



Основные положения методики оценки уровня экономической безопасности цифровых предприятий на основе методологии исследования угроз

Графов Ю.Г., аспирант, ФГБОУ ВО «МИРЭА-РТУ», Москва, Россия

Аннотация. В статье раскрыта важность исследования состояния системы экономической безопасности в условиях цифровизации общественной жизни. На основе монографического подхода был проведен анализ теоретико-методологических аспектов по исследованию угроз экономической безопасности современным предприятиям и предложен авторский метод определения контура угрозы экономической безопасности цифрового предприятий, включающий базовое экспертное исследование трех системообразующих параметров: влияния на цифровую устойчивость, возможность трансформации угрозы в стрессовую ситуацию, а также степень влияния на уровень жизнеспособности системы экономической безопасности предприятия. Был сделан вывод об отсутствии адекватной методики исследования уровня экономической безопасности цифрового предприятия с разграничением перечня работ на каждом аналитическом этапе исследования. Исходя из выделенных инвариант в системе экономической безопасности цифрового предприятия были предложены варианты комплексной их оценки, позволяющих синхронизировать массив данных в единый интегрированный показатель, позволяющий проводить сравнительный анализ цифровых субъектов, функционирующих в одной отрасли.

Ключевые слова: комплексная оценка, методика, метод контура угрозы, угрозы экономической безопасности, цифровое предприятие, цифровая устойчивость, экономическая безопасность, экономическая безопасность цифрового предприятия.

The main provisions of the methodology for assessing the level of economic security of digital enterprises based on the methodology of threat research

Grafov Yu.G., PhD student MIREA-RTU, Moscow, Russia

Annotation. The article reveals the importance of studying the state of the economic security system in the context of digitalization of public life. Based on the monographic approach, an analysis of theoretical and methodological aspects of the study of threats to economic security to modern enterprises was carried out and an author's method for determining the contour of the threat to the economic security of digital enterprises was proposed, including a point-by-point expert study of three system-forming parameters: the impact on digital stability, the possibility of transforming the threat into a stressful situation, as well as the degree of influence on the level of viability of the economic security system enterprises. It was concluded that there is no adequate methodology for studying the level of economic security of a digital enterprise with a delineation of the list of works at each analytical stage of the study. Based on the identified invariants in the system of economic security of a digital enterprise, options for a comprehensive

Key words: comprehensive assessment, methodology, threat contour method, threats to economic security, digital enterprise, digital sustainability, economic security, economic security of a digital enterprise.

Актуальность исследования экономической безопасности (ЭБ) бизнес-субъектов в условиях цифровой экономики определяет повышенный интерес со стороны научного сообщества в части предложения авторских интерпретаций понятийного аппарата, изложения методов и методических аспектов исследования влияния угроз ЭБ на текущее и возможное положение компаний в конкурентной среде, составления прогнозов важнейших квантификаторов, которые сформированы с учетом отраслевой специфики предприятия.

Проняева Л.И. и Федотенкова О.А. предлагают авторский подход для идентификации текущих и возможных угроз ЭБ, инструменты для их детализации и приводят методы, которые позволяют оперативно выявить,

проанализировать и проранжировать угрозы ЭБ, чтобы в дальнейшем выстроить адекватный алгоритм по управлению в системе ЭБ предприятия [6].

В исследованиях представителей Санкт-петербургской школы теории ЭБ-Плотникова А.В., и Харламова А.В., можно ознакомиться с результатами контент-анализа широкого спектра угроз, которые трансформируются в экономические и неэкономические шоки для предприятий реального сектора экономики. Авторы приходят к выводу, что этап выявления угроз является априори важным для поиска соответствующих инструментальных механизмов по управлению угрозами с целью поиска направлений обеспечения устойчивости бизнес-субъектов и планирования возможных последствий [7].

Например, Банк С.В. и Лапаев Д.Н. детально описывают общие методы обеспечения ЭБ от угроз, которые исходят из теневой экономики, а также аккумулируют факторы, на которые субъектам бизнеса необходимо обратить пристальное внимание при формировании своей стратегии в будущем [1].

