of cyber attacks in electronic banking. IT Security (Russia), [S.l.], v. 26, n. 2, p. 86-94, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1201>. Date accessed: 31 may 2019. doi:http://dx.doi.org/10.26583/bit.2019.2.06.

Введение

Интенсивное распространение информационных и телекоммуникационных технологий и их стремительное проникновение во все сферы человеческой деятельности выводит на новый уровень вопросы обеспечения кибербезопасности. Одновременно возникает потребность в разработке новых подходов и алгоритмов оценки рисков, связанных с особенностями функционирования систем электронного банкинга и работы организаций кредитно-финансовой сферы (ОКФС) в киберпространстве [1].

Согласно стандарту ISO/IEC 27032:2012, под киберпространством понимается «комплексная среда, возникшая в результате взаимодействия подключённых к сети «Интернет» людей, программного обеспечения и услуг, которая не существует в материальной (физической) форме». В свою очередь кибербезопасность представляет собой «сохранение конфиденциальности, целостности и доступности информации в киберпространстве» [2].

Применительно к кредитно-финансовой сфере введём понятие «риск воздействия кибератак» (РВКа), которым определим меру возрастания типичных банковских рисков[1] (включая финансовые потери), возникающих вследствие реализации кибератак на системы электронного банкинга (СЭБ) ОКФС. Под кибератаками будем понимать хакерские воздействия, инсайдерские инциденты и сбои автоматизированных банковских систем (АБС). Для объективной оценки РВКа необходимо учитывать не только обстоятельства финансовой организации, но и возможности киберпреступника.

1. Обоснование системы менеджмента информационной безопасности банка

Крупные ОКФС – это объекты критической информационной инфраструктуры (КИИ). Система менеджмента информационной безопасности (СМИБ) объектов КИИ

[1] Письмо Банка России от 23.06.2004 № 70-Т «О типичных банковских рисках».

должна быть отнесена к классу сложных систем[2]. Рациональность построения структуры таких систем обоснована подходом «Синтез через анализ» (рис. 1).

