DOI 10.31483/r-170321

Киселев Александр Александрович

Кораблева Ольга Николаевна

Городкова Варвара Игоревна

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ВЫБОРУ ИНСТРУМЕНТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННОЙ ОРГАНИЗАЦИИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

Аннотация: *в главе классифицированы специфические технологические, эксплуатационные и вендорские риски, возникающие в процессе миграции на отечественные решения и компоненты с открытым исходным кодом (Open Source), рассматривается проблема обеспечения информационной безопасности (ИБ) российских производственных организаций в условиях вынужденного и ускоренного импортозамещения зарубежных средств защиты информации. На основе анализа ландшафта угроз сформирована матрица принятия решений, позволяющая производственным организациям приоритизировать выбор инструментов ИБ, соблюдая баланс между требованиями регуляторов, непрерывностью бизнес-процессов и экономической эффективностью.*

Ключевые слова: *информационная безопасность, импортозамещение, нормативная база, риск-ориентированный подход, управление рисками.*

Abstract: *this chapter classifies specific technological, operational, and vendor-related risks that arise during the migration to domestic solutions and open-source components. It examines the challenges of ensuring information security (IS) within Russian industrial organizations, given the forced and accelerated import substitution of foreign information security tools. Based on an analysis of the threat landscape, a decision-making matrix has been developed; this matrix enables industrial organizations to prioritize their selection of IS tools while balancing regulatory requirements, business process continuity, and economic efficiency.*

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Keywords: *information security, import substitution, regulatory framework, risk-based approach, risk management.*

Введение. В последние годы все более актуальным становится вопрос о применении в деятельности российских организаций риск-ориентированного подхода, как при проведении надзорных мероприятий, так и при принятии и экспертизе проектных и управленческих решений. Так, исследователи полагают, что такой подход важен в борьбе с серьезными внешними и внутренними угрозами, связанными с замороженными отечественным активами за рубежом, санкциями, коррупционной деятельностью, взяточничеством, финансовым мошенничеством, недовыполнением бюджета, нецелевым использованием денежных средств в рамках национальных и региональных проектов и др. [16]. Кроме того, риск-ориентированный подход обеспечивает оптимальное использование трудовых, материальных и финансовых ресурсов, способствует большей эффективности работы органов контроля и надзора [6]. Как отмечает Я.С. Огородник, современные условия бизнеса характеризуются повышенной нестабильностью и усилением конкуренции, что ведет к увеличению числа и разнообразию рисков, с которыми сталкиваются современные организации. И в данных условиях традиционные системы внутреннего контроля часто оказываются неэффективными перед лицом новых вызовов, требуя более гибкого и адаптивного контроля [17].

Нужно отметить, что первое упоминание о риск-ориентированном подходе на уровне федерального законодательства в России появилось в Федеральном законе от 26 декабря 2008 года №294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», в котором появилась ст. 8.1. «Применение риск-ориентированного подхода при организации государственного контроля (надзора)» [14]. При этом риск-ориентированный подход представляется в отечественном законодательстве, как метод, используемый в различных областях для оценки и устранения рисков, связанных с деятельностью или процессами, включая выявление, определение приоритетов и управление

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

рисками. А в настоящее время уже многим российским организациям предписывается внедрять в свою практическую деятельность риск-ориентированный подход. Так, например, в информационном письме Банка России от 27 декабря 2017 года № ИН-014–12/64 «О вопросах применения рискориентированного подхода в сфере ПОД/ФТ» от 18 января 2018 года отмечалось, что риск-ориентированный подход Банку России нужен «в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма, для разработки финансовых мер по борьбе с «отмыванием» денег», так как именно риск-ориентированный подход позволяет гибко применять предупредительные меры в областях высокого риска [9]. Но у практиков возникают вопросы о том, а как в реальной обстановке, на практике реализовывать обозначенный риск-ориентированный подход в практической деятельности организаций, какие документы разрабатывать, каким образом использовать его, как метод, так как наука еще пока не дала практикам четкого понимания сущности риск-ориентированного подхода для его практической реализации [13].