Деятельность предприятия в цифровой экосистеме приводит к новым, более масштабным и мало прогнозируемым рискам, которые под влиянием факторов, исходящих как внешней, так и из внутренней среды, могут синтезироваться в более масштабные негативные процессы. Причем, отдельные виды рисков, например, риски кибербезопасности, влекут за собой такие последствия для бизнеса, которые могут стать причиной приостановления деятельности компании ввиду технических сбоев работы на сервисах, а также повысить степень уязвимости цифровой инфраструктуры и спровоцировать банкротство предприятия в следствии потери конкурентных преимуществ. Поэтому риски компаний в условиях цифровизации следует в настоящий момент отнести к наиболее важным и фокусировать внимание на них при совершенствовании ЭБ предприятий в части реализации их стратегии, в первоочередном порядке [10].

Рассмотрение имеющейся литературы, посвященной комплексному исследованию современных аспектов обеспечения ЭБ предприятий, позволил сделать вывод о том, что во встречающихся работах в большинстве своем

раскрываются общие вопросы обеспечения экономической безопасности предприятий промышленного сектора экономики, в том числе и за счет наращивания конкурентных преимуществ [5].

Отдельные труды исследователей, под руководством Бабкина А.В., посвящены уточнению терминологического аппарата исследования процессов цифровых преобразований, методическим аспектам «оценки конвергентности цифровой индустриализации и индустриальной цифровизации» с приведением круга потенциальных показателей и их апробации [2].

Многоаспектность проявления угроз в условиях цифровой трансформации предполагает применение новых методов исследования, базирующихся на цифровых технологиях. Например, подробно ознакомиться с методами машинного обучения, которые могут использоваться для решения широкого круга задач обеспечения ЭБ, можно в работах проф. Митякова Е.С. [4].

Цифровые предприятия в силу своих принципиальных отличий от предприятий, реализующих стандартную бизнес-модель, сталкиваются с нетипичными угрозами, которые в большинстве своем изучаются специалистами в сфере информационной безопасности. Однако, на наш взгляд, исследования касаются только отдельных квантификаторов, безопасности ИТ-систем, что в условиях деятельности такого феномена, как «цифровое предприятие» (цп) не учитывает другие ресурсные составляющие. Встречаются исследования, в которых предпринимается попытка некоторых обобщений угроз ЭБцп в весьма суженном формате и, как правило, вариации их экспертной диагностики. В подтверждение данной гипотезы приведем научную статью, подготовленную Кулагиной Н.А., Чепиковой Е.М. и Логачевой Н.А. [3].

Все выше сказанное, позволило автору предложить авторскую классификацию угроз ЭБцп с выделением факторов, которые их провоцируют для последующего фокусирования персонального внимания на круге проблем, решение которых следует предусмотреть в концепции стратегического развития ЦП (табл.1).

Авторская типология угроз ЭБцп и факторы их провоцирующие

Классификационный признак	Разновидности угроз	Факторы-провокаторы угроз
1	2	3
В зависимости от вида применяемых цифровых технологий	Угрозы, связанные с использованием интернета вещей	- рост стоимости оборудования; несовместимость устройств; нарушение конфиденциальности; дисбаланс в защите данных; проблемы с защитой интеллектуальной собственности; несовершенство законодательной базы; дефицит опытных специалистов; экономия топ-менеджмента на системах безопасности; сбои на отдельных этапах разработки ПО; внедрение вредоносного программного обеспечения; внедрение кодов, разработанных для использования уязвимости системы для получения к ней доступа; проведение целевых атак на отдельные компоненты в течение длительного периода времени; проведение DDoS-атак, которые ведутся из разных устройств, но имеют единую цель; использование скомпрометированных устройств, которые трудно отличимые от аналогов; модификация информации для наведения хаоса; проведение атак «человек посередине», при которых хакер перехватывает информацию и заставляет поверить, что две жертвы общаются между собой; подключение к активной сессии, при которой хакер может похитить информацию конфиденциального характера; проведение сетевой разведки с целью получения внутренней информации о состоянии ПО, инновационных разработках, работе на цифровых платформах и т.д.; перехват соединения для передачи данных
	Угрозы, связанные с анализом и использованием больших данных	
	Угрозы, связанные с применением технологий блокчейн	
	Угрозы, связанные с применением нейротехнологий и искусственным интеллектом	
	Угрозы, связанные с применением квантовых технологий	
	Угрозы, связанные с робототехникой и сенсорикой	
	Угрозы, связанные с применением новых производственных технологий	
	Угрозы, связанные с применением технологий беспроводной связи	
	Угрозы, связанные с виртуальной и дополненной реальностью	
В зависимости от умысла	Угроза причинения ущерба с умыслом	- поведение сотрудников, не соответствующее деловым канонам, порой, склоняемых конкурентами или третьими лицами для работы в их пользу, а также поведение сотрудников, которые в силу своей неопытности могут разглашать конфиденциальные требования.
	Угроза, вызванная непреднамеренными действиями лиц	
В зависимости от цели воздействия	Угроза хищения информации	- проведение бизнес-разведки конкурентами; умышленное причинение ущерба ИТ-инфраструктуре компании; подключение третьих лиц к корпоративной сети
	Угроза отключения устройств	- преднамеренно или случайно обеспечения сбоя в сети, в устройствах, невозможность использования средств технической поддержки
	Угроза технического сбоя	- уязвимость ИТ-устройств; ошибки настройки элементов; воровство;
	Угроза кадровому потенциалу	-переманивание специалистов конкурентами; предоставление заведомо ложных сведений о сотрудниках и т.д.
	Угроза деловой репутации	- распространение фейковой информации о компании, продукции, ее сотрудниках.
В зависимости от масштаба последствий	Катастрофические угрозы (свыше 500 тыс.руб.)	Возникновение провоцируют факторы, которые описаны выше
	Критические угрозы (от 200 до 500 тыс.руб.)	