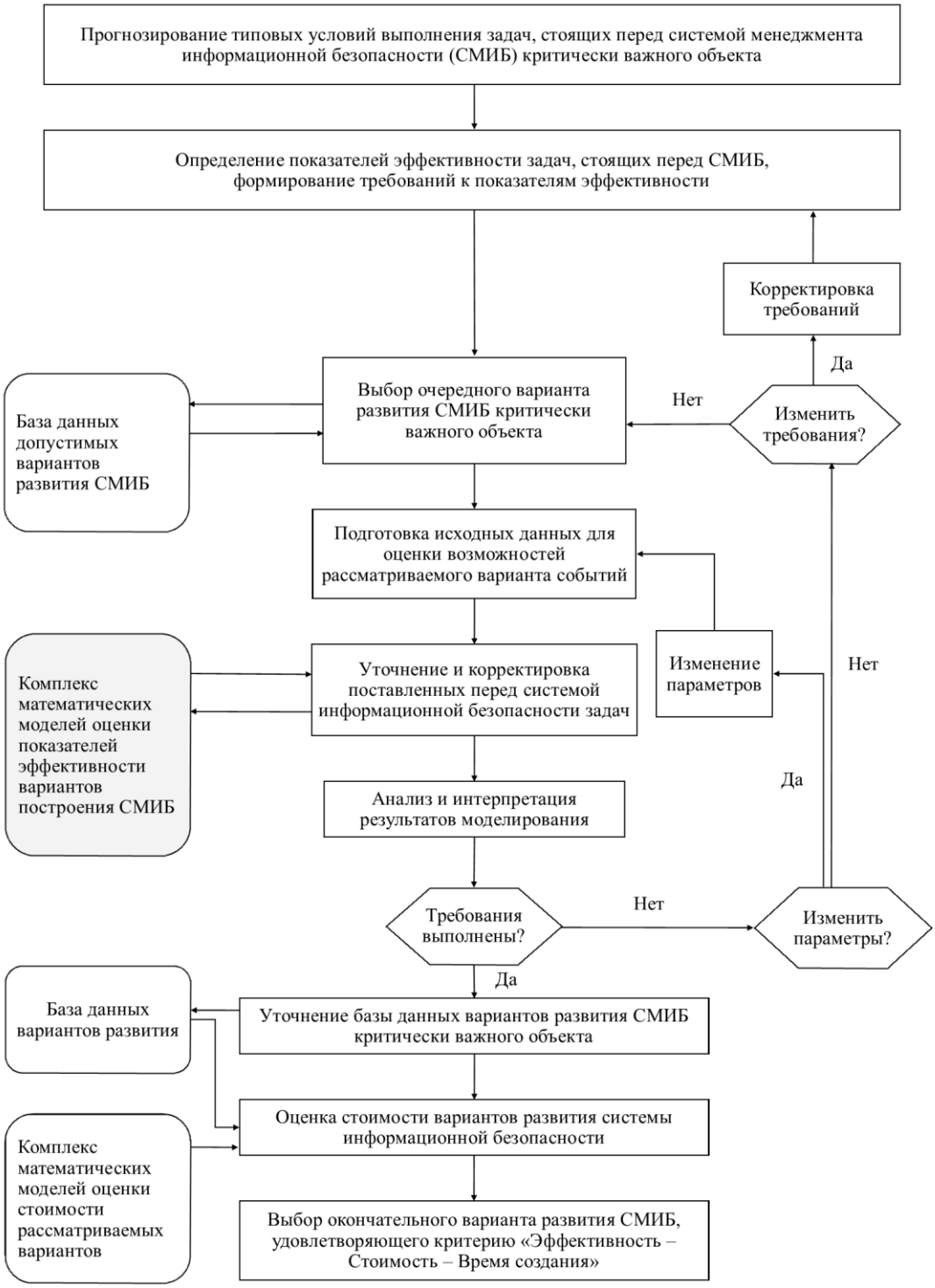

Рис. 1. Методика обоснования СМИБ «Синтез через анализ»
(Fig. 1. Methodology for justification of ISMS "Synthesis through analysis")

[2] О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон от 26 июля 2017 г. № 187-ФЗ (последняя редакция). URL: http://www.kremlin.ru/acts/bank/42128/page/1 (дата обращения 20.03.2019).

Методика обоснования СМИБ предложена в работе [3] и адаптирована к теме статьи. Математические модели оценки показателей эффективности СМИБ являются ключевым элементом методики, состав и структура которого определяются задачами защищаемой информационной системы и её функциями (сбор, хранение, обработка, передача и распространение). Некоторые из этих моделей характеризуются далее.

2. Методы оценки рисков воздействия кибератак на банки

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 РВКа чаще всего применяются:

• Метод «Дельфи» – получение мнения группы экспертов, которые выражают своё мнение индивидуально и анонимно, при этом имея возможность узнать мнения других экспертов. Результаты анализа обрабатываются статистическими методами.

• Байесовский анализ и Сети Байеса отличаются от классической статистики предположением, что параметры распределений являются не постоянными, а случайными переменными. В упрощённой форме теорема Байеса выглядит так:

$$P(A|B) = \{p(A) \cdot P(B|A)\} / P(B), \quad (1)$$

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[3] – 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 управления РВКа большой вклад внесли научные группы и компании в сфере информационных технологий, разработавшие различные методики оценки рисков. Наиболее значимые методики:

- ГРИФ компании «Digital security»;
- CCTA Risk Analysis and Management Method (CRAMM);
- методика анализа и контроля рисков RiskWatch;
- метод Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE);
- руководство по управлению рисками от компании Microsoft.

Вышеперечисленные методы позволяют оценить масштабы РВКа и необходимый уровень инвестиций в СМИБ для обеспечения её максимальной эффективности. В рамках данной статьи будет рассмотрена вероятность прямых и косвенных убытков для компании от возможной реализации РВКа.

Соглашение Базельского комитета по банковскому надзору (Basel II) для расчёта базовым индикативным методом требований к капиталу, резервируемому для покрытия потерь в ходе операционной деятельности банка, предлагает следующую формулу:

$$K_{OP} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^{3} ВД_i \quad (2)$$

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

Здесь K_{OP} – величина капитала для покрытия операционных рисков, $\frac{1}{3}\cdot\sum_{i=1}^{3} ВД_i$ – средняя величина валового дохода за последние 3 года, при условии, что $ВД_i > 0$; $\alpha = 15\%$ – коэффициент, установленный Базельским комитетом на основе опроса банков разных стран Европы [5]. Оценка размера капитала, выделяемого для покрытия операционных рисков (в том числе РВКа) по формуле (4) и данным отчётности по Российским стандартам бухгалтерского учёта «Отчёт о прибылях и убытках», для крупного российского коммерческого банка[4] выглядит следующим образом (табл. 1):

