УДК 004.056
DOI: 10.26102/2310-6018/2025.51.4.008

Моделирование обеспечения защищенности объектов критической информационной инфраструктуры финансового сектора на основе данных об организационной структуре и управлении

М.Г. Журавлева✉, Н.Ю. Сурова, З.Р. Хасанова

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Резюме. Рассмотрены современные стандарты и подходы в области обеспечения защищенности объектов критической информационной инфраструктуры применительно к организациям банковской системы. В качестве исследуемых аспектов выделены организационная структура и управления, которые оказывают влияние на уровень защищенности с точки зрения степени подготовленности персонала, распределения ролей и полномочий, готовности организации к восстановлению после возникновения инцидентов нарушения безопасности. На основе методики внутреннего аудита, применяемой в организациях банковской системы для поддержания защищенности объектов информационной инфраструктуры на достаточном уровне, предложена модель, учитывающая экспертные оценки заданных показателей организационной структуры и управления. Показаны направления улучшения метода: возможность учитывать иерархию требований к обеспечению безопасности, использовать логические правила в экспертном оценивании, на основании чего построена улучшенная модель. В качестве результатов представлена иерархия заданных частных показателей, полученная по их вербальным формулировкам, смоделированы данные и выполнена оценка уровня обеспечения информационной безопасности с помощью рассмотренных подходов. Практическая ценность работы состоит в возможности на ее основе совершенствовать мероприятия внутреннего аудита субъектов банковской системы для обеспечения достаточного уровня защищенности объектов критической информационной инфраструктуры.

Ключевые слова: обеспечение информационной безопасности, показатели требований к безопасности, уровень защищенности объектов, организации банковской системы, методика оценки соответствия, критическая информационная инфраструктура.

Благодарности: Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Для цитирования: Журавлева М.Г., Сурова Н.Ю., Хасанова З.Р. Моделирование обеспечения защищенности объектов критической информационной инфраструктуры финансового сектора на основе данных об организационной структуре и управлении. *Моделирование, оптимизация и информационные технологии.* 2025;13(4). URL: https://moitvivt.ru/ru/journal/pdf?id=2046 DOI: 10.26102/2310-6018/2025.51.4.008

Modeling the security of critical information infrastructure of the financial sector based on organizational structure and management data

M.G. Zhuravlyova✉, N.Yu. Surova, Z.R. Khasanova

Financial University under the Government of the Russian Federation, Moscow, the Russian Federation

Abstract. Standards and approaches are considered in the field of ensuring the security of critical information infrastructure objects applied to banking system organizations. The aspects under study include the organizational structure and management, which affect the level of security in terms of the degree of personnel training, distribution of roles and powers, and the organization's readiness to recover from security incidents. Based on the internal audit methodology used in banking system organizations to maintain the security of information infrastructure objects at a sufficient level, a model is proposed, taking into account expert assessments of the indicators of the organizational structure and management. The directions for improving the method are shown. It is proposed to take into account the hierarchy of security requirements, use logical rules in expert assessment, on the basis of which an improved model is built. As a result, a hierarchy of private indicators is built based on their verbal formulations, data are modeled and an assessment of the level of information security is performed using the proposed approaches. The practical value of the work consists in the possibility of improving the internal audit activities of the banking system entities on its basis to ensure a sufficient level of security of critical information infrastructure objects.

Keywords: ensuring information security, security requirements indicators, objects protection level, banking system organization, conformity assessment methodology, critical information infrastructure.

Acknowledgements: The article was prepared based on the results of research carried out at the expense of budgetary funds under a state assignment for the Financial University.

For citation: Zhuravlyova M.G., Surova N.Yu., Khasanova Z.R. Modeling the security of critical information infrastructure of the financial sector based on organizational structure and management data. *Modeling, Optimization and Information Technology*. 2025;13(4). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=2046 DOI: 10.26102/2310-6018/2025.51.4.008

Введение

Банковская система включает большую часть субъектов финансового сектора (организаций), которые реализуют в числе прочего функции отдельных аналогичных субъектов, таких как участники платежных систем и рынка ценных бумаг. Задача исследования возможностей обеспечения информационной безопасности (ИБ) на достаточном уровне объектов критической информационной инфраструктуры (КИИ) в организациях банковской системы является весьма актуальной.

В качестве объектов КИИ организаций банковской системы рассматриваются элементы иерархии используемых аппаратно-программных средств (линии связи, аппаратные средства, сетевые оборудование, приложения и сервисы, операционные системы, системы управления базами данных, банковские приложения), а также банковские технологические процессы и бизнес-процессы организации. Инструментами их защиты являются аппаратно-программные компоненты, алгоритмы, методы и модели, позволяющие обнаруживать и поддерживать обеспечение защиты объектов КИИ, в частности, методы интеллектуальной поддержки [1], алгоритмы и методы обнаружения угроз [2, 3], модели для анализа угроз и уязвимостей, использующие методы машинного обучения [4, 5], проактивной защиты [6]. Система обеспечения ИБ включает комплекс защитных мер, средств и процессов эксплуатации, а также систему менеджмента ИБ в виде процессов, непосредственно связанных с реализацией и управлением ИБ. Группы всех рассматриваемых в данном контексте процессов подлежат организации в виде цикла У. Шухарта-У.Э. Деминга [7], применяемого как модель непрерывного улучшения процессов в процессном подходе при реализации систем менеджмента качества: планирование, реализация, проверка (изучение), улучшение, планирование и т. д. Международный стандарт ISO/IEC 27001 определяет планирование как разработку действий по обработке рисков и реализации возможностей, постановку целей ИБ и способов их достижения, реализацию – как оперативное планирование необходимых процессов ИБ и управление ими, оценку и обработку рисков, проверку (изучение) – как

постоянный контроль и измерение упомянутых процессов, в том числе мониторинг, измерение, анализ, самооценку (внутренний аудит) и внешний аудит, а улучшение – как выполнение действий по непрерывному улучшению их показателей.

