УДК 338.2
Научная специальность: 5.2.3
https://elibrary.ru/uuyvdk

Риск-ориентированный подход к оценке информационно-цифровой составляющей экономической безопасности субъектов малого предпринимательства

ISSN 1812-5220

Каранина Е.В.*,
Котанджян А.В.,
Коршунов В.Л.,
Вятский государственный университет,
610000, Россия, г. Киров,
ул. Московская, 36

Аннотация

В рамках настоящей статьи рассматривается понятие информационно-цифровой составляющей экономической безопасности субъекта предпринимательства. Приводятся основные проблемы подсистемы, изменение требований к организации защиты с учетом современных реалий, а также возможности идентификации основных рисков с учетом риск-ориентированного подхода.

Цель исследования: предложение механизма оценки уровня информационно-цифровой составляющей экономической безопасности субъекта малого предпринимательства.

Задачи исследования: определение и интерпретация самого понятия информационно-цифровой подсистемы экономической безопасности, определение факторов угроз, а также обозначение перечня показателей с пороговыми значениями с последующей математической обработкой полученных данных, на примере реально функционирующей компании.

Ключевые слова: экономическая безопасность; информационно-цифровая безопасность; кибератаки; риски; риск-ориентированный подход.

Для цитирования: Каранина Е.В., Котанджян А.В., Коршунов В.Л. Риск-ориентированный подход к оценке информационно-цифровой составляющей экономической безопасности субъектов малого предпринимательства // Проблемы анализа риска. 2025. Т. 22. № 1. С. 34–45. — EDN: UUYVDK

Авторы заявляют об отсутствии конфликта интересов

Risk-Oriented Approach to Assessing the Information and Digital Component of Economic Security of Small Business Entities

Elena V. Karanina*, Asya V. Kotandzhyan , Vyacheslav L. Korshunov,
Vyatka State University, Moscow str., 36, Kirov, 610000, Russia

Abstract
This article examines the concept of the information and digital component of economic security of a business entity. The main problems of the subsystem, changes in the requirements for organizing protection taking into account modern realities, as well as the possibilities of identifying the main risks taking into account the risk-oriented approach are given.
The purpose of this article is to propose a mechanism for assessing the level of the information and digital component of economic security of a small business entity.
The objectives are to define and interpret the very concept of the information and digital subsystem of economic security, to determine threat factors, and to designate a list of indicators with threshold values with subsequent mathematical processing of the obtained data using the example of a real operating company.

Keywords: economic security; information and digital security; cyber-attacks; risks; risk-oriented approach.

For citation: Karanina E.V., Kotandzhyan A.V., Korshunov V.L Risk-oriented approach to assessing the information and digital component of economic security of small business entities // Issues of Risk Analysis. 2025;22(1):34-45. (In Russ.). — EDN: UUYVDK

The authors declare no conflict of interest

Содержание

Введение

В условиях современной экономики, характеризующейся неопределенностью и нестабильностью, деятельность компаний связана с многочисленными рисками, которые могут привести к серьезным последствиям.

Особенно актуальны в настоящее время угрозы, связанные с распространением кибератак на компании и предприятия отечественного рынка. Также идет проседание систем защиты информации и объектов на фоне ухода из страны западных IT-компаний.

С начала 2023 г. наметилась тенденция к усложнению и разнообразию кибератак. Теперь злоумышленники используют трудно обнаруживаемые вредоносные программы, автоматизированные инструменты и даже искусственный интеллект для подготовки атак. Кроме того, они часто применяют многоэтапные стратегии взлома, привлекая для этого доверенных партнеров[1].

По результатам опроса, проведенного компанией «Инфосистемы Джет» организации сталкиваются с множеством проблем и рисков, связанных с информационно-цифровой составляющей, а именно:

- дефицит квалифицированных кадров и управление талантами (нехватка специалистов, трудности с поиском и удержанием профессионалов, отсутствие необходимого опыта);
- трудности в модернизации инфраструктуры информационной безопасности при переходе на оборудование и программное обеспечение от российских производителей (отсутствие альтернативных решений);
- проблемы с поддержанием работоспособности существующих зарубежных решений;
- трудности с выделением финансирования и защитой проектов;
- проблемы в организации и управлении процессами информационной безопасности[2].