Таблица 1. Оценка размера капитала для покрытия операционных рисков в коммерческом банке страны методом базового индикатора

Наименование показателя, (тыс. руб.)/годы	**2018 год**	**2017 год**	**2016 год**
Процентные доходы (1)	8 691 892,00	5 924 488,00	4 419 351,00
Процентные расходы (2)	5 392 392,00	3 562 107,00	2 541 464,00
Чистые процентные доходы (3) = (1) – (2)	3 299 500,00	2 362 381,00	1 877 887,00
Чистые доходы от операций с ценными бумагами (4)	15 684,00	42 324,00	3 827,00
Чистые доходы от операций с иностранной валютой (5)	– 107 046,00	– 1 111 528,00	27 075,00
Чистые доходы от переоценки иностранной валюты (6)	141 596,00	1 148 287,00	– 43 134,00
Комиссионные доходы (7)	562 648,00	765 255,00	957 477,00
Прочие операционные доходы (8)	29 884,00	97 228,00	441 307,00
Итого валового дохода (9) = (3) + (4) +(5) + (6) + (7) + (8)	3 942 266,00	3 303 947,00	3 264 439,00
Среднее значение валового дохода			3 503 550,67
Требования к капиталу по операционному риску (15% от валового дохода)			525 532,60

Таким образом, требования к капиталу по операционному риску (15% от валового дохода) составляют 525 532,60 рублей. Базовый индикативный метод не учитывает физической составляющей РВКа. Учёт и оценка РВКа должны проводится в соответствии с вероятными последствиями для банка (такими как нарушение непрерывности банковской деятельности, отказ функционирования АБС, непредусмотренный финансовый ущерб), то есть на основе риск-ориентированного подхода [4].

Риск-аналитики и специалисты службы внутреннего контроля должны иметь в арсенале методики оценки РВКа, учитывающие взаимосвязи технических уязвимостей в АБС, организационных и экономических недостатков в действующих бизнес-процессах банка с масштабами ущерба для конкретной организации.

Аналитик-эксперт должен ответить на ряд контрольных вопросов по пятибалльной шкале, чтобы получить информацию о качестве управления РВКа на предприятии. Каждый вопрос имеет свой вес, который аналитик определяет самостоятельно экспертным

[4] Отчётность по РСБУ. URL: https://mkb.ru/investor/report/rsbu (дата обращения: 07.03.2019).

путём, предварительно согласовав свои действия с руководством. Индекс соответствия компонентов банка нормам внутренних нормативных актов определяется по формуле:

$$AGR = \frac{\sum(\text{Балл} \times \text{Вес})}{\sum \text{Весов}} \quad (3)$$

Значение индикатора AGR обратно пропорционально уровню качества системы управления РВКа в СЭБ. Однако, такая оценка AGR, предложенная в руководстве [6], представляет собой среднее арифметическое взвешенное и явно превышает единицу, что противоречит математическому определению вероятности, чем и является риск. Поэтому вычислим AGR проще – без присвоения веса (уровня значимости) вопросам:

$$AGR = \frac{\sum вопросов}{\sum баллов} \quad (4)$$

Некоторые эксперты [7, 8] предлагают оценивать возможные потери, используя достаточно общую формулу, в которой риск R определяется на основании агрегированных индексов качества обеспечения информационной безопасности AGR и так называемой «суммы под риском» S_R, показывающей величину ущерба.

Разделим мероприятия, выраженные агрегированными индексами, оценивающими обеспечение информационной безопасности, на программные $AGR_{ПРГ}$ и экономические $AGR_{ЭКН}$. Формула оценки РВКа имеет вид:

$$R = S_R \cdot \left(AGR_{ПРГ} + AGR_{ЭКН}\right) \quad (5)$$

Реальная практика включает также юридические, аппаратные, криптографические и физические меры безопасности. Аппаратные, программные и криптографические меры можно объединить в технические. Перечень контрольных вопросов и способ определения индексов AGR приведён в работах [7, 9, 10], относятся к соблюдению политики информационной безопасности и для экономии места в статье опускается.

Преимущество данного подхода над тем, который предлагает Basel II, состоит в учёте индивидуальных особенностей аппаратно-программного обеспечения (АПО) конкретного банка без универсальных коэффициентов для общего случая.