	Средние угрозы (от 50 до 200 тыс.руб.)	
	Незначительные угрозы (до 50 тыс.руб)	
В зависимости от сложности управления	Управляемые	Угрозы, которые возможно устранить или уменьшить их влияние с помощью собственных специалистов. Провоцирующими факторами выступают все выше перечисленные.
	Неуправляемые	Угрозы, которые возможно устранить или уменьшить их влияние с помощью специалистов, которые необходимо привлекать. Провоцирующими факторами выступают все выше перечисленные.
В зависимости от источника возникновения	Внутренние угрозы	Исходят из состояния IT- инфраструктуры, возможности ее постоянного обновления и средств защиты, ресурсного потенциала компании, действий топ-менеджеров
	Внешние угрозы	Исходят из внешней среды цифрового предприятия, которую следует детализировать на макроокружение и среду непосредственного окружения.
В зависимости от природы возникновения	Нормативные угрозы	Несовершенство нормативно-правовой базы для регулирования цифровой деятельности
	Экономические угрозы	Уменьшение финансового бюджета для внедрения цифровых технологий, продвижения конечной цифровой продукции и т.д.
	Технологические угрозы	Снижений инвестиций в НИОКР, в развитие IT-инфраструктуры, обучение сотрудников; непродуманность смены бизнес-модели и т.д.
	Угрозы из системы внутренней культуры предприятия	Отсутствие механизма по привлечению сотрудников компаний в общий процесс управления рисками
	Угрозы экологического характера	Отсутствием специальных площадок и мусорных контейнеров для отработанного оборудования, технических средств, отсутствие программ для их своевременной утилизации или их повторной переработки.
В зависимости от воли и желания человека	Объективные угрозы	- полностью определяются поведением человека
	Субъективные угрозы	- не зависят от поведения человека (например, катастрофы, стихийные бедствия и т.д.)
В зависимости от учета в системе мониторинга предприятия	Учтенные в системе мониторинга компании, в бизнес-планах, цифровых проектах	- связаны с организацией и эффективностью системы стратегического планирования; бюджетированием, применением цифровых технологий для построения аналитической работы на предприятии.
	Хаотично возникшие при реализации цифровых решений	- связаны с просчетом в цифровых решениях, их недоработкой, незнанием текущей ситуации на рынке; невозможностью быстрой адаптации деятельности компании под новые цифровые вызовы

По нашему мнению, для составления архитектуры угроз ЭБцп необходимо использовать методы экспертной оценки, в основу которых заложено проставление баллов по трем взаимосвязанным критериям: влияние на цифровую устойчивость, возможность трансформации угрозы в стрессовую ситуацию и направленность влияния на жизнеспособность системы ЭБцп. При помощи построения аддитивной модели предоставляется возможность