Однако современные условия обеспечения информационной безопасности (ИБ) деятельности производственных организаций в условиях объявляемых недружественными странами различных экономических и политических санкций против российских организаций, внедрения технологий искусственного интеллекта (ИИ) и необходимости реализации стратегии импортозамещения актуализируют необходимость применения риск-ориентированного подхода к выбору инструментов обеспечения ИБ производственных организаций, так как он помогает обеспечивать оптимальное использование трудовых, материальных и финансовых ресурсов организаций, способствует обеспечению большей эффективности их работы, в том числе в области ИБ. Нужно учитывать, что с 2025 года часть ограничений на использование иностранного ПО и средств защиты информации (СЗИ) уже вступила в силу, с апреля 2026 года уже действуют новые штрафы, с июня 2026 года становится обязательной дорожная карта импортозамещения. Базовый дедлайн перехода значимых объектов КИИ на российские решения будет с 1 января 2028 года, а для ряда специальных сценариев

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

сроки могут сдвигаться до 2031–2036 годов. Однако с учётом реальных сроков аудита, пилотирования, миграции и обучения персонала запас времени ощутимо меньше, чем кажется [8]. Вследствие этого целью данной статьи ставится обоснование риск-ориентированного подхода в роли методологической основы выбора отечественных средств защиты информации в условиях импортозамещения с учетом современных технологических и регуляторных реалий.

В роли объекта исследования рассматривается современная производственная организация, функционирующая в условиях высокой интенсивности и деструктивности цифровых угроз.

Актуальность темы обусловлена тем, что в настоящее время идет резкое увеличение рисков в деятельности производственных организаций, в том числе, киберрисков в области обеспечения ИБ в условиях цифровизации многих производственных процессов и внедрения технологий ИИ и планомерного усиления регуляторного контроля интеграция отечественных средств защиты информации (СЗИ), который перестал быть механической процедурой выбора позиций из реестра Минцифры РФ.

Материал и методы исследования. Основными методами исследования являются включенное наблюдение, мнения специалистов и экспертов по исследуемой тематике, обсуждение проблем на различных конференциях и встречах исследователей с практиками, изучение научных разработок по исследуемой проблематике в интересах определения перспектив разрешения существующих проблем. Так, например, исследование проблем внедрения риск-ориентированного подхода осуществляли Н. Е. Булетова, А. М. Губин и Н. Ю. Романенко [4], Н.А. Казакова и Е.И. Ефремова [10], А.А. Спиридонова и Е.Г. Хомутова [20], Р.В. Колесов [15], А.М. Балтина [2], А.И. Сазонов [19], Л.Н. Орлова [18], С.Е. Титор [21], С.В. Головин [5] и многие др.

Результаты исследования и их обсуждение. В настоящее время на законодательном уровне активно рассматривается важность риск-ориентированного подхода в обеспечении эффективности практической деятельности организаций. Это связано с тем, что, во-первых, он предполагает рациональное распре-

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

деление ресурсов; не «распыляя» ресурсов на тотальные проверки, позволяет осуществлять контроль точечно, лишь там, где риск негативных последствий может быть значительным. Это позволяет освободившиеся ресурсы направлять на цифровизацию процессов или автоматизацию анализа данных и др. Во-вторых, он создает благоприятные условия для развития добросовестного бизнеса, снимая различные бюрократические барьеры в виде излишних проверок и излишних требований. В-третьих, такой подход позволяет своевременно выявлять потенциальные угрозы и своевременно на них реагировать, что меняет парадигму с «реагирования на сбой» на «предотвращение проблемы». При этом, как отмечает С.М. Барышникова, риск-ориентированный подход приобретает динамический характер, поскольку могут меняться со временем, как факторы и условия деятельности подконтрольного лица, так и установленные контролирующим органом критерии отнесения лиц к определенной категории риска или классу опасности [3].