Также наблюдается крайне негативная тенденция по увеличению числа утечки информации по вине сотрудников (рис. 1).

Рис. 1. Динамика количества утечек информации по вине сотрудников среди опрошенных компаний[3].

Figure 1. Dynamics of the number of information leaks due to the fault of employees among the surveyed companies

При этом ситуация с внедрением средств информационной защиты стабилизируется: процессы налажены, компании хорошо оснащены и даже масштабируют защиту. Прослеживается влияние новых нормативных требований и повышенного общественного внимания к вопросам защиты данных.

Все это требует предложения определенного подхода к понятию информационно-цифровой составляющей экономической безопасности, а также исследования возможных направлений анализа рисков в этой подсистеме.

1. Понятие и сущность информационно-цифровой составляющей экономической безопасности компаний

В рамках концепции устойчивого развития, которая широко используется в современном мире, под экономической безопасностью понимается равновесие внутренней структуры открытой системы, включающей в себя социально-экономические и экологические аспекты. Это равновесие позволяет системе стабильно функционировать, воспроизводиться и развиваться. Кроме того, важным аспектом является гармоничное взаимодействие системы с окружающей средой [1].

Исследователи изучают экономическую безопасность на разных уровнях экономической системы, но основное внимание уделяется микроуровню. Здесь все еще есть спорные моменты относительно компонентов экономической безопасности [2]. Однако ряд ученых сходится во мнении, определяющем отнесение информационной компоненты или составляющей к одной из подсистем экономической

[1] Итоги года. Годовой отчет Центра информационной безопасности компании «Инфосистемы Джет» // URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf (дата обращения: 15.02.2025).

[2] Итоги года. Годовой отчет Центра информационной безопасности компании «Инфосистемы Джет» // URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf (дата обращения: 15.02.2025).

[3] Исследование уровня информационной безопасности в организациях России. Отчет «СёрчИнформ» // URL: https://ict.moscow/static/pdf/files/godovoe-issledovanie-2023.pdf (дата обращения: 15.02.2025).

безопасности. При этом глобальные процессы цифровой трансформации предъявляют новые требования к обеспечению информационной безопасности компаний, такие как:

- повышение требований к укреплению информационно-цифровой компоненты хозяйствующих субъектов в целях защиты от киберпреступлений;
- следование основным веяниям технологического прорыва;
- «оцифровка» бизнес-процессов;
- развитие и распространение цифровых каналов продаж.

Так, подобные изменения технологического и финансового характера, предопределившие понятие цифровизации экономического сектора, видоизменяют и понятие информационной безопасности добавлением нового компонента — информационно-цифровую составляющую [3].

Сегодня в условиях перехода к цифровой экономике информация стала ценным активом каждой организации. Одной из важных задач в области защиты активов является обеспечение информационной безопасности. Без регулярного мониторинга информационной безопасности невозможно обеспечить стабильное финансовое положение экономических агентов. В то же время неорганизованный подход к обеспечению информационной безопасности может создать риск потери информационных активов и вызвать финансовую нестабильность организации. Поэтому для снижения рисков каждая организация должна создать отлаженную систему безопасности, которая позволит постоянно управлять уровнем информационной безопасности.

Таким образом, под информационно-цифровой составляющей экономической безопасности субъекта предпринимательства понимается достаточный уровень обеспечения общих принципов информационной безопасности наряду с овладением и внедрением цифровых технологий в соответствии с протекающими бизнес-процессами компании, а также обеспечением цифровой гигиены и цифровой грамотности ее сотрудников [3].

Также под информационной безопасностью компании следует понимать комплекс мер и инструментов, направленных на: обеспечение защиты и безопасности информационных ресурсов, обеспечение достоверности и конфиденциальности информации, используемой в экономической деятельности, и на предотвращение угроз, связанных с несанкционированным доступом, хищением, подменой и искажением информации. Эти компоненты включают меры по защите персональных данных, меры информационной безопасности для корпоративных систем и меры кибербезопасности [4].

