УДК 004.056 DOI: 10.18698/2541-8009-2018-04-294

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РАЗРАБОТКИ МЕТОДИКИ УПРАВЛЕНИЯ РИСКАМИ В GRC-РЕШЕНИИ ДЛЯ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РФ И ЕЕ РЕШЕНИЕ

О.С. Абрамова mol4el93@yandex.ru
SPIN-код: 3360-1088

Е.В. Постернак kripsy93@yandex.ru
SPIN-код: 7581-4305

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Многие виды деятельности активно регулируются государством в области информационной безопасности. В данной статье рассмотрена необходимость применения системы класса GRC для организаций банковской системы в РФ. Одним из регуляторов в банковской сфере выступает Банк России. В данной статье рассмотрены документы, которые регулируют процесс управления рисками в организациях банковской системы РФ. Описана математическая модель методики управления рисками в GRC-решении для организаций банковской системы РФ и ее решение, необходимые для последующей разработки методики управления рисками.

Ключевые слова

Угрозы в информационной сфере, Банк России, информационный актив, информационная безопасность, оценка информационных рисков, средство защиты информации, модель нарушителя, менеджмент информационной безопасности, уровень защиты информации

Поступила в редакцию 29.03.2018

Введение. Информационная безопасность (ИБ) — состояние защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере [1]. Основная цель бизнеса — получение прибыли. Угрозы могут повлечь финансовые потери, падение репутации, санкции со стороны государства. Менеджмент рисков ИБ является ядром системы менеджмента [2]. Эффективная система менеджмента информационной безопасности (СМИБ) позволяет выявить недостатки в информационной системе, но требует первоначальных финансовых вложений [3].

Одно из главных условий успешного внедрения системы управления ИБ — систематическое выполнение следующих процессов: пересмотр угроз, анализ рисков, отслеживание инцидентов [4]. Для поддержания перечисленных выше процессов целесообразно применять систему класса Governance, Risk management and Compliance (GRC).

Концепция GRC-системы заключается в том, что деятельность компании разделяется на три компонента: корпоративное управление, управление рисками и соблюдение требований. GRC-система позволяет управлять организацией в сфере информационной безопасности на основе оценки рисков в соответ-

ствии с нормативными правовыми и корпоративными требованиями по защите информации [5].

В силу того что концепция данных систем пришла с Запада относительно недавно, она мало ориентирована на российский рынок, что является проблемой для эффективного использования системы класса GRC. Для решения указанной проблемы необходимо проанализировать нормативную базу, сформировать требования к управлению рисками в GRC-системе для организаций банковской системы РФ, что позволит разработать математическую модель разработки методики управления рисками в GRC.

Методика оценки рисков нарушения информационной безопасности. Банк России — юридическое лицо, которое осуществляет надзор за деятельностью кредитных организаций и банковских групп.

Банк России в качестве рекомендаций предлагает методику оценки рисков информационной безопасности РС БР ИББС–2.2–2009 для предоставления формализованного способа анализа системы обеспечения ИБ, выявления слабых мест в защите, что способствует совершенствованию уровня системы обеспечения ИБ [6].

В методике РС БР ИББС–2.2–2009 установлены способы и порядки проведения оценки рисков нарушения ИБ организаций банковской системы РФ. Данная методика сформирована на базе подходов к управлению рисками, предлагаемых комплексом международных стандартов серии 27000, включая опыт Банка России [7]. В документе определяется подход к оценке рисков нарушения ИБ:

1) определение перечня типов информационных активов на основе классификации информационных активов;

2) определение перечня типов объектов среды для каждого из типа информационных активов;

3) определение источников угроз для каждого из типов объектов среды;

4) определение степени возможности реализации для указанных угроз;

5) определение степени тяжести последствий для указанных типов информационных активов;

6) проведение оценки рисков ИБ.

Следует указать, что в рамках данной методики основными свойствами ИБ считаются:

1) конфиденциальность;

2) целостность;

3) доступность.