Одновременно исследователи, несмотря на все заявленные достоинства риск-ориентированного подхода, выявляют ряд проблем, возникающих при его практической реализации.

Так, например, С.М. Барышникова отмечает, что одной из наиболее острых является некачественная разработка критериев отнесения объектов контроля к различным категориям риска. Зачастую применяемые показатели не охватывают всю специфику деятельности субъекта. В результате итоговая оценка риска оказывается неполной и может не отражать реальное положение дел. Кроме того, процедура получения статуса объекта с низким уровнем риска во многих случаях чрезмерно усложнена, что снижает её практическую ценность и ставит под сомнение её целесообразность. Важным вопросом остаётся и недостаточная правовая защищённость юридических лиц и индивидуальных предпринимателей при проведении внеплановых проверок [3].

А.А. Спиридонова и Е.Г. Хомутова в статье «риск-ориентированный подход в системе менеджмента качества промышленного предприятия: проблема выбора методов управления рисками» полагают, что при внедрении риск-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

ориентированного подхода на практике организации сталкиваются с трудностью выбора методов оценки риска и на основании этого делают вывод, что для реализации риск-ориентированного подхода в организациях необходимо внедрять в организациях «риск-ориентированное мышление» [20].

В монографии «Методология риск-ориентированного контроля и контроллинга эффективности бизнеса» Н.А. Казакова и Е.И. Ефремова выражают точку зрения, что риск-ориентированный подход касается лишь системы контроля и оценки деятельности организаций, осуществляемой посредством «оценки определенной системой количественных показателей». В связи с отсутствием такой системы, они подчеркивают необходимость рассмотрения «методических аспектов риск-ориентированного внутреннего контроля» [10].

Одновременно некоторые практики и исследователи предполагают, что риск-ориентированный подход позволяет предупредить возможность «ухода от налогов» [23].

И эти проблемы требуют конкретного разрешения с учетом специфики и особенностей деятельности производственных организаций. А появление технологий искусственного интеллекта еще больше актуализируют необходимость решения обозначенных проблем, в том числе для обеспечения их ИБ.

В современных условиях непрерывной цифровой трансформации и обострения геополитических факторов информационные ресурсы окончательно закрепили за собой статус базового стратегического ресурса современных организаций. Главная сложность сегодняшнего дня заключается в том, что привычные алгоритмы создания систем ИБ полностью утратили свою актуальность. На протяжении долгого времени отечественный бизнес базировал свои защитные контуры на международных практиках и стандартах, включая методологии NIST и ISO, а также на глубоком внедрении масштабных технологических сред разработчиков. До введения масштабных санкционных ограничений ИБ-директора оперировали широким спектром иностранных продуктов, что позволяло осуществлять точечную настройку элементов защиты под бизнес-модель конкретной организации. В актуальных реалиях этот инструментарий оказался

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

заблокирован: часть вендоров прекратила операционную деятельность и сервисное обслуживание на территории РФ, другие заблокировали получение патчей безопасности, а легальная пролонгация лицензий или масштабирование оставшихся систем стали невозможными.

Положение дел осложняется глубокой трансформацией среды угроз – интенсификацией целевых кибератак (APT) и активным использованием злоумышленниками генеративного искусственного интеллекта. На этом фоне дефицит привычного софта коренным образом переформатировал принципы обеспечения киберустойчивости. Информационная безопасность сегодня перестала восприниматься как рутинная сервисная функция ИТ-отдела – сегодня она выступает стратегическим фактором выживания и операционной жизнеспособности всей производственной организации. Управление операционными киберрисками вошло в контур глобального корпоративного менеджмента, определяющего непрерывность всех производственных и сервисных цепочек. Вектор развития ИБ сегодня задается жесткой необходимостью форсированной миграции на независимый программно-аппаратный стек и одновременного выполнения строгих требований регуляторов в области защиты персональных данных (ФЗ №152), конфиденциальной информации (ФЗ №98) и безопасности КИИ (ФЗ №187 и сопутствующий приказ ФСТЭК №239). Просчеты на этапе архитектурного планирования и поддержки ИБ-инфраструктуры влекут за собой уже не локальные сбои в сети, а глобальные финансовые потери, деструктивное влияние на репутацию бренда и применение жестких мер административного или уголовного воздействия [11].