Укреплению позиций цифровой экономики и обеспечению стабильности и безопасности информационно-цифровой составляющей безопасности представителей бизнеса препятствуют следующие риск-факторы:

- компрометация цифровых данных пользователей — сотрудников и клиентов компании;
- внешние атаки на информационно-цифровую платформу;
- технологические риски обеспечения целостности киберзащиты;
- потеря конкурентных преимуществ в гонке «цифровых вооружений»;
- нехватка квалифицированных кадров в сфере обеспечения информационной безопасности и разработок ИКТ [5].

В рамках информационно-цифровой безопасности компаний можно рассмотреть два основных типа угроз:

1) непреднамеренные — выражаются ошибками в управлении;

2) преднамеренные — незаконное получение информации другими лицами.

Причиненные ущербы от таких рисков способны принести различные последствия:

- подрыв деловой репутации организации;
- раскрытие личных данных отдельных лиц, сопряженное с ущербом для них;
- финансовые потери от разглашения охраняемой (конфиденциальной) информации;
- ущерб, связанный с восстановлением нарушенных информационных ресурсов;
- убытки, возникшие в результате невозможности исполнения обязательств перед третьими сторонами;
- моральный и материальный ущерб от нарушения работы всего предприятия [6].

Немаловажным является выявление источников вышеперечисленных угроз, которые, в свою очередь, подразделяются на две категории: внешние и внутренние (рис. 2).

Рис. 2. Внешние и внутренние угрозы информационной безопасности предприятия

Figure 2. External and internal threats to enterprise information security

Поэтому в условиях, когда информационная составляющая экономической безопасности становится все более важной для всех организаций, системы информационной безопасности должны быть оптимизированы, а их мониторинг и оценка — организованы.

Для эффективной организации информационной безопасности необходим анализ угроз и уязвимостей информационной системы, а также оценка связанных с ними рисков. Только после этого можно приступать к выбору и внедрению соответствующих технических мер защиты [7].

Главной целью создания системы информационной безопасности является обеспечение конфиденциальности, целостности и доступности информации.

К созданию своих систем информационной безопасности все компании подходят по-разному. Некоторые формируют собственные организационные структуры и департаменты, опираясь на свой опыт, другие доверяют защиту информации аутсорсинговым компаниям. В зависимости от сферы деятельности по-разному решаются и проблемы информационной безопасности компании. Для более полного понимания основных принципов построения и поддержки таких систем в российских компаниях рассмотрим методы и способы, которые они применяют для обеспечения информационной безопасности [8].

Максимальная эффективность защиты достигается за счет использования системного подхода. В процессе защиты информационных систем организации принимается ряд мер по предвидению, предотвращению и устранению угроз безопасности.

На практике для обеспечения информационной безопасности используются различные меры. Условно их можно разделить на три группы (рис. 3).

К первой группе относятся материальные средства, представленные оборудованием, техническими устройствами и компьютерной техникой, а также финансовые вложения. Вторая группа обеспечивает нормативно-правовое регулирование процессов,

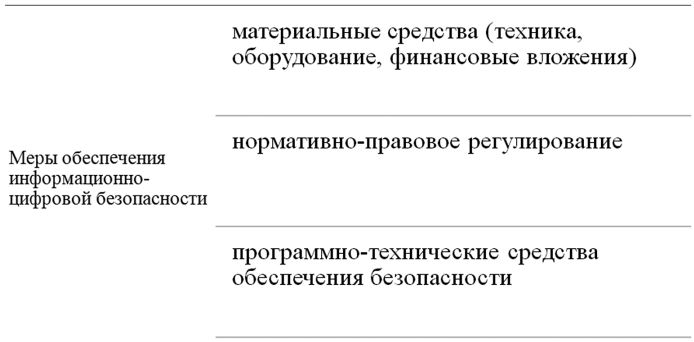

Рис. 3. Направления мер обеспечения информационно-цифровой безопасности

Figure. 3. Areas of measures to ensure information and digital security

связанных с информационной безопасностью. Таким образом, в рамках организации существуют различные документы, например, в виде регистрационных, правоустанавливающих и правоудостоверяющих документов, договоров.