Алгоритмы обнаружения нарушений безопасности, модели угроз и уязвимостей, построенные по данным о всевозможных атаках на аппаратном и программном уровнях, попытках автоматического проникновения, могут иметь высокую точность предсказания и способствовать поддержанию должного уровня ИБ, но решающее значение на практике часто имеет человеческий фактор. Поэтому процессы организации службы ИБ, распределения ролей и полномочий, обучения персонала, готовности средств и процедур реагирования на инциденты необходимо детально прорабатывать и непрерывно улучшать. Это может быть реализовано в рамках этапа проверки (изучения), который носит исследовательский характер и предполагает разработку и совершенствование методов, связанных с изучением уровня защищенности.

Положения по обеспечению информационной безопасности (ИБ) и измерению уровня соответствия ИБ требованиям, непосредственно влияющим на уровень защищенности, в банковской системе РФ устанавливает стандарт СТО БР ИББС-1.0-2014[1]. В [8] предложена модель аудита, нацеленная в большей степени на реализацию требований международных стандартов по обеспечению ИБ. В [9] рассматривается методика оценки рисков, учитывающая вероятности осуществления всех возможных угроз, которые оценивают эксперты, но достаточно сложная для реализации без использования специальных программных средств. Предложенный в [10] подход к контролю защищенности информации объектов КИИ может рассматриваться как общая стратегия обеспечения ИБ, однако для анализа влияния отдельных факторов, связанных с ИБ, на уровень защищенности в субъектах банковской системы требуется более детальная методика. Если внутренний аудит организации банковской системы проводится на основе стандарта СТО БР ИББС-1.0-2014, применяется методика оценки соответствия ИБ, представленная в стандарте СТО БР ИББС-1.2-2014[2]. Она основана на усреднении значений показателей, оценивающих требования к обеспечению безопасности, выборе минимальных значений, проста для практической реализации службой ИБ организаций. Представляет интерес использование данной методики в качестве основы для оценки влияния отдельных групп факторов, в частности, организационных и управленческих, на уровень защищенности объектов КИИ.

Материалы и методы

Можно выделить следующие основные факторы системы обеспечения ИБ, относящиеся к структуре организации и управления в организациях банковской системы:

– иерархия управления;
– распределение ролей и полномочий;
– наличие службы ИБ;
– наличие процессов реагирования на инциденты;
– уровень подготовки персонала.

[1] СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации: Общие положения: стандарт Банка России: издание официальное: принят и введен в действие Распоряжением Банка России от 17 мая 2014 года № Р-399: дата введения 2014-06-01. – Москва; 2014. – 44 с.

[2] СТО БР ИББС-1.2-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации: Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014: стандарт Банка России издание официальное: принят и введен в действие Распоряжением Банка России от 17 мая 2014 года № Р-399: дата введения 2014-06-01. – Москва; 2014. – 101 с.

Цель предлагаемого подхода состоит в построении модели для оценки уровня ИБ на основе перечисленных факторов и выбора ключевых элементов, составляющих данные факторы.

Рассматриваемая методика СТО БР ИББС-1.2-2014 описывает порядок вычисления уровня ИБ для проведения самооценки организации банковской системы на основании групповых и частных показателей, соответствующих данным требованиям, а также критерии для их экспертной оценки.

Введем обозначения. Пусть имеется множество из p вербально заданных организационных и управленческих факторов s_i:

$$S = \{s_i\},\ i = 1, \ldots, p,$$

множество групповых показателей m_j общим количеством n:

$$M = \{m_j\},\ j = 1, \ldots, n,$$

множество частных показателей q_{jh}:

$$Q = \{q_{jh}\},\ j = 1, \ldots, n,\ h = 1, \ldots, r_j,$$

где r_j – количество частных показателей для группового показателя m_j.

Имеются также результирующие коэффициенты EV_1, EV_2, EV_3, R. Они соответствуют текущему уровню ИБ (EV_1), менеджменту ИБ (EV_2), уровню осознания ИБ (EV_3) и результирующему уровню соответствия ИБ требованиям стандарта СТО БР ИББС-1.0-2014 (R), который с позиций проведения самооценки определяет уровень защищенности объектов КИИ организаций банковской системы.

Результаты анализа требований к системам ИБ и менеджмента ИБ, групповых и частных показателей на предмет их соответствия перечисленным факторам представлены в Таблице 1.

Таблица 1 – Сопоставление элементов структуры организации и управления, требований к обеспечению ИБ и показателей для оценки уровня ИБ
Table 1 – Comparison of organizational and management structure elements, information security requirements, and indicators for assessing the level of information security

№ п/п	Фактор	Требования к …	Частные показатели
1	s_1 – иерархия управления	службе ИБ, ее структуре, независимости	Все частные показатели из группы m_{11} (M11)
2	s_2 – распределение ролей и полномочий	назначению и распределению ролей, обеспечению доверия к персоналу, в том числе полномочий, ролей и/или ответственных за выполнение ролей – по всем областям ИБ	m_1 (M1), $q_{7\,3}$ (M7.3), $q_{9\,38}$ - $q_{9\,40}$ (M9.38-M9.40), $q_{9\,42}$ (M9.42), $q_{9\,59}$ - $q_{9\,60}$ (M9.59-M9.60), m_{11} (M11), $q_{12\,6}$ (M12.6), $q_{13\,10}$ (M13.10), $q_{13\,11}$ (M13.11), $q_{14\,6}$ (M14.6), $q_{15\,22}$ (M15.22), $q_{16\,4}$ (M16.4), $q_{17\,3}$ (M17.3), $q_{17\,4}$ (M17.4), $q_{18\,7}$ (M18.7), $q_{18\,8}$ (M18.8), $q_{19\,7}$ (M19.7), $q_{19\,8}$ (M19.8), $q_{20\,12}$ (M20.12), $q_{20\,13}$ (M20.13), $q_{21\,5}$ (M21.5), $q_{21\,6}$ (M21.6), $q_{22\,9}$ (M22.9), $q_{22\,10}$ (M22.10), $q_{23\,8}$ (M23.8), $q_{23\,9}$ (M23.9), $q_{24\,7}$ (M24.7), $q_{24\,8}$ (M24.8), $q_{25\,8}$ (M25.8), $q_{25\,9}$ (M25.9), $q_{26\,8}$ (M26.8), $q_{27\,1}$ (M27.1)

Таблица 1 (продолжение)
Table 1 (continued)

3	s_3 – наличие ИБ	службе ИБ (ее наличию)	$q_{11\,1}$ (М11.1)
4	s_4 – наличие процессов реагирования на инциденты	обнаружению и реагированию на инциденты; обеспечению непрерывности бизнеса, его восстановлению после прерывания	Все частные показатели, относящиеся к групповым: m_{19} (М19), m_{20} (М20), m_{21} (М21)
5	s_5 – уровень подготовки персонала	реализации программ по обучению и повышению осведомленности в области ИБ	Все частные показатели, относящиеся к групповому m_{18} (М18), а также $q_{20\,11}$ (М20.11), $q_{1\,20}$ (М1.20), $q_{9\,42}$ (М9.42)

Примечание: частные показатели здесь и далее представлены в обозначениях, введенных выше; в скобках указаны их исходные обозначения.