В настоящее время в деятельности производственных организаций критически необходим системный подход, предполагающий комплексное внедрение защитных решений на основе глубокого анализа реальных киберрисков – оценки вероятности реализации угроз, уязвимости критических активов и прогнозирования потенциального ущерба для бизнеса. Главной причиной этих изменений стало окончательное введение жестких нормативных барьеров. Так, с 1 января 2026 года в полную силу вступили ограничения, установленные Указом

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Президента РФ №250 от 01.05.2022: применение иностранных средств защиты информации на объектах критической информационной инфраструктуры запрещено [22]. Это только одно из звеньев глубокой трансформации российского рынка информационной безопасности. По исследованиям центра стратегических разработок, за 2025 года объем сегмента средств защиты информации на рынке вырос до 271 млрд. рублей, прибавив 18,1%, но при этом доля иностранных решений всё ещё составляют около 27% установленной базы организаций [24]. Одновременно с этим 1 марта 2026 года вступил в силу Приказ ФСТЭК №117, который нормативно закрепил отказ от декларативного выполнения предписаний в пользу гибкого управления актуальными киберрисками.

Указанные трансформации нормативного поля ставят отечественный бизнес в условия беспрецедентно строгого контроля, который варьируется от категорических табу на использование импортного софта до императивной необходимости выстраивания процессного риск-менеджмента и систематического взаимодействия с надзорными органами. В то же время государственная политика обладает свойством динамической корректировки: директивные сроки миграции пересматриваются с учетом фактических темпов импортозамещения, а правовая чистота использования СЗИ подтверждается многоуровневыми институциональными фильтрами.

Л.Н. Орлова и Д.А. Васильева справедливо отмечают, что важным принципом государственного регулирования также является определение ответственности за работу регуляторов, что проявляется в соблюдении строгой детерминанты «власть = ответственность». Принцип объективной беспристрастности предполагает равенство перед нормами и правилами всех экономических субъектов, при этом сами правила должны быть понятны всем участникам экономических процессов. Также данный принцип определяет оценку справедливости и законности применяемых процедур и правил [18].

Для проектирования жизнеспособной стратегии соответствия новым требованиям ниже приведена структуризация базовых источников права. Это дает

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

возможность сопоставить векторы контроля надзорных органов и сформировать стратегический план развития ИТ-инфраструктуры организации (табл. 1) [1].

Таблица 1

Схема нормативных требований регулирования импортозамещения и безопасности КИИ

Нормативно-правовые ограничения	Указ Президента РФ №166 от 30.03.2022. - Запрет иностранного ПО на значимых объектах КИИ госорганах и заказчиков
	Указ Президента РФ №250 от 01.05.2022 - Полный запрет на СЗИТ из недружественных стран и зарубежные ИБ-услуги
Процессные правила	Приказ ФСТЭК России №117 (в силе с 01.03.2026)
	- Переход от номинального выполнения требований на риск-ориентированную модель
Инструменты контроля	Минцифры (Реестр российского ПО) - Подтверждение отечественного происхождения СЗИ
	ФСТЭК/ФСБ (Сертификация) - Подтверждение реальных защитных свойств СЗИ
Меры ответственности	КоАП РФ (в редакции ФЗ №104-ФЗ
	- Резкое ужесточение штрафов (рост в 2,5–25 раз) и увеличение срока давности по ИБ-нарушениям с 60 дней до 1 года

Таким образом, представленная на схеме нормативная база к 2026 году формирует правила нормативно – правового регулирования в области информационной безопасности. Организации обязаны не просто механически заменить иностранные СЗИ отечественными аналогами (как того требуют Указы №166 и №250), но и выстроить доказуемую, процессно-ориентированную систему защиты в рамках Приказа ФСТЭК №117. Данная модель предполагает, что выбор механизмов защиты жестко привязан к результатам анализа рисков, а их эффективность непрерывно контролируется на основе измеримых показателей. Именно нормативное введение обязательных показателей защищенности трансформирует риск-ориентированный подход из теоретической концепции в прямую юридическую обязанность подконтрольных субъектов [1].