В этом контексте третья группа мер направлена на обеспечение технической поддержки информационной безопасности, с целью обеспечения доступности, целостности и конфиденциальности информации. Эти меры включают в себя использование разнообразных технических средств для защиты таких объектов, как: технические устройства и маршрутизаторы; каналы связи и системы удаленного доступа; серверы; программные средства и софт; базы данных, а также различные методы и способы обеспечения безопасности.

Основные принципы, на которых строится работа систем безопасности, включают:

1. Соответствие мер защиты, осуществляемых системой, актуальным угрозам безопасности, принимая во внимание различные риски и потенциальные уязвимости.

2. Постепенное создание системы с тщательным планированием и определением этапов, чтобы оптимизировать финансовые затраты и при этом сохранить единую концепцию системы.

3. Защита инвестиций путем использования имеющихся средств и систем защиты информации для построения системы, что позволяет снизить затраты на капиталовложения.

4. Централизованное управление и мониторинг системы безопасности для обеспечения более эффективного контроля и реагирования на возможные угрозы.

5. Учет и эффективная интеграция системы безопасности с существующими процессами управления информационными технологиями, чтобы создать более гармоничное и согласованное функционирование всей организации.

Таким образом, эти принципы являются фундаментом для создания надежных и эффективных систем безопасности, которые гарантируют сохранность информации и обеспечивают защиту от возможных угроз. С целью предложения механизма диагностики состояния информационно-цифровой составляющей экономической безопасности компании предполагается ориентироваться на вышеуказанные принципы при разработке показателей, оценивающих уровень безопасности этой подсистемы.

2. Методика оценки уровня информационно-цифровой составляющей экономической безопасности субъекта малого предпринимательства

В настоящее время существует достаточное количество публикаций, отражающих различные аспекты экономической безопасности и, в частности, информационной безопасности (например, физические аспекты защиты, контроль доступа, защита конфиденциальной информации и персональных данных, риск недостоверности информации и его влияние на экономическую безопасность), каждая из которых отражает свой подход к проблеме [7, 9]. Тем не менее, можно отметить, что комплексный подход к анализу и оценке информационной составляющей экономической безопасности в большинстве случаев не применяется. В таких случаях предметом исследования часто становится один из аспектов информационной безопасности.

Существует несколько факторов, которые могут объяснить эту проблему:

1. Методы оценки информационных рисков и угроз недостаточно проработаны в связи с быстро изменяющейся ситуацией в области информационной безопасности и появлением новых технологий.

2. Оценка полученных убытков от реализации рисков и угроз является сложной задачей из-за трудностей прогнозирования всех возможных последствий, включая влияние на репутацию организации.

3. События, связанные с нарушением информационной безопасности, и их последствия часто не являются идентичными и стандартизированными, так как они зависят от конкретных субъектов и объектов информационной безопасности.

4. Получение итогового результата в области информационной безопасности зависит от принятия комплексных решений, поэтому определить конкретные меры, которые максимально повысят уровень информационной безопасности, становится достаточно сложно.

Один из важных этапов разработки системы информационной безопасности организации — это выявление, анализ и оценка рисков информационной безопасности. Верность оценки рисков напрямую влияет на эффективность всей системы информационной безопасности организации.

Если речь идет об оценке информационного компонента экономической безопасности, следует отметить, что показатели информационной безопасности можно разделить на две категории: количественные и стоимостные.