Основные частные показатели по каждому фактору организационной структуры и управления, предназначенные для оценки соответствующих требований, перечислены в четвертом столбце данной таблицы. При ее формировании учитывались лишь обязательные показатели. Помимо выбранных частных показателей, в результирующую модель необходимо включить непосредственно связанные с ними аналоги. Соответствующее сопоставление представлено в Таблице 2.

Таблица 2 – Аналоги частных показателей организационной структуры и управления
Table 2 – Analogues of private indicators of organizational structure and management

№ п/п	1	2	3	4	5	6	7
Выбранные частные показатели	$q_{11\,1} - q_{11\,13}$	$q_{11\,15}$	$q_{16\,4}$	$q_{12\,6}$	$q_{13\,10} - q_{13\,11}$	$q_{14\,6}$	$q_{17\,3} - q_{17\,4}$
Аналоги	$q_{28\,1} - q_{28\,13}$	$q_{28\,14}$	$q_{29\,4}$	$q_{30\,3}$	$q_{30\,9} - q_{30\,10}$	$q_{30\,13}$	$q_{30\,27} - q_{30\,28}$
№ п/п	8	9	10	11	12	13	14
Выбранные частные показатели	$q_{18\,1} - q_{18\,2}$	$q_{18\,7} - q_{18\,8}$	$q_{19\,7} - q_{19\,8}$	$q_{20\,3}$	$q_{20\,12}$	$q_{20\,13}$	$q_{21\,5} - q_{21\,6}$
Аналоги	$q_{31\,1} - q_{31\,2}$	$q_{31\,3} - q_{31\,4}$	$q_{31\,5} - q_{31\,6}$	$q_{31\,7}$	$q_{31\,8}$	$q_{31\,9}$	$q_{32\,1} - q_{32\,2}$
№ п/п	15	16	17	18	19	20	
Выбранные частные показатели	$q_{22\,9} - q_{22\,10}$	$q_{23\,8} - q_{23\,9}$	$q_{24\,7} - q_{24\,8}$	$q_{25\,8} - q_{25\,9}$	$q_{26\,8}$	$q_{27\,11}$	
Аналоги	$q_{32\,5} - q_{32\,6}$	$q_{32\,10} - q_{32\,11}$	$q_{32\,12} - q_{32\,13}$	$q_{33\,8} - q_{33\,9}$	$q_{34\,2}$	$q_{34\,4}$	

Каждый из обязательных частных показателей может иметь одну из трех категорий – первую, вторую или третью. Для каждого частного показателя, относящегося к первой категории, проверяется и наличие документации для соответствующего требования, которое он оценивает, и выполнение требования. Для показателей второй категории проверяется лишь наличие документации, а для показателей третьей категории – выполнение соответствующего требования.

Для обязательных частных показателей первой и третьей категории в соответствии с методикой СТО БР ИББС-1.2-2014 устанавливается шкала, учитывающая степень выполнения соответствующих требований с помощью значений: «нет», «частично», «да», а для обязательных показателей второй категории – шкала со

значениями «нет», «да». Для частных показателей первой категории значениям поставлены в соответствии числа от 0 до 1 следующим образом:

– «нет» – 0 (внутренняя документация отсутствует);

– «частично» – 0,25 (есть внутренняя документация есть, требования не выполняются);

– «частично» – 0,5 (есть внутренняя документация, требования выполняются не в полном объеме);

– «частично» – 0,75 (есть внутренняя документация есть, требования выполняются почти в полном объеме);

– «да» – 1 (есть внутренняя документация, требования выполняются целиком).

Для частных показателей второй категории:

– «нет» – 0 (нет внутренней документации);

– «да» – 1 (есть внутренняя документация).

Для частных показателей третьей категории используется сопоставление:

– «нет» – 0 (требования не выполняются);

– «частично» – 0,5 (требования выполняются частично);

– «да» – 1 (требования выполняются целиком).

Таким образом, каждый показатель, в зависимости от категории, может принимать значения из следующих множеств:

– A = {0, 0,25, 0,5, 0,75, 1} – категория 1;

– B = {0, 1} – категория 2;

– C = {0, 0,5, 1} – категория 3.

Если же для частного показателя по каким-то значимым причинам нет оценки, то числовое сопоставление в этом случае не применяется, для такого показателя используется текстовое обозначение «н/о». На практике при выполнении самооценки в организации банковской системы применяется экспертное оценивание значений частных показателей ИБ разных категорий на основе представленных шкал и соответствий вариантов их значений числам, обозначающим степень их результативности.

Так как частные показатели, не представленные в Таблице 1, не являются актуальными для данного исследования, их можно определить как неоцениваемые и в дальнейшем не учитывать. Также не учитываются частные показатели, которые носят необязательный характер (рекомендуемые).

Структуру объектов из введенных множеств, в том числе с учетом выделенных частных показателей, связей между ними, и результирующих коэффициентов EV_1, EV_2, EV_3, R можно представить в виде схемы, изображенной на Рисунке 1.