синхронизации проставленных оценок в комплексный показатель, путем перемножения параметров (табл.2)

Таблица 2

Перечень критериев для оценки угроз и рисков ЭБ_{цп}

Влияние на цифровую устойчивость		Возможность трансформации угрозы в стрессовую ситуацию		Направленность влияния на жизнедеятельность системы ЭБ _{цп}	
1	Низкая	1	Отсутствует возможность	1	Низкая
2	Средняя	2	Низкая возможность	2	Средняя
3	Высокая	3	Средняя возможность	3	Высокая
4	Максимальная	4	Высокая возможность	4	Максимальная
Контур угрозы		Диапазоны интегрированной оценки			
		Начало		Окончание	
Катастрофические угрозы		48		64	
Критические угрозы		18		36	
Средние угрозы		8		16	
Незначительные угрозы		1		8	

В свою очередь, сравнение полученного результирующего значения с рекомендуемыми диапазонами позволяет сформировать заключение о состоянии контура угроз и необходимости их последующей детализации на основе приемов детерминированного факторного анализа.

Одним из нерешенных вопросов в настоящий момент времени в теории обеспечения экономической безопасности на микро-уровня, остается отсутствие методики исследования ЭБ_{цп}, с четко выделенными этапами и видами работ, которые требуется выполнить на каждом этапе. Об этом позволил судить круг изучаемых работ по данной предметной области исследования, в частности Руденко М.Н. и Долгановой Я.А. [8].

Поэтому нами был предложен методический инструментарий, который объединяет в себе последовательность аналитических действий, результатом которых является формирование координированной системы мероприятий, целевой направленностью которых выступает обеспечение цифровой устойчивости ЦП к многоаспектным вызовам и угрозам ЭБ (рис.1).