В основе методики лежит сопоставление информационно-цифровых характеристик в виде результата

Рис. 4. Механизм управления и идентификации рисков экономической безопасности компании

Figure 4. Mechanism of management and identification of economic security risks of the company

деятельности компании со среднеотраслевыми показателями (также в учет берутся средние показатели аналогичной подсистемы на региональном уровне). Для построения групповых и интегральных индикаторов оценивания осуществляется перевод показателей типа x в единую балльную характеристику X, измеряемую в шкале от 1 до 100 баллов на основе пороговых уровней безопасности x^l и x^h ($x^l < x^h$) методом кусочно-линейного масштабирования. Так, для показателя x, большее значение которого характеризует более высокий уровень безопасности, т.е. для потенциал-формирующего фактора (или коротко — фактора потенциала) используется следующая формула:

$$\begin{cases} \text{если } x < x^l, \text{то } X = 1, \\ \text{если } x > x^h, \text{то } X = 100, \\ \text{иначе } X = \dfrac{x - x^l}{x^h - x^l} \cdot 99 + 1. \end{cases} \quad (1)$$

Значение оценки в один балл означает очень низкий уровень безопасности (за нижним порогом безопасности x^l), а в 100 баллов — очень высокий уровень безопасности (за верхним порогом безопасности x^h).

Балльная оценка $1 < X < 34$ означает низкий уровень безопасности;

$34 \le X < 67$ — средний уровень безопасности;

$67 \le X < 100$ — высокий уровень безопасности.

Формирование пороговых уровней x^l и x^h осуществляется так, чтобы балльная оценка $X \ge 67$ означала результат не хуже среднего отраслевого (регионального). В этом контексте оценка уровня экономической безопасности фактически представляет собой анализ конкурентоспособности.

Комплексная оценка информационно-цифровой безопасности формируется на основе системы индикаторов безопасности, имеющей иерархическую структуру, интегральная оценка — на основе обобщенной оценки групповых индикаторов.

Для апробации предложенной методики в качестве объекта анализа была выбрана компания Кировской области, являющаяся представителем малого бизнеса региона, функционирующая на рынке более семи лет. Основным видом деятельности компании является «Торговля оптовая писчебумажными и канцелярскими товарами».

Показатели для оценки состояния информационно-цифровой составляющей выбранного объекта были определены путем письменного опроса руководства компании и анализом финансовой отчетности.

Результаты опроса руководства позволили сделать вывод о грамотном построении бизнес-процессов компании и их цифровизации. Наиболее значимые бизнесс-процессы, автоматизированные посредством цифровых платформ представлены на рис. 5.

Исходя из этого, делаем вывод, что основные три направления деятельности компании торговой отрасли: лидогенерация, складской и бухгалтерский учет, а также бизнес-аналитика полностью цифровизированы, бизнес-процессы организованны и прозрачны.

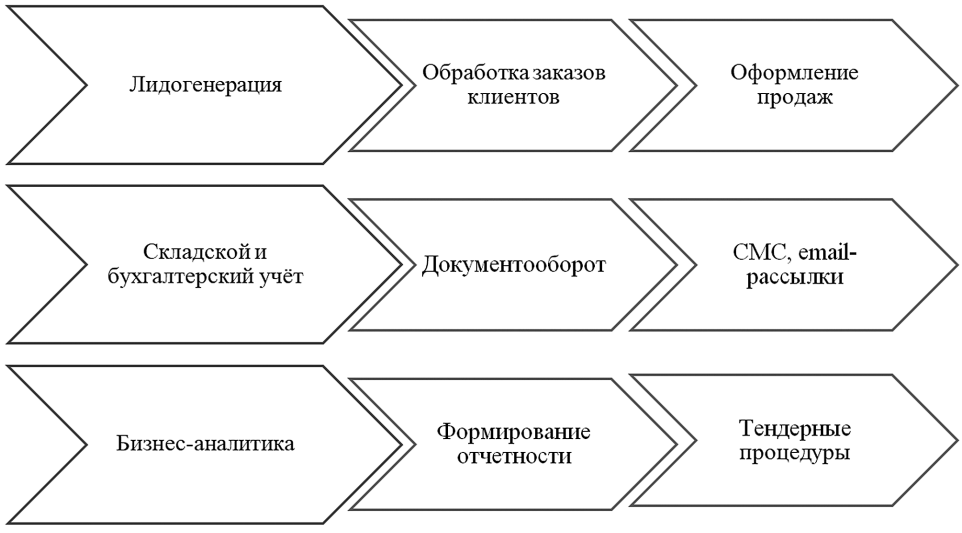

Рис. 5. Направления цифровой трансформации бизнес-процессов рассматриваемой компании

Figure 5. Directions of digital transformation of business processes of the company in question

Тем не менее, одной из уязвимых зон информационно-цифровой подсистемы является отсутствие интегрированной системы, хотя процесс был запланирован на 2025 г.