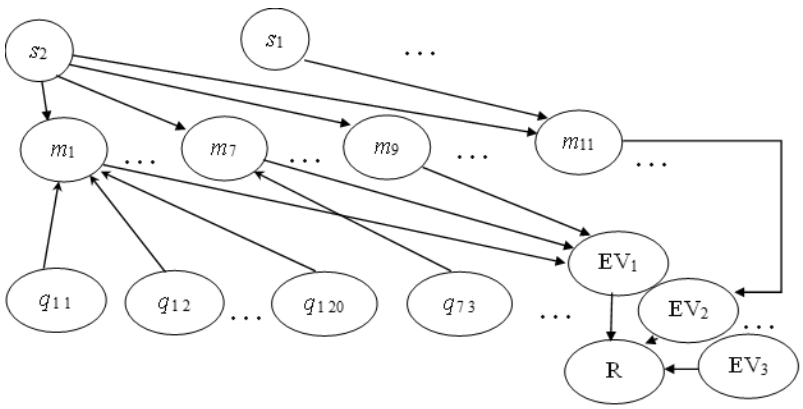

Рисунок 1 – Структура показателей выполнения требований к защищенности
Figure 1 – Indicator structure for security requirements

На схеме (Рисунок 1) показано, что те или иные подмножества групповых показателей m_j относятся к определенным факторам организационной структуры или управления; групповые показатели вычисляются на основе частных показателей q_{jh}, а результирующие коэффициенты, в свою очередь, вычисляются по групповым.

Для построения модели оценки величины R рассмотрим порядок реализации методики СТО БР ИББС-1.2-2014 в контексте учета лишь элементов организационной структуры и управления. Для проведения самооценки и вычисления коэффициента R на первом шаге необходимо провести экспертную оценку значений частных показателей и присвоить им числовые значения в соответствии с категориями. Затем вычисляются значения групповых показателей по формулам:

$$m_j = \begin{cases} 0, q_{jh} = 0 \ \forall h, \\ \frac{1}{r_j}\sum_{h=1}^{r_j} q_{jh}, \text{иначе.} \end{cases} \quad (1)$$

Далее следует вычислить коэффициенты EV_1, EV_2 и EV_3, которые в рассматриваемом случае учитывают только показатели, оценивающие требования к организационной структуре и управлению.

Коэффициент EV_1 вычисляется по формуле (СТО БР ИББС-1.2-2014, стр. 10–11):

$$\mathrm{EV}_1 = \min\left\{k1_1 \frac{(m_1 + m_7)}{2}, k1_2 m_1, k1_3 m_1, k1_4 m_9\right\}, \quad (2)$$

где коэффициенты $k1_1$, $k1_2$, $k1_3$, $k1_4$ в рассматриваемом случае задаются либо равными 1, либо 0,85 – если хотя бы один из частных показателей, соответствующих используемым в (2) групповым показателям, равен 0.

Коэффициент EV_2 вычисляется по формуле:

$$\mathrm{EV}_2 = k2 \ \frac{1}{17}\sum_{j=11}^{27} m_j, \quad (3)$$

где значение $k2$ равно 1, если все частные показатели, соответствующие групповым из (3) являются ненулевыми, 0,85 – если количество нулевых частных показателей из этого множества изменяется от 1 до 25, и 0,7 – если количество нулевых частных показателей превышает 25.

Коэффициент EV_3 вычисляется по формуле:

$$\mathrm{EV}_3 = k3 \ \frac{1}{7}\sum_{j=28}^{34} m_j, \quad (4)$$

где значение $k3$ равно 1, если все частные показатели, соответствующие групповым из (4) являются ненулевыми, 0,85 – если количество нулевых частных показателей из этого множества изменяется от 1 до 10, и 0,7 – если количество нулевых частных показателей превышает 10.

Итоговый коэффициент R, показывающий соответствие ИБ требованиям стандарта, вычисляется как минимальное значение из EV_1, EV_2 и EV_3.

Следующим этапом является выделение ключевых частных показателей. При этом следует учесть, что между частными показателями имеются иерархические связи. Для их выделения нужно проанализировать конкретные вербальные формулировки значений частных показателей и построить соответствующие иерархии.

Частные показатели, входящие в рассмотренную исходную модель, которая учитывает организационные и управленческие факторы, неравномерно влияют на результат. Кроме того, данный вариант построения модели «перемешивает» частные показатели, которые в Таблице 1 привязаны к конкретным факторам организационной структуры и управления. Поэтому имеет смысл построить модель, в которой учтены все факторы и непосредственно связанные с ними частные показатели из Таблицы 1. При ее

построении следует принять во внимание иерархию частных показателей, в том числе в аспекте повышения весов ключевых показателей. В таком случае исходные групповые показатели m_j рассчитываться не будут, вместо них оцениваются вклады факторов в модель.

Рассмотрим улучшенную модель, основанную на экспертных оценках, логических правилах и взвешенных значениях показателей.

Пусть каждому из p организационных и управленческих факторов ставится в соответствие подмножество Q_j частных показателей размером q_j из множества Q:

$Q_j = \{q_{ij}\}$, $|Q_j| = q_j$, $i = 1, \ldots, p$, $j = 1, \ldots, q_j$, где q_j – количество частных показателей для фактора i; для упрощения дальнейшего описания введены новые индексы.

Между показателями из группы, относящейся к конкретному фактору s_i, могут иметь место иерархические связи, задаваемые с помощью матрицы, в первом столбце которой хранятся главные (ключевые) частные показатели, во втором столбце – количества подчиненных показателей, а в оставшихся столбцах – сами подчиненные частные показатели, соответствующие главным. Пример фрагмента такой матрицы (индексы в данном случае соответствуют групповым показателям m_j) выглядит следующим образом:

$$\begin{bmatrix} q_{1\,1} & 9 & q_{1\,2} & \cdots & q_{1\,10} \\ q_{1\,12} & 1 & q_{1\,13} & & \\ q_{1\,14} & 1 & q_{1\,15} & & \\ q_{1\,16} & 1 & q_{1\,17} & & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ q_{21\,1} & 5 & q_{21\,2} & \cdots & q_{21\,6} \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}. \quad (5)$$

В матрице (5) показатель $q_{1\,1}$ является ключевым в группе из десяти показателей ($q_{1\,1}$, $q_{1\,2}$, …, $q_{1\,10}$), показатель $q_{1\,12}$ является ключевым, в группе из двух показателей ($q_{1\,12}$, $q_{1\,13}$) и т.д.