В своей основе данный подход представляет собой методологию управления безопасностью, при которой ресурсы концентрируются на наиболее критичных активах, вероятных угрозах и значимых уязвимостях, а не распределяются равномерно по всей инфраструктуре. Его основополагающий принцип за-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

ключается в том, что защищать необходимо те компоненты, которые критически важны для непрерывности бизнеса, причем в той степени, в какой это экономически и технологически оправдано.

Для перехода от нормативной теории к практике разработан пошаговый алгоритм выбора отечественных СЗИ, увязывающий оценку рисков с финальным внедрением продуктов. При этом в данном алгоритме можно выделить шесть базовых этапов этого процесса: категорирование бизнес-процессов и инвентаризация ИТ-активов; моделирование угроз и расчет величины киберрисков; определение целевого уровня защиты и нормативный комплаенс; подбор и сравнительный анализ отечественных СЗИ; пилотирование и верификация решений; эксплуатация, мониторинг и адаптивный пересмотр (табл. 2).

Таблица 2

Этапы алгоритма риск-ориентированного выбора СЗИ

Ключевое содержание	Отраслевая специфика	Инструменты	Результат
Категорирование бизнес-процессов и инвентаризация ИТ-активов			
Формирование реестра бизнес-процессов с оценкой критичности. Маппинг (сопоставление) процессов с ИТ-инфраструктурой (серверы, СУБД, сети). Оценка ценности данных через потенциальный ущерб (прямой, косвенный, затраты на восстановление)	Критические последствия атак: - пром. сектора: остановка производства, сбой техпроцесса, аварии. - финсектор и услуги: компрометация данных, репутационный ущерб	Оценка ущерба по 3 векторам: - прямой финансовый; - косвенный (отток клиентов); - стоимость восстановления	Реестр критических ИТ-активов с привязкой к бизнес-процессам и оценкой ценности данных
Моделирование угроз и расчет величины киберрисков			
Скрининг актуальных угроз под архитектуру системы. Моделирование специфических рисков миграции (адаптация, совместимость СЗИ, «окно уязвимости»)	Сложности мультивендорности, невозможность автоматизации без бесшовной интеграции	Количественный расчет ALE (годовых потерь)	Реестр рисков включает: - описание, - владельца, - уровень, - вариант обработки, - приоритет внедрения)
Определение целевого уровня защиты и нормативный комплаенс			
Определение соразмерного уровня защиты на основе критичности рисков. Наложение обязательных законодательных требований на риск-	Баланс между реальной защищенностью (соразмерность затрат уровню угрозы) и формальным	Категорирование объектов КИИ. Определение УЗ ПДн. Приказы ФСТЭК России	Техническое задание / Профиль безопасности с целевым набором компенсирующих мер и классов