Оперируя имеющейся информацией о состоянии системы информационной безопасности рассматриваемой компании, представим возможные индикаторы безопасности (табл. 1).

Индикаторы для оценки состояния информационно-цифровой безопасности подразумевают:

1. Темп роста вложений в развитие цифровизации бизнеса отражает изменение расходов на ПО в динамике, где:

$С_{тек.пер.}$ — сумма вложений в программное обеспечение в текущем периоде;

$С_{пред.пер.}$ — сумма вложений в программное обеспечение в предыдущем периоде.

2. Коэффициент цифровизации бизнес-процессов компании определяет степень автоматизации с помощью цифровых технологий бизнес-процессов компании, где:

$Ч_{об.}$ — общее число основных и вспомогательных бизнес-процессов компании;

$Ч_{циф.}$ — число бизнес-процессов, имеющих цифровые решения.

3. Защищенность корпоративных данных подразумевает степень защищенности критической информации компании, где:

$К_{общ.}$ — объем информации, разглашение которой может повлечь негативные последствия для предприятия,%;

$К_{защ.}$ — общий объем защищенной информации.

4. Оценка работы IT-отдела подразумевает анализ качества работы соответствующего персонала, где:

$ЧП_{п}$ — численность работников, непреднамеренные действия которых привели к утечке информации из-за низкого уровня подготовки персонала к распознаванию угроз безопасности, чел.;

$ЧП_{общ.}$ — общая численность работников, имеющих доступ к закрытой информации, чел.

Последующий перевод обозначенных индикаторов рассматриваемой компании в балльные значения при помощи формулы 1 дал следующие результаты (табл. 2).

Таким образом, можно сделать вывод, что на текущий момент информационная подсистема экономической безопасности компании находится на должном уровне защищенности. Вложения в развитие цифровизации бизнеса демонстрировали стабильный рост в 2020–2022 г., в 2023 г. наблюдался рост порядка 2%, что не позволило индикатору выйти в безрисковую зону безопасности. Остальные показатели находились в границах значений, соответствующих высокому уровню безопасности.

Таблица 1. Комплекс индикаторов информационно-цифровой безопасности

Table 1. Set of indicators of information and digital security

Группа показателей	Индикатор	Направление оптимизации	Формула расчета	Пороговые значения x^l и x^h, соответственно
Информационная безопасность	1. Темп роста вложений в развитие цифровизации бизнеса	Максимизация	$\frac{С_{тек.пер.}}{С_{пред.пер.}} \times 100 - 100$	5; 10%
	2. Коэффициент цифровизации бизнес-процессов компании	Расчетная величина	$\frac{Ч_{об.}}{Ч_{циф.}}$	80; 100%
	3. Защищенность корпоративных данных	Максимизация	$\frac{К_{защ.}}{К_{общ.}}$	95; 100%
	4. Оценка работы IT-отдела	Максимизация	$\frac{ЧП_{общ} - ЧП_{п}}{ЧП_{общ}}$	95; 100%

Таблица 2. Интегральная оценка индикаторов информационно-цифровой безопасности компании
Table 2. Integrated assessment of information and digital security indicators of the company

Индикаторы безопасности	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
Интегральная оценка информационной безопасности	75	100	100	100	75
Темп роста вложений в развитие цифровизации бизнеса	1	100	100	100	1
Коэффициент цифровизации бизнес-процессов компании	100	100	100	100	100
Защищенность корпоративных данных	100	100	100	100	100
Оценка работы ИТ-отдела	100	100	100	100	100

Заключение

Экономическая безопасность субъектов малого бизнеса — это определенное состояние защищенности хозяйственной деятельности компании, которое позволяет ему развиваться и сохранять финансовую стабильность, несмотря на негативное влияние внешних и внутренних факторов. Для того чтобы обеспечить подобное состояние, важно своевременно идентифицировать возможные риски, в том числе в контексте обеспечения цифровой трансформации бизнеса.