В общем случае рассматривается f множеств категорий, которые может иметь показатель:

$$A_1 = \{a_{11}, a_{12}, \ldots, a_{1l_1}\} – \text{категория 1};$$
$$A_2 = \{a_{21}, a_{22}, \ldots, a_{2l_2}\} – \text{категория 2};$$
$$\ldots$$
$$A_f = \{a_{f1}, a_{f2}, \ldots, a_{fl_f}\} – \text{категория } f,$$

где l_1, l_2, …, l_f – мощности перечисленных множеств, первые значения множеств – $a_{11}, a_{21}, \ldots, a_{f1}$ равны 0 и означают полное невыполнение требований по документированию и реализации мер и процессов, связанных с обеспечением безопасности, последние значения множеств $a_{1l_1}, a_{2l_2}, \ldots, a_{fl_f}$ равны 1 и означают полное выполнение этих требований. Промежуточные значения подразумевают частичное выполнение требований.

Показатели q_{ij} задаются на основании оценок экспертов, которые, исследуя наличие внутренних документов и степени выполнения требований, выбирают для них те или иные значения.

Зададим простые логические правила и алгоритм для поддержки выполнения экспертной оценки значений частных показателей. Пусть q_{it} – некоторый ключевой частный показатель из матрицы вида (5), а $\{q_{it+1}, q_{it+2}, \ldots, q_{it+k\ (k>2)}\}$ – множество подчиненных ему показателей. Если экспертный анализ показал, что его значение равно

0, значит, можно не проверять значения подчиненных показателей, а установить их в 0. В этом случае экспертная система может содержать логические правила вида:

ЕСЛИ q_{it} ЕСТЬ 0, ТО q_{it+1} ЕСТЬ 0 И q_{it+2} ЕСТЬ 0 И… И q_{it+k} ЕСТЬ 0.

Алгоритм поддержки выполнения экспертной оценки содержит следующие шаги:

1. Задать *i, t*; оценить показатель q_{it}. ЕСЛИ показатель q_{it} ключевой – шаг 2, ИНАЧЕ – шаг 3.
2. ЕСЛИ q_{it} ЕСТЬ 0, ТО q_{it+1} ЕСТЬ 0 И q_{it+2} ЕСТЬ 0 И… И q_{it+k} ЕСТЬ 0.
3. ЕСЛИ есть еще показатели для оценки – шаг 1, ИНАЧЕ – шаг 4.
4. Конец алгоритма.

Оценка согласованности мнений экспертов может проводиться на основе коэффициента конкордации[3].

Оценка вклада *i*-го фактора может быть построена на основе средневзвешенных значений показателей. Пусть после экспертной оценки значений показателей с учетом логических правил имеются следующие данные:

- q_{ik} – ненулевой ключевой показатель, $k = k_1, \ldots, k_n$, их количество равно n;
- q_{ij} – ненулевой подчиненный показатель, $j = j_{1\,k}, \ldots, j_{n_k\,k}$, для q_{ik};
- n_k – количество ненулевых показателей, подчиненных q_{ik};
- q_{ih} – ненулевой независимый показатель, $h = h_1, \ldots, h_r$, их количество равно r.

Обозначим через w_{ij} веса всех ненулевых частных показателей с индексами i, j.

Значение вклада *i*-го фактора, $i = 1, 2, \ldots, p$, в модель оценки уровня соответствия ИБ требованиям стандарта СТО БР ИББС-1.0-2014, $\mathrm{E}s_i$, можно вычислить по формуле:

$$\mathrm{E}s_i = \frac{\sum_{k=k_1}^{k_n} w_{ik}q_{ik} + \sum_{k=k_1}^{k_n} \sum_{j=j_{1k}}^{j_{n_k k}} w_{ij}q_{ij} + \sum_{h=h_1}^{h_r} w_{ih}q_{ih}}{\sum_{k=k_1}^{k_n} w_{ik} + \sum_{k=k_1}^{k_n} \sum_{j=j_{1k}}^{j_{n_k k}} w_{ij} + \sum_{h=h_1}^{h_r} w_{ih}}, \quad (6)$$

где второе слагаемое в числителе представляет собой взвешенную сумму всех подчиненных показателей; если обозначить их общее количество через $\sum n_k$, это слагаемое можно записать так:

$$\sum_{j=j_1}^{j_{\sum n_k}} w_{ij}q_{ij},$$

индексы $j_1, j_2, \ldots, j_{\sum n_k}$ являются индексами всех подчиненных показателей.

Для задания весов определим доли весов: $w_1 = 0{,}5$ (50 %) – для ключевых показателей; $w_2 = 0{,}3$ (30 %) – для подчиненных показателей; $w_3 = 0{,}2$ (20 %) – для независимых показателей. Вес каждого ключевого показателя равен w_1/n, вес каждого подчиненного – $w_2/\sum n_k$, вес каждого независимого – w_3/r.

Значения оценок $\mathrm{E}s_i$ при необходимости следует привести к промежутку [0, 1]. Для этого найдем максимальное из них:

$$\mathrm{E}s_{imax} = \max_{i\in\{1,2,\ldots,p\}}(\mathrm{E}s_i).$$

Выполним нормирование:

$$\mathrm{E}s_{inorm} = \frac{\mathrm{E}s_i}{\mathrm{E}s_{imax}}.$$

Результирующее значение R′, характеризующее уровень соответствия ИБ стандарту, можно вычислить как минимальное из всех полученных оценок:

$$\mathrm{R} = \min_{i\in\{1,2,\ldots,p\}}(\mathrm{E}s_{inorm}).$$

[3] Айвазян С.А., Енюков И.С., Мешалкин Л.Д. *Прикладная статистика: исследование зависимостей.* Москва: Финансы и статистика; 1985. 487 с.

Результаты

Проверка возможности практического применения предложенного подхода включает построение рассмотренных моделей на основе моделирования экспертных оценок частных показателей и обнаружения между ними отношений иерархии.

Для выявления ключевых показателей проведен анализ вербальных формулировок рассматриваемых частных показателей, построена иерархия связей между ними. Результаты выбора главных и подчиненных показателей показаны в Таблице 3: если значение главного показателя в результате экспертной оценки оказывается равным нулю, то из формулировок подчиненных показателей следует, что их значения также должны быть нулевыми.