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

модель	соответствием (комплаенсом.	(базовые наборы мер)	защиты СЗИ
Подбор и сравнительный анализ отечественных СЗИ			
Скрининг рынка СЗИ (NGFW, IDS/IPS, СКЗИ, защита от НСД) по двухэтапной системе фильтрации. Исключение избыточного функционала, не востребованного в инфраструктуре	Отсекающие критерии (обязательные): - актуальная запись в Реестре Минцифры; - действующий сертификат СТЭК/ФСБ; - совместимость с импортонезависимым стеком (Astra, РЕД ОС, Alt)	Сравнительные метрики: - совокупная стоимость владения (TCO); - LA/Параметры техподдержки вендора; - уровень зрелости продукта; - плотность покрытия модели угроз	Сравнительная матрица СЗИ с обоснованием выбора оптимального решения и расчетом TCO
Пилотирование и верификация решений			
- Развертывание выбранных прототипов СЗИ на тестовом стенде. - Проверка функционирования в условиях, максимально приближенных к продуктивным	Участники испытаний: - служба ИБ (техническая проверка); - владельцы бизнес-процессов (проверка влияния на производительность и непрерывность сервисов)	Методика испытаний на реальном или изолированном сегменте инфраструктуры	Протокол испытаний (Тест-репорт) с подтверждением совместимости, эффективности и готовности к внедрению
Эксплуатация, мониторинг и адаптивный пересмотр			
- Перевод СЗИ в промышленную эксплуатацию. - Непрерывный мониторинг эффективности, обновление баз и реагирование на новые уязвимости	Триггеры для актуализации: - изменение ИТ-инфраструктуры; - появление новых векторов атак; - изменение нормативных требований регуляторов; - корректировка бизнес-процессов	Регулярный цикл контроля показателей защищенности в соответствии с Приказом ФСТЭК №117	Актуализированная модель угроз, обновленный реестр рисков и отчетность для регуляторов

Предложенный алгоритм позволяет трансформировать процесс импортозамещения СЗИ из стихийного подбора продуктов в системную, риск-ориентированную процедуру. Интеграция риск-ориентированной аналитики взамен формального выполнения нормативных требований кардинально меняет качество ИБ-инфраструктуры.

Даже с учетом развитого законодательного контура и присутствия на рынке эффективных российских разработок, практическая реализация программ импортозамещения наталкивается на серьезные инженерно-технологические пре-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

пятствия. В отдельных продуктовых сегментах достижение полной технологической независимости в краткосрочной перспективе представляется маловероятным. К подобным дефицитным категориям ИТ-рынка можно отнести программные комплексы для обеспечения безопасности контейнеризированных приложений и экосистем оркестрации (в частности, Kubernetes), платформы класса SOAR, автоматизирующие процессы реагирования на инциденты, а также узкоспециализированный софт для индустриальных систем класса АСУ ТП.

Масштаб данной проблемы наглядно иллюстрируют аналитические отчеты ассоциации «Цифровая энергетика»: на генерирующих мощностях отечественного ТЭК до сих пор функционирует свыше 15 тысяч аппаратных и программных узлов производства недружественных стран. При этом совокупные инвестиции в тотальное обновление инфраструктуры составляют порядка 300–500 млн. рублей в расчете на один энергетический блок [8]. В условиях столь высокой инерционности единственным законным компромиссом остается контролируемая пролонгация эксплуатации импортных защитных систем. Однако это требует обязательного развертывания компенсирующих механизмов безопасности – внедрения систем глубокого сетевого мониторинга, строгой изоляции и сегментации трафика, а также жестких регламентов разграничения прав доступа. Весь комплекс указанных процедур подлежит детальному документированию и официальному согласованию с надзорными ведомствами. При этом О.С. Ерохина доказывает, что применение риск-ориентированного подхода предполагает построение конструктивных моделей управления рисками. Значимым вопросом для применения данного подхода сегодня является вопрос об основаниях отнесения технологий искусственного интеллекта к высокорисковым. При определении уровня риска применения технологии искусственного интеллекта необходимо применять такие критерии, как тип технологии ИИ, сферу ее применения, а также уровень ее потенциальной опасности для окружающей среды, здоровья, других фундаментальных прав граждан [7].

Таким образом, существование технологических разрывов в критических отраслях доказывает, что риск-ориентированный подход сегодня выступает

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

единственным жизнеспособным инструментом ИБ-менеджмента. Он позволяет производствненным организациям отказаться от слепого копирования зарубежных систем и перейти к гибкому планированию компенсирующих и технических мер. Сформулированный в работе алгоритм обеспечивает баланс между жестким нормативным комплаенсом и реальной экономической эффективностью систем защиты в период масштабной технологической трансформации, в том числе внедрения в организациях технологий ИИ.