Представители малого бизнеса сталкиваются с многочисленными угрозами и рисками в процессе ведения своей деятельности. Существует множество методов для классификации рисков и их типов, а также способов их определения. Относительно рисков информационной подсистемы безопасности следует отметить их постоянное видоизменение и преобразование, а увеличение числа кибератак и развитие технологических возможностей злоумышленников, создает высокие требования к организации системы защиты.

Однако для каждого конкретного представителя малых компаний наиболее эффективным подходом к группировке рисков является их разделение по направлениям деятельности, связка показателей на уровне региона и отдельного субъекта.

Исходя из примера предложенного механизма оценки рисков информационно-цифровой составляющей конкретной компании, можно разработать и адаптировать собственный комплекс индикаторов, их пороговых значений и направлений для оптимизации, учитывая специфику бизнеса и потребности региона.

Список источников [References]

1. Быков А. А. О современных угрозах, рисках и возможностях // Проблемы анализа риска. 2024. Т. 21. № 1. С. 8–11 [Bykov A. A. About today's threats, risks, and opportunities // Issues of Risk Analysis. 2024;21(1):8–11. (In Russ.)]
2. Соколов А. П. Управление информационной составляющей в системе экономической безопасности предприятия // Вестник Алтайской академии экономики и права. 2024. № 2–2. С. 267–273. https://doi.org/10.17513/vaael.3271 [Sokolov A. P. Information component management in the system of economic security of the enterprise // Bulletin of the Altai Academy of Economics and Law. 2024;(2–2):267–273. (In Russs.) https://doi.org/10.17513/vaael.3271]
3. Каранина Е. В. Цифровые финансы и экосистемы: обеспечение устойчивого и безопасного развития / Е. В. Каранина, А. В. Котанджян. М: Научная библиотека, 2023. 156 с. EDN JZPWMA [Karanina E. V. Digital Finance and Ecosystems: Ensuring Sustainable and Safe Development / E. V. Karanina, A. V. Kotanjyan. M: Scientific Library, 2023. 156 p. (In Russ.) EDN JZPWMA]
4. Котанджян А. В. Киберугрозы и вызовы цифровой трансформации бизнеса / А. В. Котанджян, Д. С. Лутошкина // Студент. Наука. Регион: сборник материалов III региональной антиконференции, Киров, 23 октября 2024 г. Киров: Издательство «Радуга-ПРЕСС», 2024. С. 105–107 [Kotanjyan A. V. Cyber threats and challenges of digital business transformation / A. V. Kotanjyan, D. S. Lutoshkina // Student. Science. Region: collection of materials from the III regional anti-conference, Kirov, October 23, 2024 Kirov: Raduga-PRESS Publishing House, 2024. P. 105–107. (In Russ.)]