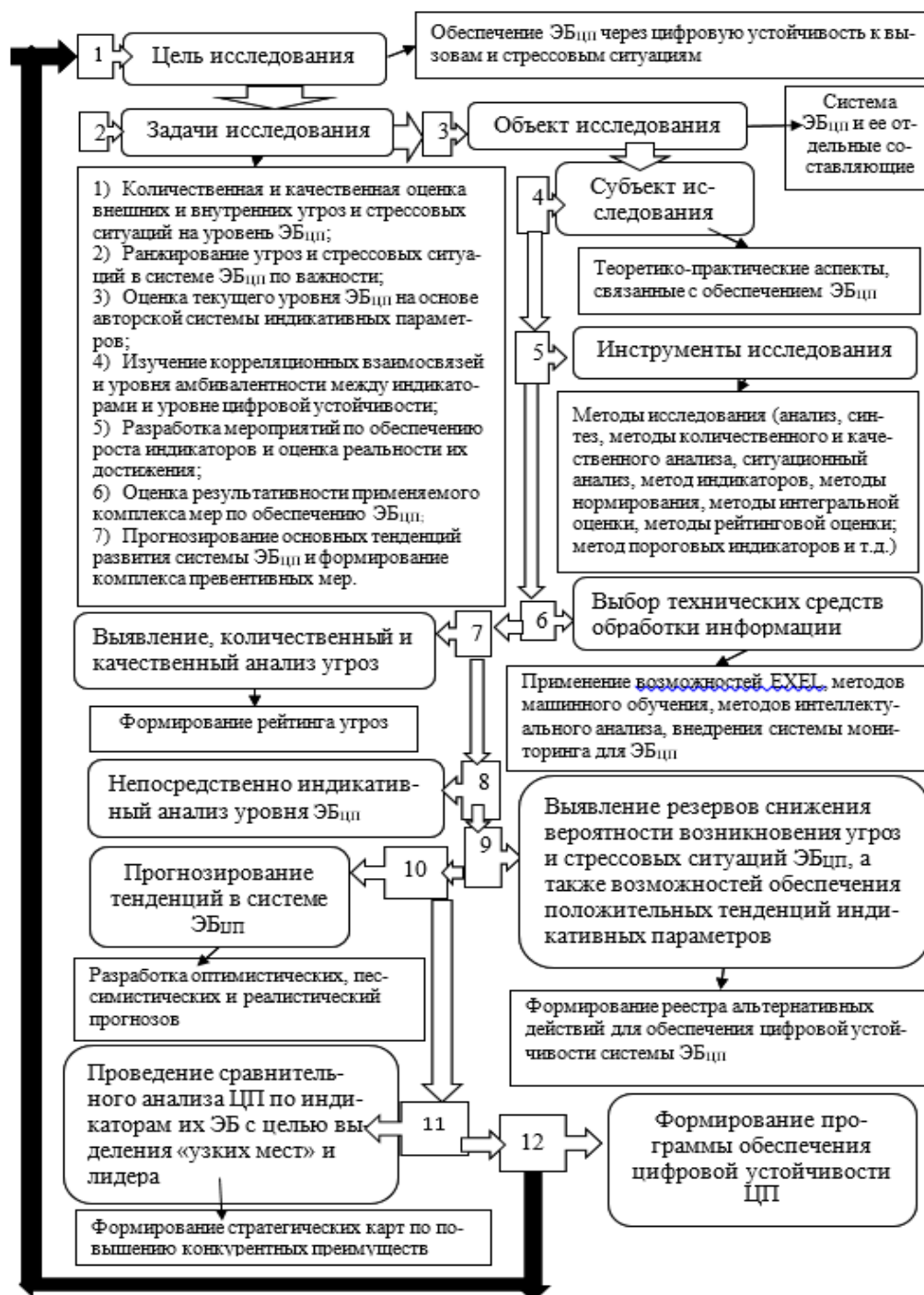


Рис. 1 – Последовательность этапов в авторской методике для оценки уровня ЭБЦП

Особенностью авторского подхода является структурирование системы ЭБЦП на такие инварианты, как информационная, интеллектуальная, финансовая, технологическая и операционная, поэтому уровень цифровой устойчивости, как наилучшее проявление качественного состояния системы ЭБЦП может быть представлено в виде следующей функциональной зависимости:

$$Q_v = f\{ I; O; \int; Y; T \} \rightarrow \max \quad (1)$$

Где I- соответствует качественному состоянию информационной безопасности цифрового предприятия (число индикаторов =4);

O- соответствует качественному состоянию операционной безопасности цифрового предприятия (число индикаторов =6);

$\int$ - соответствует качественному состоянию финансовой безопасности цифрового предприятия (число индикаторов =4);

Y- соответствует качественному состоянию интеллектуальной безопасности цифрового предприятия (число индикаторов =6);

T- соответствует качественному состоянию технологической безопасности цифрового предприятия (число индикаторов =7).

Таким образом, получаем общее число анализируемых индикаторов для комплексной оценки уровня ЭБЦП равное 27.

Для приведения показателей с различными единицами измерения в единую шкалу необходимо воспользоваться процедурой нормирования данных. Комплексная оценка состояния отдельной инварианты определяем, как отношение полученного значения к общему числу входящих параметров для исследования инварианты (например, по интеллектуальной подсистеме это значение будет тождественно 6). Анализ динамики индикаторов для выявления положительных или отрицательных тенденций проводится на основе расчета средней геометрической по темпам роста комплексного значения инвариант по отношению к предыдущему периоду исследования.

Общие методические аспекты по выведению комплексных оценок проиллюстрированы на рис. 2.

По нашему мнению, архитектура построения предложенного методического подхода позволяет получить метрические значения, которые возможно анализировать в динамике, релевантны исходя из интересов стейкхолдеров, конкретизированы для каждой из выделенных инвариант ЦП.