3. Разработка алгоритма оценки РВКа

Для выработки соответствующих контрмер по обеспечению кибербезопасности рассмотрим связь обстоятельств, отягчающих ответственность взломщика, образующих эффективность кибероружия, которую можно оценить численно в зависимости:

1) от возрастания размера ущерба, понесённого вследствие реализации РВКа в СЭБ, – условные денежные единицы (n);

2) от эскалации усреднённого значения коэффициента интеллектуального развития киберпреступников, привлечённых к ответственности (IQ);[5]

3) от возрастания периода времени, затраченного на восстановление непрерывности банковской деятельности после реализации РВКа, – часы (r);

4) от снижения промежутка времени, необходимого для изготовления и применения кибероружия для реализации РВКа, – часы (t);

[5] Определение источника угрозы выходит за рамки исследования. Однако все действия в Интернете отслеживаются Web-серверами, регистрируются в специальных журналах и могут быть предоставлены защите потерпевшей стороны.

5) от сокращения стоимости производства/приобретения АПО для реализации кибератак – условные денежные единицы (d);

6) от снижения количества накладных расходов по использованию АПО для нарушения кибербезопасности – условные денежные единицы (v).

Определение эффективности ff кибероружия выглядит следующим образом:

$$ff = \frac{n \cdot IQ \cdot r}{(d+v) \cdot t} \quad (6)$$

За основу взята формула из [11] и модифицирована автором настоящей статьи. Наиболее уместна формула (6) при оценке эффективности ботнета (сети хостов с работающими ботами, используемой обычно для проведения DDoS-атак). В состав ботнета могут входить устройства интернета вещей, защита которых описана в [12, 13].

Сочетание формул (2), (4), (5) и (6) позволяет оценить размер капитала, выделяемого для покрытия убытков от РВКа следующим образом:

$$R_{PBKa} = \frac{K_{OP}}{ff} + S_R \cdot AGR \quad (7)$$

Здесь ff – безразмерный коэффициент, который позволяет дать количественную оценку действиям взломщика и определить их долю в составе K_{OP}. Таким образом, использование формулы (7) системой управления непрерывностью деятельности кредитной организации развивает и детализирует оценку РВКа, что способствует росту ответственности ОКФС за электронный банкинг.

Компоненты СМИБ, которые утратили своё основное значение, снижают общий уровень безопасности. Пример рудиментарного компонента СМИБ – голосовой звук парнокопытного животного, воспроизводимый известным антивирусом при обнаружении вирусной атаки. Вспоминается притча Л.Н. Толстого про пастуха-шутника [14]. Этот маркетинговый ход может вызвать желание отключить программу, занимает строчки программного кода и ресурсы компьютера [15].

Такие дефекты кажутся незначительными и не могут быть учтены при оценке РВКа по формулам (2), (5) или (7). Их математическое моделирование аналогично легендарной задаче о зёрнах на шахматной доске, где нужно определить сумму зёрен при увеличении их количества в 2 раза на следующей клетке, начиная с одного. Зёрна аналогичны дефектам, клетки доски – рабочим дням, основание 2 – абстрактное выражение изъяна человеческого фактора в системе «Человек – Машина».

Шахматная доска состоит из $8 \times 8 = 64$ клеток. Сумма зёрен при их удвоении:

$$Zr_{64} = 1 + 2 + 4 + 8 + ... + 2^{63} = \sum_{i=0}^{63} 2^i = 2^{64} - 1 = 1844674407\ 3709551615 \quad (8)$$

Значение $Zr_{64} = 2^{64} - 1$ представляет собой максимальное 64-битное беззнаковое целое FFFF FFFF FFFF $FFFF_{16}$. Таковы вероятные последствия операционного дефекта, подтверждающие слова президента ПАО «Сбербанк России» Г.О. Грефа о том, что «маленькая ошибка, закравшаяся в алгоритм, может приводить к очень большим последствиям»[6].

Хотелось бы выразить замечание о пластиковых картах платёжных систем России. На поверхности банковской карты «Золотая корона» отсутствуют идентификационные номера (номер карты, код безопасности, срок действия), фамилия и имя владельца. Это

[6] Г.О. Греф заявил, что Сбербанк потерял миллиарды рублей из-за ошибок искусственного интеллекта. URL: https://tass.ru/ekonomika/6158745 (дата обращения 26.02.2019).