Безопасность финансовых (банковских) операций. ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» позволяет достичь следующих целей:

1) определить уровни защиты информации и соответствующие им требования к содержанию базового состава организационных и технических мер защиты информации;

2) определить адекватный состав мер защиты информации актуальным угрозам безопасности информации и уровень принятого организацией операционного риска;

3) добиться эффективности стандартизированного контроля мероприятий по защите информации.

Математическая постановка задачи и ее решение. Для решения задачи разработки методики управления рисками в GRC-решении для организаций банковской системы РФ необходимо решить две отдельные задачи:

1) выявить недостаточность и избыточность применения контрмер к объектам среды;

2) определить наборы эффективных контрмер для обработки недопустимых рисков.

Постановка задачи определения недостаточности и избыточности применения контрмер. Пусть $O = \{o_1,...,o_n\}$ — множество объектов среды информационной системы банковской организации, $K = \{k_1,...,k_m\}$ — множество организационных и технических мер защиты информации, $T = \{t_1,...,t_n\}$ — множество базовых наборов контрмер (требования к базовым наборам контрмер) для объектов множества O, где $t_i = \{t_i^1,...,t_i^m\}$, t_i^j определяется по формуле

$$t_i^j = \begin{cases} 0, \text{ если контрмера } k_j \text{ не обязательна к применению для объекта } o_i; \\ 1, \text{ иначе,} \end{cases}$$

где k_j — объект множества K; o_i — объект множества O.

Постановка задачи определения недостаточности и избыточности применения контрмер звучит следующим образом: необходимо оценить применение или неприменение каждой контрмеры из множества K к каждому объекту множества O, выявив недостаточность и избыточности применения контрмер согласно требованиям к базовым наборам контрмер T [8].

Решение задачи определения недостаточности и избыточности применения контрмер. Пусть матрица A_1 — матрица проверки выполнения требований для базового набора средств защиты:

$$A_1(i,j) = \begin{cases} 0, \text{ если контрмера } k_j \text{ для объекта } o_i \text{ обязательна, но не используется;} \\ 1, \text{ если контрмера } k_j \text{ для объекта } o_i \text{ не обязательна и не используется;} \\ 2, \text{ если контрмера } k_j \text{ для объекта } o_i \text{ обязательна и используется;} \\ 3, \text{ если контрмера } k_j \text{ для объекта } o_i \text{ не обязательна и не используется,} \end{cases}$$

где $A_1(i, j)$ — элемент матрицы $A_1[n, m]$; k_j — контрмера из множества K; o_i — объект из множества O.

Матрица $A_1[n,m]$ состоит из строк элементов множества *O* и из столбцов элементов множества *K*. Данная матрица предоставляет информацию о возможной недостаточности или избыточности применения контрмер.

Решение задачи определения недостаточности и избыточности применения контрмер: необходимо построить матрицу проверки выполнения требований для базового набора средств защиты $A_1[n,m]$. Если матрица $A_1[n,m]$ имеет хотя бы один элемент $A_1(i,j)$, значение которого равно нулю, необходимо рассмотреть применение контрмеры k_j к объекту среды o_i и пересмотреть данную матрицу снова. Требования для базового набора средств защиты выполнены, если матрица $A_1[n,m]$ не имеет нулевых элементов $A_1(i,j)$, в противном случае присутствует нарушение требований к базовому набору средств защиты. Если матрица $A_1[n,m]$ имеет значения, равные трем, необходимо рассмотреть применение контрмеры k_j к объекту o_i и пересмотреть данную матрицу снова [9]. Таким образом получится избавиться от необоснованной избыточности применения контрмер.

Постановка задачи определения наборов эффективных контрмер для обработки недопустимых рисков. Пусть $R=\{r_1,...,r_c\}$ — множество рисков информационной безопасности. Согласно ГОСТ Р 57580.1–2017, понизить риск можно лишь до определенного уровня, соответственно нет необходимости искать минимальный риск, достаточно добиться выполнения следующего условия — допустимая величина риска не должна быть меньше текущей величины риска.