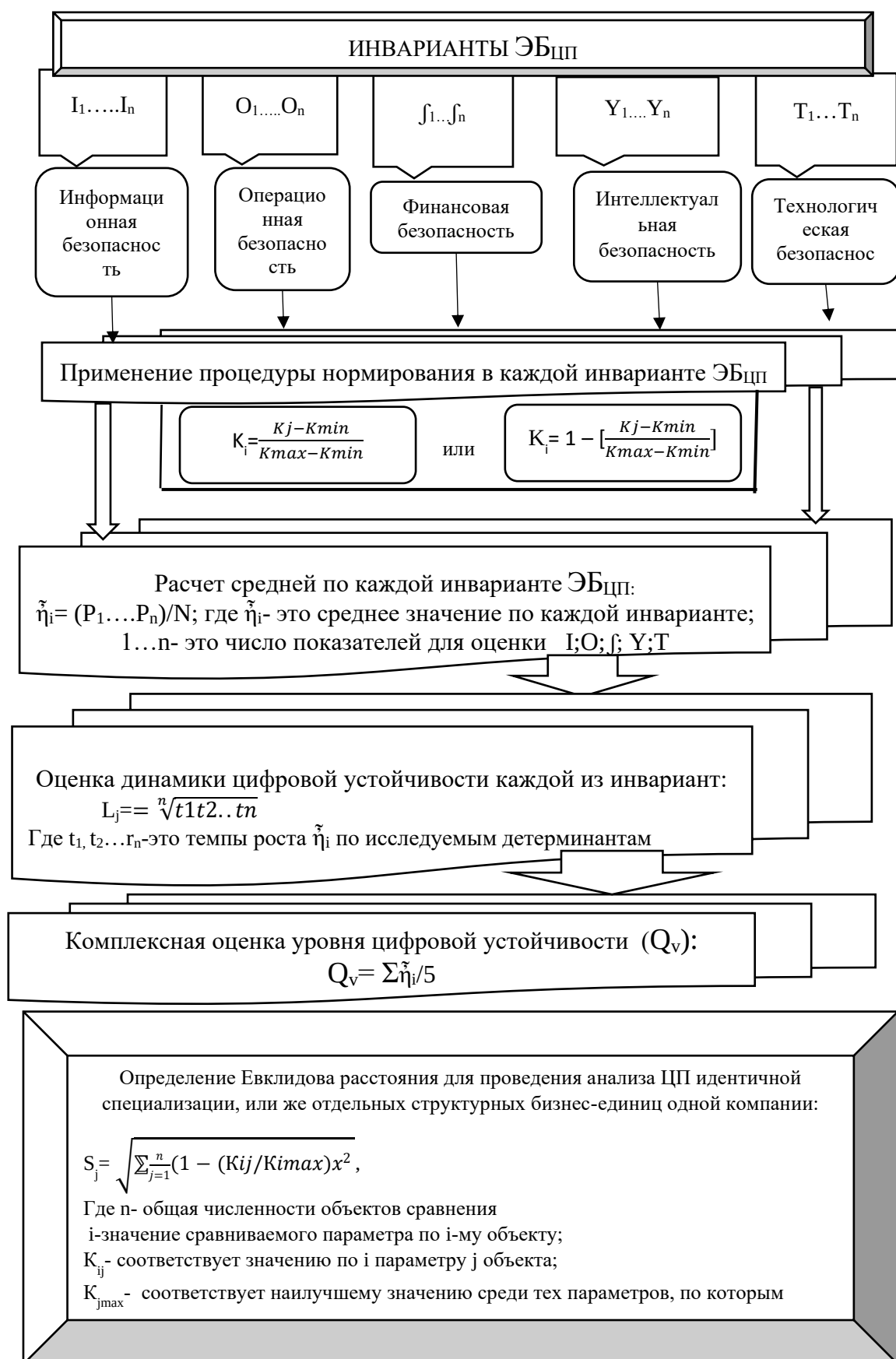


Рис. 2 – Последовательность расчета комплексных оценок для оценки уровня экономической безопасности ЦП и рейтингования объектов

В свою очередь, полученные результирующие интегрированные параметры представляют собой базу для выработки общей концепции обеспечения ЭБЦП, содержащей конкретизированные мероприятия по недопущению угроз и кризисных событий, повышению уровня цифровой устойчивости, что является фундаментом для достижения самодостаточной системы ЭБЦП, для которой свойственна индифферентность и надежность.

Таким образом, результаты, представленные в научной статье, позволяют резюмировать, что предлагаемый авторский методический подход позволяет комплексно исследовать состояние внутренних компонентов системы ЭБЦП, исследовать их тенденции на предмет установления положительных и негативных угроз, количественно оценить угрозы с помощью определения контура их влияния, а также за счет предоставляет широкие возможности для межфирменного анализа с помощью инструментов рейтингования.