снижает потери от приёмов социальной инженерии. Мошенник, который знает фамилию клиента и данные карты, убедительным голосом представляется сотрудником службы безопасности и требует назвать кодовое слово, может ввести в заблуждение многих.

Эмбоссированные или напечатанные номера представляют собой рудиментарные компоненты СМИБ (см. формулу (8)), оставшиеся после распространения импринтеров. Промежутка времени между потерей/кражей карты и моментом её блокирования пользователем в обслуживающем банке может оказаться достаточно для совершения мошеннических действий по опознавательным номерам на пластиковой карте, которых нет на картах системы «Золотая корона».

Заключение

Недостатки в работе СМИБ ОКФС (как объектов КИИ) представляют собой прямые источники операционного риска и РВКа включительно. Эти недостатки могут приводить к существенным потерям денежных средств как кредитной организации, так и её клиентов.

Структура управления РВКа должна базироваться:

- на рекомендациях регулирующих органов (Федеральная служба безопасности России, Центральный банк Российской Федерации, Федеральная служба по техническому и экспортному контролю и др.);
- на потребностях и масштабах бизнеса, приоритетных процессах, позволяющих обеспечивать эффективное управление данным риском;
- на научно-исследовательских и опытно-конструкторских работах учёных.

В статье сравниваются методы оценки рисков, формализован алгоритм оценки РВКа для ОКФС на основе имеющихся методов и показан экспоненциальный рост последствий операционного дефекта, возникшего как следствие рудиментарных компонентов СМИБ. Идентификационные номера на поверхности банковской карты являются рудиментарными компонентами СМИБ, снижающими её общий уровень.

СПИСОК ЛИТЕРАТУРЫ:

1. E. Zio. The future of risk assessment. Reliability Engineering & System Safety, vol. 177, September 2018, P. 176–190. URL: https://doi.org/10.1016/j.ress.2018.04.020.
2. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity // International Organization for Standardization. URL: http://www.iso.org/standard/44375.html (дата обращения: 05.03.2019).
3. Костогрызов А.И., Лазарев В.М., Любимов А.Е. Прогнозирование рисков для обеспечения эффективности систем информационной безопасности в их жизненном цикле // Правовая информатика. 2013. № 4. С. 4–16.
4. Разработка методики проверки сведений, предоставляемых при заключении договора о банковском обслуживании, на основе риск-ориентированного подхода: отчёт о НИР (заключительный) / Финансовый университет при Правительстве Российской Федерации, Руководитель Шеремет И.А.; исполнители: Дворянкин С.В., Евсеев В.Л., Скородумов Б.И., Велигура А.Н., Крылов Г.О., Овчинникова Ю.Е., Устинов Р.А., Бердюгин А.А., Воеводин А.Ю. М.: 2017. 191 с. № ГР АААА-А17-117060110141-9.
5. Алескеров Ф.Т., Андриевская И.К., Пеникас Г.И., Солодков В.М. Анализ математических моделей Базель II. – М.: ФИЗМАТЛИТ, 2013. – 296 с.
6. Волков А.А. Управление рисками в коммерческом банке: практическое руководство. – М.: Издательство «Омега-Л», 2015. – 156 с.
7. Ревенков П.В. Внутренний контроль в банках: оценка риска воздействия компьютерных атак // Финансы и кредит. 2019. Т. 25, № 3. С. 500–513. URL: https://doi.org/10.24891/fc.25.3.500.
8. Кузнецов А.В., Ненашев С.М. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5 (13). С. 23–25.
9. Славин Б.Б. В «обществе 5.0» главную движущую силу развития составляют наукоемкие знания // БИТ. Бизнес & Информационные технологии. 2019. № 1 (84). С. 56–59.
10. 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. DOI: 10.24891/fc.24.3.629.

11. Расторгуев С.П. О проявлении скрытых в структуре системы предрасположенностей // Информационные войны. 2017. № 1 (41). С. 92–97.
12. Астье, Жан Ив; Жуков, Игорь Юрьевич; Мурашов, Олег Николаевич. Системы управления «умный дом» и Интернет вещей. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 18-29, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/260> (дата обращения: 01. 03. 2019). doi:http://dx.doi.org/10.26583/bit.2017.3.02.
13. Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of software vulnerability detection in certification testing, Journal of Physics: Conference Series (см. в книгах), 2018, vol. 1015. P. 042033. DOI: 10.1088/1742-6596/1015/4/042033.
14. Синки Дж. Финансовый менеджмент в коммерческом банке и в индустрии финансовых услуг. – М.: Альпина Бизнес Букс, 2017. – 1018 с.
15. Козлов Ю.Е., Евсеев В.Л. Мультимодальная трехмерная динамическая подпись // Безопасность информационных технологий. 2017. Т. 24. № 4. С. 44–51.