Введем следующие понятия: уровень риска C_{r_i} — величина, показывающая уровень риска r_i на данный момент, целевой уровень риска $C_{\text{цел.}r_i}$ — величина, показывающая приемлемый уровень риска r_i, обработанный уровень риска $C_{\text{обраб.}r_i}$ — величина, показывающая уровень риска r_i после обработки, затраты на обработку риска $C_{\text{стоим.обраб.}r_i}$ — величина, показывающая стоимость обработки риска r_i.

Введем понятие недопустимость риска. Риск r_i является недопустимым, если выполняется неравенство

$$C_{r_i} > C_{\text{цел.}r_i},$$

где C_{r_i} — величина, показывающая уровень риска r_i на данный момент; $C_{\text{цел.}r_i}$ — величина, показывающая приемлемый уровень риска r_i.

Введем понятие обработанный риск. Риск r_i считается обработанным, если выполняется неравенство

$$C_{\text{обраб.}r_i} + C_{\text{стоим.обраб.}r_i} \le C_{\text{цел.}r_i},$$

где $C_{\text{обраб.}r_i}$ — величина, показывающая уровень риска r_i после обработки; $C_{\text{стоим.обраб.}r_i}$ — величина, показывающая стоимость обработки риска r_i; $C_{\text{цел.}r_i}$ — величина, показывающая приемлемый уровень риска r_i.

Постановка задачи определения набора эффективных контрмер для обработки каждого риска звучит следующим образом: во множестве R необходимо определить недопустимые риски и найти наборы эффективных контрмер для их обработки [10].

Решение задачи определения наборов эффективных контрмер для обработки недопустимых рисков. Введем понятие набор внедряемых контрмер для обработки риска r_i $K_{\text{внедр.}i} = \{k_1^i,...,k_m^i\}$, где k_j^i определяется по формуле

$$k_j^i = \begin{cases} 1, \text{ если контрмера } k_j \text{ используется для обработки риска } r_i; \\ 0, \text{ если иначе,} \end{cases}$$

где k_j — рассматриваемая контрмера из множества K; r_i — рассматриваемый риск из множества R.

Введем следующие понятия: уровень риска при внедрении набора контрмер $C_{K_{\text{внедр.}i}}$ — величина, показывающая уровень риска r_i на данный момент при внедрении набора контрмер $K_{\text{внедр.}i}$, стоимость внедрения набора контрмер при обработке риска r_i $C_{\text{контр.}K_{\text{внедр.}i}}$ — стоимость внедрения набора контрмер $K_{\text{внедр.}i}$ для обработки риска r_i [11].

Введем функцию C_i от m переменных — функция определения величины уровня риска r_i при внедрении набора контрмер $k_1^i,...,k_m^i$:

$$C_i(k_1^i,...,k_m^i) = y, \ y \in \mathbb{R},$$

где $k_1^i,...,k_m^i$ — набор внедряемых контрмер для обработки риска r_i; $\mathbb{R}$ — множество действительных чисел.

Введем функцию $C_{\text{контр.}i}$ от m переменных — функция определения стоимости внедрении набора контрмер $k_1^i,...,k_m^i$ для обработки риска r_i:

$$C_{\text{контр.}i}(k_1^i,...,k_m^i) = y, \ y \in \mathbb{R},$$

где $k_1^i,...,k_m^i$ — набор внедряемых контрмер для обработки риска r_i; $\mathbb{R}$ — множество действительных чисел.

Введем функцию $Ef_{\text{контр.}i}$ от m переменных — функция определения эффективности набора контрмер $k_1^i,...,k_m^i$ для риска r_i:

$$Ef_{\text{контр.}i}(k_1^i,...,k_m^i) = C_{\text{цел.}r_i} - C_i(k_1^i,...,k_m^i) - C_{\text{контр.}i}(k_1^i,...,k_m^i),$$

где $k_1^i,...,k_m^i$ — набор внедряемых контрмер для обработки риска r_i; $C_{\text{цел.}r_i}$ — величина, показывающая приемлемый уровень риска r_i; $C_i(k_1^i,...,k_m^i)$ — функция

определения величины уровня риска r_i при внедрении набора контрмер $k_1^i,...,k_m^i$; $C_{\text{контр.}i}(k_1^i,...,k_m^i)$ — функция определения стоимости внедрения набора контрмер $k_1^i,...,k_m^i$ для обработки риска r_i.