В качестве ключевых показателей организационной структуры и управления выбирается каждый главный частный показатель из первого и третьего столбцов Таблицы 3.

Для получения модели оценки уровня соответствия ИБ требованиям стандарта на основе формул (1)–(4), а также улучшенной модели (6) выполнено моделирование значений частных показателей. Сгенерированы три примера экспертных оценок частных показателей, два из которых содержат близкие к 1 значения, а последний – близкие к 0. Для построения частной модели на основе факторов организационной структуры и управления вычислялись оценки EV_1–EV_3 и R, как описано выше. Для построения улучшенной модели была использована представленная в Таблице 3 иерархия выбранных показателей для вычисления их весов в (6), получены значения Es_i, $i = 1, 2, \ldots, 5$ и R. Нормирование не применялось, так как сумма весов равна 1.

Таблица 3 – Иерархия связей между частными показателями
Table 3 – Hierarchy of relationships between private indicators

Главный частный показатель	Подчиненные частные показатели	Главный частный показатель	Подчиненные частные показатели
$q_{1\,1}$	$q_{1\,2} - q_{1\,10}$	$q_{19\,7}$	$q_{19\,8}$
$q_{1\,12}$	$q_{1\,13}$	$q_{20\,1}$	$q_{20\,4} - q_{20\,5}$
$q_{9\,59}$	$q_{9\,60}$	$q_{20\,2}$	$q_{20\,3} - q_{20\,13}$
$q_{11\,1}$	$q_{11\,2} - q_{11\,15}$	$q_{20\,3}$	$q_{20\,4}$, $q_{20\,7} - q_{20\,10}$
$q_{11\,2}$	$q_{11\,6} - q_{11\,15}$	$q_{20\,12}$	$q_{20\,13}$
$q_{13\,10}$	$q_{13\,11}$	$q_{21\,1}$	$q_{21\,2} - q_{21\,6}$
$q_{17\,3}$	$q_{17\,4}$	$q_{21\,5}$	$q_{21\,6}$
$q_{18\,1}$	$q_{18\,2} - q_{18\,8}$	$q_{22\,9}$	$q_{22\,10}$
$q_{18\,2}$	$q_{18\,3}$	$q_{23\,8}$	$q_{23\,9}$
$q_{18\,7}$	$q_{18\,8}$	$q_{24\,7}$	$q_{24\,8}$
$q_{19\,1}$	$q_{19\,2} - q_{19\,8}$	$q_{25\,8}$	$q_{25\,9}$

Примечание: использованы те же обозначения частных показателей, что и в Таблице 1.

Фрагмент результатов представлен в Таблице 4; значения показателя $q_{27\,1}$ не показаны, они равны 1 во всех примерах; частные показатели, содержащие в обозначении номера 28 и больше (аналоги), не показаны, так как они дублируют соответствующие значения представленных показателей (Таблица 2).

Таблица 4 – Результаты моделирования
Table 4 – Simulation results

q	$q_{1\,1}$	$q_{1\,3}$	$q_{1\,4}$	$q_{1\,5}$	$q_{1\,6}$	$q_{1\,7}$	$q_{1\,8}$	$q_{1\,9}$	$q_{1\,10}$
1	1,00	0,75	1,00	1,00	1,00	1,00	0,75	1,00	1,00
2	0,75	0,75	1,00	1,00	1,00	0,75	0,75	0,75	0,75
3	0,50	0,75	0,00	1,00	0,75	0,75	1,00	0,75	0,25
q	$q_{1\,11}$	$q_{1\,12}$	$q_{1\,13}$	$q_{1\,18}$	$q_{1\,19}$	$q_{1\,20}$	$q_{1\,21}$	$q_{7\,3}$	$q_{9\,38}$
1	1,00	0,75	1,00	1,00	1,00	1,00	0,75	1,00	0,75
2	0,75	0,75	1,00	1,00	1,00	1,00	1,00	0,75	0,75
3	0,50	1,00	0,00	1,00	0,00	0,00	0,25	0,50	0,50
q	$q_{9\,39}$	$q_{9\,40}$	$q_{9\,42}$	$q_{9\,59}$	$q_{9\,60}$	$q_{11\,1}$	$q_{11\,2}$	$q_{11\,3}$	$q_{11\,5}$
1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
2	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
3	1,00	0,50	0,50	0,50	1,00	0,50	0,50	0,50	0,50
q	$q_{11\,6}$	$q_{11\,7}$	$q_{11\,8}$	$q_{11\,9}$	$q_{11\,10}$	$q_{11\,11}$	$q_{11\,12}$	$q_{11\,13}$	$q_{11\,14}$
1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
2	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
3	1,00	1,00	0,50	0,50	0,50	0,50	0,50	0,50	0,50
q	$q_{11\,15}$	$q_{12\,6}$	$q_{13\,10}$	$q_{13\,11}$	$q_{14\,6}$	$q_{15\,22}$	$q_{16\,4}$	$q_{17\,3}$	$q_{17\,4}$
1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
2	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
3	1,00	1,00	1,00	0,50	1,00	1,00	1,00	0,50	0,50
q	$q_{18\,1}$	$q_{18\,2}$	$q_{18\,3}$	$q_{18\,4}$	$q_{18\,5}$	$q_{18\,6}$	$q_{18\,7}$	$q_{18\,8}$	$q_{18\,9}$
1	1,00	0,75	1,00	1,00	1,00	1,00	1,00	1,00	0,75
2	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
3	0,50	0,25	0,00	0,00	1,00	0,50	0,50	1,00	0,75
q	$q_{19\,2}$	$q_{19\,3}$	$q_{19\,4}$	$q_{19\,5}$	$q_{19\,6}$	$q_{19\,7}$	$q_{19\,8}$	$q_{20\,1}$	$q_{20\,2}$
1	0,75	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
2	0,75	1,00	1,00	1,00	1,00	1,00	1,00	0,75	1,00
3	0,50	0,25	0,50	1,00	1,00	1,00	0,50	0,25	1,00
q	$q_{20\,3}$	$q_{20\,4}$	$q_{20\,5}$	$q_{20\,6}$	$q_{20\,7}$	$q_{20\,8}$	$q_{20\,9}$	$q_{20\,10}$	$q_{20\,11}$
1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
2	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
3	1,00	0,50	1,00	1,00	1,00	0,75	1,00	0,50	1,00
q	$q_{20\,12}$	$q_{20\,13}$	$q_{21\,1}$	$q_{21\,2}$	$q_{21\,3}$	$q_{21\,4}$	$q_{21\,5}$	$q_{21\,6}$	$q_{22\,9}$
1	1,00	1,00	1,00	0,75	1,00	1,00	1,00	1,00	1,00
2	1,00	1,00	0,75	1,00	1,00	1,00	1,00	1,00	1,00
3	1,00	1,00	0,25	1,00	0,50	0,50	1,00	0,50	0,50
q	$q_{22\,10}$	$q_{23\,8}$	$q_{23\,9}$	$q_{24\,7}$	$q_{24\,8}$	$q_{25\,8}$	$q_{25\,9}$	$q_{26\,8}$	
1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	
2	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	
3	1,00	0,50	1,00	1,00	0,50	1,00	1,00	0,50	