5. Лолаева А. С. Информационная безопасность в свете развития цифровой экономики в Российской Федерации // Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего: сборник статей III Международной научно-практической конференции, Мельбурн, 20 февраля 2021 года Мельбурн: МЦНИР «Научный взгляд», 2021. С. 90–98. EDN MPYDNN [Lolaeva A. S. Information security in the light of the development of the digital economy in the Russian Federation // Interdisciplinary research: past experience, present opportunities, future strategies: collection of articles III of the International Scientific and Practical Conference, Melbourne, February 20, 2021 Melbourne: ICNIR "Scientific view", 2021. P. 90–98. (In Russ.) EDN MPYDNN]
6. Никитин А. В. Информационная составляющая экономической безопасности // Современная наука: прогнозы, факты, тенденции развития: Сборник материалов XV Международной научно-практической конференции, посвященной 60-летию Чебоксарского кооперативного института (филиала) Российского университета кооперации, Чебоксары, 31 января 2022 года. Чебоксары: Чебоксарский кооперативный институт (филиал) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации», 2022. С. 461–467 [Nikitin A. V. Information component of economic security // Modern science: forecasts, facts, development trends: Collection of materials of the XV International Scientific and Practical Conference dedicated to the 60th anniversary of the Cheboksary Cooperative Institute (branch) of the Russian University of Cooperation, Cheboksary, January 31, 2022. Cheboksary: Cheboksary Cooperative Institute (branch) of the autonomous non-profit educational organization of higher education of the Central Union of the Russian Federation "Russian University of Cooperation," 2022. P. 461–467. (In Russ.)]
7. Андреева Д. А., Малинин А. М. Комплексная экономическая безопасность социально-экономических систем в контексте перспектив экономического роста // Технико-технологические проблемы сервиса. 2020. № 2(52). С. 64–69 [Andreeva D. A., Malinin A. M. Integrated economic security of socio-economic systems in the context of economic growth prospects // Technical and Technological Problems of the Service. 2020;(2):64–69. (In Russ.)]
8. Селищев В. А., Чечуга О. В., Наседкин М. Н. Построение системы информационной безопасности предприятия // Известия ТулГУ. Технические науки. 2009. № 1–2. С. 137–144 [Selishchev V. A., Chechuga O. V., Nasedkin M. N. Building an information security system for an enterprise // Izvestia TulSU. Technical sciences. 2009;(1–2):137–144. (In Russ.)]
9. Караулов В. М. Исследование экономической безопасности регионов на основе оценки потенциала и рисков // Проблемы анализа риска. 2023. Т. 20. № 6. С. 10–23. [Karaulov V. M. The study of the economic security of regions based on the assessment of potential and risks // Issues of Risk Analysis. 2023;20(6):10–23. (In Russ.)]
10. Рудакова Т. А., Бондаренко А. С. Инструментарий оценки информационной составляющей экономической безопасности предприятия // Лизинг. 2019. № 6. 47–55 [Rudakova T. A., Bondarenko A. S. Toolkit for assessing information component of economic security of the enterprise // Journal "Leasing". 2019;(6):47–55. (In Russ.)]

Сведения об авторах

Каранина Елена Валерьевна: доктор экономических наук, профессор, заведующий кафедрой финансов и экономической безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Вятский государственный университет» (ВятГУ)
Количество публикаций: более 450
Область научных интересов: экономическая безопасность региона, оценка рисков, резилиенс-диагностика безопасности и устойчивости региональных экосистем
ResearcherID: L-1395-2016
Scopus Author ID: 57192661919
ORCID: 0000-0002-5439-5912
Контактная информация:
Адрес: 610000, г. Киров, ул. Московская, д. 36
Karanina@vyatsu.ru

Котанджян Ася Валентиновна: старший преподаватель кафедры финансов и экономической безопасности Вятского государственного университета (ВятГУ)
Количество публикаций: более 100
Область научных интересов: управление рисками, экономическая безопасность, кадровая составляющая экономической безопасности, информационная безопасность

Scopus Author ID: 57216910073
ORCID: 0000-0002-2043-1356
Контактная информация:
Адрес: 610000, г. Киров, ул. Свободы, д. 122
usr21823@vyatsu.ru

Коршунов Вячеслав Леонидович: аспирант кафедры финансов и экономической безопасности Вятского государственного университета (ВятГУ)

Количество публикаций: более 5
Область научных интересов: стандарты управления рисками и экономической безопасности, информационная безопасность малого бизнеса
ORCID: 0009-0008-1372-6771
Контактная информация:
Адрес: 610000, г. Киров, ул. Свободы, д. 122
usr21823@vyatsu.ru

Статья поступила в редакцию: 27.01.2025
Одобрена после рецензирования: 04.02.2025
Принята к публикации: 05.02.2025
Дата публикации: 28.02.2025

The article was submitted: 27.01.2025
Approved after reviewing: 04.02.2025
Accepted for publication: 05.02.2025
Date of publication: 28.02.2025