Введем определение эффективный набор контрмер $K_{\text{эф.контр.}i} = \{k_1^i,...,k_m^i\}$ для обработки риска r_i:

$$K_{\text{эф.контр.}i} = \max_{K_{\text{внедр.}i}^j = \left\{k_1^i,...,k_m^i\right\}} \left(Ef_{\text{контр.}i}(K_{\text{внедр.}i}^0),...,Ef_{\text{контр.}i}(K_{\text{внедр.}i}^{2^m}) \right),$$

где $Ef_{\text{контр.}i}(K_{\text{внедр.}i}^l)$ — функция определения эффективности одного из наборов контрмер $k_1^i,...,k_m^i$ для риска r_i.

Решение задачи определения набора эффективных контрмер для обработки недопустимых рисков звучит следующим образом: необходимо для каждого риска r_i из множества R найти эффективный набор контрмер $K_{\text{эф.контр.}i} = \{k_1^i,...,k_m^i\}$ [12].

Выводы. Данная работа позволила сформулировать математическую постановку задачи разработки методики управления рисками в GRC-решении для организаций банковской системы РФ и ее решение.

Сформулированная математическая постановка является основой для разработки методики управления рисками в GRC-решении для организаций банковской системы РФ.

Разработка методики управления рисками в рамках системы класса GRC для организации банковской системы РФ поможет усовершенствовать систему менеджмента информационной безопасности, повысить эффективность проведения аудита на соответствие требованиям стандартов [13].

Следующий этап научной работы заключается в описании модели управления рисками, детализация объектов и процессов, которые должны присутствовать в системе.

На основе данной методики будет реализован соответствующий модуль системы класса GRC.

Литература

[1] Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции. *Вопросы кибербезопасности*, 2014, № 1(2), с. 67–73.

[2] Дорофеев А.В. Менеджмент информационной безопасности: управление рисками. *Вопросы кибербезопасности*, 2014, № 2(3), с. 66–73.

[3] Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности. *Вопросы кибербезопасности*, 2014, № 4(7), с. 49–54.

[4] Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры. *Вопросы кибербезопасности*, 2013, № 1(1), с. 17–27.

[5] Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. *Семь безопасных информационных технологий*. Москва, ДМК Пресс, 2017, 224 с.

[6] Скворцов М.А., Шахалов И.Ю. Обзор методов и средств оценки рисков информационной безопасности. *Безопасные информационные технологии (Бит-2016)*. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2016, с. 265–269.

[7] Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013. *Вопросы кибербезопасности*, 2014, № 3(4), с. 69–73.

[8] Булдакова Т.И., Миков Д.А. Обеспечение согласованности и адекватности оценки факторов риска информационной безопасности. *Вопросы кибербезопасности*, 2017, № 3(21), с. 8–15.

[9] Чукляев И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем. *Вопросы кибербезопасности*, 2016, № 4(17), с. 61–71.

[10] Казарин О.В., Репин М.М. Особенности анализа рисков утечки конфиденциальной информации по техническим каналам при создании радиоэлектронных средств. *Вопросы кибербезопасности*, 2015, № 4(12), с. 62–69.

[11] Петренко Ю.А., Петренко С.А. Лучшая практика управления непрерывностью бизнеса. *Защита информации. Инсайд*, 2010, № 5(35), с. 12–21.

[12] Никифоров Д.А. Эволюция ИБ. Разработки в области защиты информации, изменившиеся до неузнаваемости. *Защита информации. Инсайд*, 2015, № 6(66), с. 44–45.

[13] Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз. *Вопросы кибербезопасности*, 2017, № 3(21), с. 16–23.