	EV_1	EV_2	EV_3	R	Es_1	Es_2	Es_3	Es_4	Es_5	R'
1	0,94	0,99	1,00	0,94	0,76	1,00	1,00	0,77	0,99	0,76
2	0,81	0,99	1,00	0,81	0,76	1,00	1,00	0,75	1,00	0,75
3	0,44	0,66	0,80	0,44	0,41	0,79	0,50	0,62	0,49	0,41

Примечания: использованы те же обозначения частных показателей, что и в Таблице 1; q – общее обозначение для списка частных показателей; числа 1, 2, 3 в первом столбце – номера примеров.

Обсуждение

Пример классификации конкретных требований к обеспечению информационной безопасности на основе анализа их содержания представлен в Таблице 3. Рассмотрим, например, групповой показатель m_1, отвечающий за требования, предъявляемые при назначении и распределении ролей и обеспечении доверия к персоналу. Частный показатель $q_{1\,1}$ из Таблицы 3, содержащий вопрос о том, выделены ли роли работников организации банковской системы, непосредственно влияет на группу других показателей, относящихся к данному групповому, содержащих, в частности, вопросы о том, формируются ли роли, связанные с обеспечением ИБ, отсутствуют ли роли, которые совмещают функции разработки и сопровождения программного обеспечения или банковских информационных систем и т. д. Если роли не выделены, то значения подчиненных показателей будут равны 0. Таким образом, показатель q_{11} можно определить как ключевой. Более объективный анализ может проводиться систематически с помощью изучения мнений экспертов из числа работников организаций банковской системы или внешних аудиторов. Возможен автоматизированный подход, предполагающий построение семантической сети на основе вербальных формулировок показателей, что потребует дополнительных ресурсов.

При построении частной модели на основе рассматриваемой методики можно сказать, что для вычисления групповых показателей и отдельных коэффициентов применяется принцип равных влияний – вычисляются простые арифметические средние экспертных оценок показателей. Если определенное количество исходных данных отсутствует, упомянутые средние умножаются на понижающие коэффициенты, причем даже невыполнение одного требования приводит к такому сценарию. При выполнении вычислений, связанных с уровнем ИБ и результирующим уровнем соответствия требованиям к обеспечению ИБ, используется худший случай – выбирается минимальная из сравниваемых оценок. Такая модель может быть использована для дополнительных внутренних проверок. Если необходимо расширить список частных показателей, изменения коснутся формулы (2) для вычисления EV_1.

В Таблице 4 смоделированы 3 примера значений частных показателей, в первом и втором – большая часть их значений близка к 1, а в третьем показан гипотетический вариант неудовлетворительного состояния уровня защищенности объектов КИИ. По результатам, представленным в Таблице 4, можно сделать вывод о том, что на оценку R, вычисленную в соответствии с (1)–(4), в большей степени влияет уровень ИБ (EV_1), так как в контексте учета лишь требований к организационной структуре и управлению, общее количество частных показателей, по которым вычисляется уровень менеджмента ИБ (EV_2), значительно превышает аналогичное для EV_1. Иными словами, в представленных случаях основное влияние на результат оценки соответствия оказывают процессы распределения ролей и полномочий. Если же значения большей части показателей, относящихся к менеджменту ИБ, опустятся ниже 1, то понятно, что при высоком уровне процессов, влияющих на EV_1, результат будет зависеть от уровня менеджмента ИБ.

Если говорить об улучшенной модели, в примерах 1 и 2 из Таблицы 4, более близких к реальной ситуации, факторы Es_1, Es_4, Es_5 сильнее влияют на конечный результат, что корректно отражает структуру требований к обеспечению ИБ. Улучшенная модель в целом позволяет более детально оценить влияние факторов и ужесточает требования к обеспечению безопасности. Использование логических правил, весовых коэффициентов, иерархии требований к обеспечению безопасности создают возможности для полноценной реализации стратегии совершенствования в цикле

Шухарта-Деминга. Посредством корректировки значений весов, полученных на основе некоторой накопленной статистики в организации банковской системы, модель может быть гибко настроена на оценку фактического уровня защищенности объектов КИИ.