Библиографический список:

1. Банк С.В., Лапаев Д.Н., Хусаинов М.К. Методы обеспечения экономической безопасности хозяйствующего субъекта от угроз теневой экономики // *Russian Journal of Management*. – 2024. – Т. 12. – № 1. – С. 380-389.
2. Бабкин А.В., Шкарупета Е.В., Ташенова Л.В. Методика оценки конвергентности цифровой индустриализации и индустриальной цифровизации в условиях индустрии 4.0 и 5.0 // *π-Economy*. 2023. – Т. 16. – № 5. – С. 91-108.
3. Кулагина Н.А., Чепикова Е.М., Логачева Н.А. Систематизация угроз экономической безопасности в условиях цифровой трансформации // *Экономические науки*. – 2021. – № 197. – С. 128-134.
4. Митяков Е.С. Машинное обучение в задачах обеспечения экономической безопасности // *Развитие и безопасность*. – 2020. – № 4 (8). – С. 92-105.
5. Наугольнова И.А., Летунов Е.А. Направления повышения конкурентоспособности промышленного предприятия в эпоху цифровой экономики // *Информатизация в цифровой экономике*. – 2023. – Том 4. – № 3. – С. 295-306.

6. Проняева Л.И., Федотенкова О.А. Идентификация угроз и оценка экономической безопасности предприятий // Национальные интересы: приоритеты и безопасность. – 2019. – № 8. – С. 1479.

7. Плотников А.В., Харламов А.В. Направления нейтрализации негативного влияния неэкономических шоков на реальный сектор экономики России // Известия Санкт-Петербургского государственного экономического университета. – 2023. – № 1 (139). – С. 50-58.

8. Руденко М.Н., Долганова Я.А. Методический подход к оценке экономической безопасности хозяйствующего субъекта в цифровой среде. В книге: Шестая международная конференция «Управление бизнесом в цифровой экономике». Сборник тезисов выступлений. Под общей редакцией И.А. Аренкова и М.К. Ценжарик. Санкт-Петербург, – 2023. – С. 416-423.

9. Савельева Н.К., Макарова М.В. Цифровизация современных компаний: возможности реализации и риски // Креативная экономика. – 2021. – Т. 15. – № 10. – С. 3755-3768.

References:

1. Bank S.V., Lapaev D.N., Khusainov M.K. Methods of Ensuring Economic Security of an Economic Entity from Shadow Economy Threats // Russian Journal of Management. – 2024. – Vol. 12. – № 1. – P. 380-389.

2. Babkin A.V., Shkarupeta E.V., Tashenova L.V. Methodology for Assessing the Convergence of Digital Industrialization and Industrial Digitalization in the Context of Industry 4.0 and 5.0 // π -Economy. 2023. – Vol. 16. – № 5. – P. 91-108.

3. Kulagina N.A., Chepikova E.M., Logacheva N.A. Systematization of Economic Security Threats in the Context of Digital Transformation // Economic Sciences. – 2021. – № 197. – P. 128-134.

4. Mityakov E.S. Machine learning in the tasks of ensuring economic security // Development and security. – 2020. – № 4 (8). – P. 92-105.

5. Naugolnova I.A., Letunov E.A. Directions for increasing the competitiveness of an industrial enterprise in the era of the digital economy // Informatization in the digital economy. – 2023. – Vol. 4. – № 3. – P. 295-306.

6. Pronyaeva L.I., Fedotenkova O.A. Identification of threats and assessment of the economic security of enterprises // National interests: priorities and security. – 2019. – № 8. – P. 1479.

7. Plotnikov A.V., Kharlamov A.V. Directions for Neutralizing the Negative Impact of Non-Economic Shocks on the Real Sector of the Russian Economy // Bulletin of the St. Petersburg State University of Economics. – 2023. – № 1 (139). – P. 50-58.

8. Rudenko M.N., Dolganova Ya.A. Methodological approach to assessing the economic security of an economic entity in the digital environment. In the book: Sixth International Conference «Business Management in the Digital Economy». Collection of abstracts of speeches. General editors I.A. Arenkov and M.K. St. Petersburg, – 2023. – P. 416-423.

9. Savelyeva N.K., Makarova M.V. Digitalization of modern companies: implementation opportunities and risks // Creative Economy. – 2021. – Vol. 15. – №10. – P. 3755-3768.

Для цитирования: Графов Ю.Г., Основные положения методики оценки уровня экономической безопасности цифровых предприятий на основе методологии исследования угроз / Российский экономический интернет-журнал. – 2024. – № 3. URL:

© Графов Ю.Г., Российский экономический интернет-журнал 2024, № 3