Абрамова Ольга Сергеевна — студентка кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Постернак Евгений Валерьевич — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Шахалов Игорь Юрьевич, доцент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

MATHEMATICAL REPRESENTATION OF DEVELOPING RISK MANAGEMENT PRINCIPLES IN GRC-SOLUTION FOR THE BANKING SYSTEM ORGANIZATIONS OF THE RUSSIAN FEDERATION AND ITS DERIVATION

O.S. Abramova mol4el93@yandex.ru
SPIN-code: 3360-1088

E.V. Posternak kripsy93@yandex.ru
SPIN-code: 7581-4305

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Many types of activity are actively regulated by the state in the information security area. This article considers the necessity for applying the system of the GRC class for the banking system organizations in the Russian Federation. The Bank of Russia is one of the regulators in the banking sector. The article examines the documentation that regulates the risk management process in the banking system organizations of the Russian Federation. We describe a mathematical model of the risk management techniques in the GRC-solution for the banking system organizations of the Russian Federation and its derivation, necessary for the follow-on development of the risk management techniques.

Keywords

Threatening in the area of information, the Bank of Russia, data asset, information security, information security risk assessment, information security tool, adversary model, information security management, information protection level

References

[1] Dorofeev A.V., Markov A.S. Information security management: basic concepts. *Voprosy kiberbezopasnosti*, 2014, no. 1(2), pp. 67–73.

[2] Dorofeev A.V. Information security management: risk management. *Voprosy kiberbezopasnosti*, 2014, no. 2(3), pp. 66–73.

[3] Mikov D.A. Analysis of methods and tools which are used in the various stages of information security risk assessment. *Voprosy kiberbezopasnosti*, 2014, no. 4(7), pp. 49–54.

[4] Chobanyan V.A., Shakhalov I.Yu. Analysis and synthesis of the requirements to the systems of safety of objects of the critical information infrastructure. *Voprosy kiberbezopasnosti*, 2013, no. 1(1), pp. 17–27.

[5] Barabanov A.V., Dorofeev A.V., Markov A.S., Tsirlov V.L. Sem' bezopasnykh informatsionnykh tekhnologiy [Seven safe informational technologies]. Moscow, DMK Press publ., 2017, 224 p.

[6] Skvortsov M.A., Shakhalov I.Yu. Obzor metodov i sredstv otsenki riskov informatsionnoy bezopasnosti [Review on methods and tools of informational security risk assessment]. *Bezopasnye informatsionnye tekhnologii (Bit-2016)* [Safe Informational Technologies (BIT-2016)]. Moscow, Bauman Press, 2016, pp. 265–269.

[7] Dorofeev A.V. Information security management: transition to ISO 27001: 2013. *Voprosy kiberbezopasnosti,* 2014, no. 3(4), pp. 69–73.

[8] Buldakova T.I., Mikov D.A. Ensuring the concordance and the adequacy of information security risk factors assessment. *Voprosy kiberbezopasnosti*, 2017, no. 3(21), pp. 8–15.
[9] Chuklyaev I.I. Methodical providing complex management of risks of informational security of function-oriented information resources management information systems. *Voprosy kiberbezopasnosti*, 2016, no. 4(17), pp. 61–71.
[10] Kazarin O.V., Repin M.M. The features of the risk analysis of confidential information leak through technical channels for creating radio-electronic equipment. *Voprosy kiberbezopasnosti*, 2015, no. 4(12), pp. 62–69.
[11] Petrenko Yu.A., Petrenko S.A. The best practice to control business continuity. *Zashchita informatsii. Insayd*, 2010, no. 5(35), pp. 12–21.
[12] Nikiforov D.A. Evolyutsiya IB. Evolution of information security: developments that have changed beyond recognition. *Zashchita informatsii. Insayd*, 2015, no. 6(66), pp. 44–45.
[13] Revenkov P.V., Berdyugin A.A. Expansion of the operational risk profile in banks under increase of DDoS-threats. *Voprosy kiberbezopasnosti*, 2017, no. 3(21), pp. 16–23.

Abramova O.S. — student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Posternak E.V. — student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — I.Yu. Shakhalov, Assoc. Professor, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.