REFERENCES:

[1] E. Zio. The future of risk assessment. Reliability Engineering & System Safety, vol. 177, September 2018, P. 176–190. DOI: https://doi.org/10.1016/j.ress.2018.04.020.
[2] ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. International Organization for Standardization. URL: http://www.iso.org/standard/44375.html (accessed: 05.03.2019).
[3] Kostogryzov A.I., Lazarev V.M., Lyubimov A.E. Risk prediction to ensure effectiveness of information security systems in their life cycle. Legal Informatics [Pravovaya informatika]. 2013, №. 4. P. 4–16. (in Russian).
[4] Sheremet I. A., Dvoryankin S. V., Evseev V. L., Skorodumov B. I., Veligura A. N., Krylov G. O., Ovchinnikova Yu. E., Ustinov R. A., Berdyugin A. A., Voevodin A. Yu. Razrabotka metodiki proverki svedeniy, predostavlyayemykh pri zaklyuchenii dogovora o bankovskom obsluzhivanii, na osnove risk-oriyentirovannogo podkhoda. Otchet o NIR [Development of methodology for verifying information provided when concluding a contract on banking services based on risk-management. Report on research]. Moscow, Financial University under the Government of the Russian Federation, 2017. 191 p. SR number AAAA-A17-117060110141-9 (in Russian).
[5] Aleskerov F.T., Andrievskaya I.K., Penikas G.I., Solodkov V.M. Analiz matematicheskikh modeleĭ Bazel' II [Analysis of mathematical models of Basel II]. Moscow, FIZMATLIT Publ., 2013. 296 p.
[6] Volkov A.A. Upravlenie riskami v kommercheskom banke: prakticheskoe rukovodstvo [Risk management in commercial bank: A practical guide]. Moscow, Omega-L Publ., 2015, 156 p.
[7] Revenkov P.V. Internal control in banks: Assessing the risk of cyber attacks. Finansy i kredit [Finance and Credit]. 2019, vol. 25, №. 3. S. 500–513. URL: https://doi.org/10.24891/fc.25.3.500. (In Russian).
[8] Kuznetsov A.V., Nenashev S.M. Method of determining recorded events. Cybersecurity issues [Voprosy kiberbezopasnosti]. 2015, № 5 (13). P. 23–25. (in Russian).
[9] Slavin B.B. In “society 5.0” high-tech knowledge constitutes the main driving force for development. BIT. Business & Information Technology [BIT. Biznes & Informatsionnyye tekhnologii]. 2019, vol. 1 (84). P. 56–59. (in Russian).
[10] 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, №. 3. P. 629–640. DOI: 10.24891/fc.24.3.629 (in Russian)
[11] Rastorguev S.P. About manifestation of hidden predispositions in structure of system. Information Wars [Informatsionnyye voyny]. 2017, № 1 (41). P. 92–97. (in Russian).
[12] Astier, Jean Yves; Zhukov, Igor Yurievich; Murashov, Oleg Nikolaevich. Smart Building Management Systems and Internet of Things. IT Security, [S.l.], v. 24, n. 3, p. 18-29, july 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/260 (accessed: 01. 03. 2019) doi:http://dx.doi.org/10.26583/bit.2017.3.02.
[13] Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of software vulnerability detection in certification testing, Journal of Physics: Conference Series (see in books), 2018, vol. 1015. P. 042033. DOI: 10.1088/1742-6596/1015/4/042033.
[14] Joseph F. Sinkey. Finansovyy menedzhment v kommercheskom banke i v industrii finansovykh uslug [Commercial bank financial management in the financial-services industry]. Moscow, Alpina Business Books, 2017. 1018 p.
[15] Kozlov Yu.E., Evseev V.L. Multimodal three-dimensional dynamic signature. Information technology security [Bezopasnost' informatsionnykh tekhnologiy]. 2017, vol. 24, №. 4. P. 44–51. (in Russian).

Поступила в редакцию – 03 апреля 2019 г. Окончательный вариант – 31 мая 2019 г.
Received – April 03, 2019. The final version – May 31, 2019.