Выводы.

1. Риск-ориентированный подход в настоящее время рассматривается в соответствии с действующим законодательством в качестве метода, используемого в различных областях деятельности производственных организаций для оценки и устранения рисков, связанных с деятельностью или процессами, включая выявление, определение приоритетов и управление рисками. Он особенно важен в борьбе с серьезными внешними и внутренними угрозами, связанными с замороженными отечественным активами за рубежом, санкциями, коррупционной деятельностью, взяточничеством, финансовым мошенничеством, недовыполнением бюджета, нецелевым использованием денежных средств в рамках национальных и региональных проектов, при котором уровень и интенсивность контрольных мероприятий ставится в зависимость от отнесения субъекта контроля к одному из уровней риска или классов опасности [16].

2. Риск-ориентированный подход предлагает более гибкий и эффективный способ управления рисками по сравнению с традиционными системами внутреннего контроля производственных организаций, сосредоточивая внимание на самых значимых угрозах и особенно киберугрозах. Внедрение риск-ориентированного подхода позволяет организациям улучшить планирование и контроль рисков, создать более эффективные контрольные механизмы, снизить финансовые убытки и повысить устойчивость бизнеса, в том числе, в условиях цифровизации и использования технологий ИИ.

3. Успешная реализация риск-ориентированного подхода требует от производственных организаций четкой идентификации и адекватной оценки рисков,

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

разработки и внедрения эффективных контрольных мер, а также постоянного мониторинга и корректировки системы внутреннего контроля. При этом организации, реализующие риск-ориентированный подход должны быть «вооружены» научными методиками его реализации, например, для отнесения деятельности юридических лиц и (или) используемых ими производственных объектов к определенной категории риска, определенному классу (категории) опасности с учетом специфики деятельности, выделению критических рисков и их оценки для выработки конкретных мероприятий по снижению негативных последствий рисков [12].

4. Применение риск-ориентированного подхода в производственных организациях обеспечит более высокий уровень производственной безопасности без привлечения дополнительных ресурсов контролирующих органов при планировании проверок.

5. Для точного понимания механизмов риск-ориентированного подхода необходимо изучить особенности его применения по отношению к конкретным типам государственного контроля с учетом специфики деятельности производственных организаций.

5. Активная цифровизация производственных процессор в организациях и внедрение технологий ИИ способствуют формированию устойчивой системы риск-ориентированного подхода, адаптированного к современным вызовам, и позволяет организациям улучшать планирование деятельности и контроль рисков, создать более эффективные контрольные механизмы, снижать финансовые убытки и повышать устойчивость бизнеса.

6. Однако успешная реализация риск-ориентированного подхода требует от производственных организаций четкой идентификации и оценки рисков, разработки и внедрения эффективных контрольных мер, а также постоянного мониторинга и корректировки системы внутреннего контроля с использованием технологий ИИ и автоматизированных систем поддержки принятия управленческих решений.

Список литературы

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

1. Анализ рисков и оценка эффективности информационной безопасности. – URL: https://compliance-control.ru/blog/analiz-riskov-i-oczenka-effektivnosti-informaczionnoj-bezopasnosti-metodologii-metriki-i-roi-v-2025–2026/ (дата обращения: 05.10.2026). – Текст : электронный.

2. Балтина, А. М. Реализация риск-ориентированного подхода в управлении государственными финансами / А. М. Балтина // Вестник Академии знаний. – 2023. – № 6 (59). – С. 461–465.

3. Барышникова, С. М. Применение риск-ориентированного подхода в контрольно-надзорной деятельности / С. М. Барышникова // Молодой ученый. – 2025. – № 20 (571). – С. 387–389.

4. Булетова, Н. Е. Применение риск-ориентированного подхода к управлению экономической интеграцией субъектов Российской Федерации в условиях развития цифровой экономики / Н. Е. Булетова, А. М. Губин, Н. Ю. Романенко // Право и цифровая экономика. – 2023. – № 2 (20). – С. 5–13.