Заключение

Цикл Шухарта-Деминга содержит в качестве одного из обязательных этапов непрерывное улучшение, которое относится не только к самой системе обеспечения ИБ в организациях финансового сектора, но и подходам, позволяющим оценивать степень защищенности объектов КИИ. В работе построены и исследованы модели для оценки уровня обеспечения ИБ организаций банковской системы на основе внутреннего аудита, использующие в качестве факторов требования к организационной структуре и управлению, в том числе с применением экспертных оценок, простых логических правил, с учетом иерархии частных показателей оценки требований к обеспечению ИБ. На основе построения иерархии показателей определены ключевые частные организационные и управленческие показатели. Такой подход позволяет оценивать уровень защищенности объектов КИИ банковской системы с помощью внутреннего аудита, является простым, как и предлагаемые стандартами в области обеспечения ИБ методики, полезен для анализа уровня защищенности, учитывающего аспекты организационной структуры и управления в качестве элементов уязвимости в системах обеспечения ИБ, а также может быть распространен без потерь общности на все оцениваемые факторы ИБ и менеджмента ИБ. Дальнейшее исследование в рассматриваемом направлении предполагает построение моделей машинного обучения для решения задач оптимизации управленческих механизмов с целью повышения уровня защищенности объектов КИИ.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Токарев В.Л., Сычугов А.А. Интеллектуальная поддержка обнаружения инцидентов информационной безопасности. *Моделирование, оптимизация и информационные технологии.* 2023;11(1). https://doi.org/10.26102/2310-6018/2023.40.1.006
   Tokarev V.L., Sychugov A.A. Intelligent Support for Detecting Information Security Incidents. *Modeling, Optimization and Information Technology.* 2023;11(1). (In Russ.). https://doi.org/10.26102/2310-6018/2023.40.1.006
2. Милосердов И.В., Малышев В.А. Статистический алгоритм обнаружения угроз компьютерной безопасности. *Моделирование, оптимизация и информационные технологии.* 2020;8(4). https://doi.org/10.26102/2310-6018/2020.31.4.020
   Miloserdov I.V., Malyshev V.A. Statistical Algorithm for Detecting Computer Security Threats. *Modeling, Optimization and Information Technology.* 2020;8(4). (In Russ.). https://doi.org/10.26102/2310-6018/2020.31.4.020
3. Чернов Д.В. Метод количественной оценки опасности реализации угроз безопасности информации объектов критической информационной инфраструктуры потенциальными нарушителями. *Моделирование, оптимизация и информационные технологии.* 2025;13(2). https://doi.org/10.26102/2310-6018/2025.49.2.013
   Chernov D.V. A Method for Quantifying the Danger of Implementing Threats to the Information Security of Objects of Critical Information Infrastructure by Potential Violators. *Modeling, Optimization and Information Technology.* 2025;13(2). (In Russ.). https://doi.org/10.26102/2310-6018/2025.49.2.013

4. Карпухин А.И. Оценка уровня защищенности объектов критической инфраструктуры с использованием машинного обучения и семантического анализа текстового описания угроз и уязвимостей. *Экономика строительства*. 2025;(6):479–482.
Karpukhin A.I. Assessing the Security Level of Critical Infrastructure Facilities Using Machine Learning and Semantic Analysis of Text Descriptions of Threats and Vulnerabilities. *Construction Economics*. 2025;(6):479–482. (In Russ.).
5. Palchevsky E.V., Antonov V.V., Filimonov N.B., et al. Development of a Method for Training a Pulse Neural Network and its Application in a New Approach for Analyzing Network Traffic and Detecting DDos Attacks. [Preprint]. SSRN. URL: https://doi.org/10.2139/ssrn.5009235 [Accessed 16th June 2025].
6. Корчагин С.А., Рубцов Д.Ю., Беспалова Н.В., Сердечный Д.В. Разработка интеллектуальных моделей проактивной защиты критической инфраструктуры финансового сектора на примере информационного обеспечения контрактных систем. *Моделирование, оптимизация и информационные технологии*. 2024;12(4). https://doi.org/10.26102/2310-6018/2024.47.4.005
Korchagin S.A., Rubtsov D.Yu., Bespalova N.V., Serdechny D.V. Development of Intelligent Models for Proactive Protection of Critical Infrastructure of the Financial Sector Using the Example of Information Support for Contract Systems. *Modeling, Optimization and Information Technology*. 2024;12(4). (In Russ.). https://doi.org/10.26102/2310-6018/2024.47.4.005
7. Деминг Э. *Менеджмент нового времени: простые механизмы, ведущие к росту, инновациям и доминированию на рынке.* Москва: Альпина Паблишер; 2022. 184 с.
Deming E. *The New Economics.* Moscow: Alpina Publisher; 2022. 184 p. (In Russ.).
8. Сиротский А.А., Резниченко С.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов. *Безопасность информационных технологий.* 2021;28(3):103–117. https://doi.org/10.26583/bit.2021.3.09
Sirotskiy A.A., Reznichenko S.A. A Formalized Model of an Organization Information Security Audit for Compliance with the Requirements of Standards. *IT Security (Russia).* 2021;28(3):103–117. (In Russ.). https://doi.org/10.26583/bit.2021.3.09
9. Колычев В.Д., Буданов Н.А. Комплексная методика оценки рисков информационной безопасности в коммерческом банке. *Безопасность информационных технологий.* 2021;28(2):83–97. https://doi.org/10.26583/bit.2021.2.08
Kolychev V.D., Budanov N.A. Development of a Comprehensive Methodology for Assessing Information Security Risks in a Commercial Bank. *IT Security (Russia)*. 2021;28(2):83–97. (In Russ.). https://doi.org/10.26583/bit.2021.2.08
10. Бакшеев А.С., Лившиц И.И. Разработка методики контроля уровня защищенности информации объектов критической информационной инфраструктуры. *Вопросы кибербезопасности.* 2023;(2):85–98.
Baksheev A.S., Livshitz I.I. Development of a Methodology for Monitoring the Level of Information Security of Critical Information Infrastructure Objects. *Voprosy kiberbezopasnosti*. 2023;(2):85–98. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Журавлева Марина Гарриевна, кандидат технических наук, доцент Финансового университета при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: magzhuravleva@fa.ru
ORCID: 0009-0002-5576-4377

Marina G. Zhuravlyova, Candidate of Engineering Sciences, Associate Professor of Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Сурова Надежда Юрьевна, кандидат экономических наук, доцент Финансового университета при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: naysurova@fa.ru
ORCID: 0000-0001-7851-4587

Nadezhda Y. Surova, Candidate of Economic Sciences, Associate Professor of Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Хасанова Зиля Рустэмовна, старший преподаватель Финансового университета при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: zrkhasanova@fa.ru
ORCID: 0000-0002-4683-1673

Zilya R. Khasanova, Senior Lecturer of Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Статья поступила в редакцию 15.08.2025; одобрена после рецензирования 15.09.2025; принята к публикации 30.09.2025.

The article was submitted 15.08.2025; approved after reviewing 15.09.2025; accepted for publication 30.09.2025.