5. Головин, С. В. Применение риск-ориентированного подхода в ведомственном контроле финансово-хозяйственной деятельности / С. В. Головин // Финансы. – 2023. – № 5. – С. 53–58.

6. Егельская, Е. В. Аспекты применения риск-ориентированного подхода на опасных производственных объектах / Е. В. Егельская, М. Ю. Романенко // Безопасность техногенных и природных систем. – 2020. – С. 45–49.

7. Ерахтина, О. С. Риск-ориентированный подход к правовому регулированию отношений в сфере разработки и применения технологий искусственного интеллекта / О. С. Ерахтина // Законы России: опыт, анализ, практика. – 2022. – № 10. – С. 101–104.

8. Импортозамещение средств защиты информации: практический план перехода для российских организаций. – URL: https://www.ec-rs.ru/blog/sredstva-zashhity-informacii/importozameshchenie-sredstv-zashchity-informatsii-prakticheskiy-plan-perekhoda-dlya-rossiyskikh-orga/ (дата обращения: 05.10.2026). – Текст : электронный.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

9. О вопросах применения риск-ориентированного подхода в сфере ПОД/ФТ : информационное письмо Банка России от 27 декабря 2017 года № ИН-014–12/64 // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/71751262/ (дата обращения: 05.10.2026). – Текст : электронный.

10. Казакова, Н. А. Методология риск-ориентированного подхода контроля и контроллинга эффективности бизнеса: монография / Н. А. Казакова, Е. И. Ефремова. – 2-е изд., испр. и доп. – Москва : ИНФРА-М, 2021. – 234 с.

11. Кибербезопасность-2026: обзор ключевых классов решений и трендов импортозамещения. – URL: https://www.fa.ru/university/structure/university/uso/press-service/press-releases/kiberbezopasnost-2026-obzor-klyuchevykh-klassov-resheniy-i-trendov-importozameshcheniya (дата обращения: 05.10.2026). – Текст : электронный.

12. Киселев, А. А. Внедрение риск-ориентированного подхода в практику деятельности организаций: проблемы и пути их решения / А. А. Киселев // Право и экономическое развитие: актуальные вопросы: монография / В. Б. Батиевская, М. В. Келехсаева, Т. Е. Ситохова [и др.]; Чувашский государственный институт культуры и искусств. – Чебоксары : Среда, 2023. – С. 78–93.

13. Киселев, А. А. Риск-ориентированный подход как фактор обеспечения конкурентоспособности отечественных организаций / А. А. Киселев // Прогрессивная экономика. – 2023. – № 11. – С. 50–63.

14. Киселев, А. А. Риск-ориентированный подход: проблемы и пути его реализации / А. А. Киселев // Технологии интеллектуального строительства: научно-технический и производственный журнал. – 2024. – № 1. – С. 6–10.

15. Koltsov, R. V. Risk-oriented approach in the activities of organizations: problems of theory and practice for its implementation / R. V. Koltsov, A. A. Kiselev // Journal of regional and international competitiveness. – 2023. – Vol. 4. – P. 28–40.

16. Кононенко, Е. Риск применения риск-ориентированного подхода / Е. Кононенко, Г. Черкасский // Роль технического регулирования и стандартизации в эпоху цифровой экономики : сб. статей участников III Междунар. науч.-

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

практ. конф. молодых ученых (Екатеринбург, 25 ноября 2021 г.). – Екатеринбург : Ажур, 2021. – С. 213–220.

17. Огородник, Я. С. Риск-ориентированный подход как часть системы внутреннего контроля / Я. С. Огородник // Вестник евразийской науки. – 2024. – Т. 16, № 6.

18. Орлова, Л. Н. Применение риск-ориентированного подхода в практике государственного регулирования (на примере электроэнергетического комплекса) / Л. Н. Орлова, Д. А. Васильев // Вестник Алтайской академии экономики и права. – 2020. – № 12–3. – С. 584–592.

19. Сазонов, А. И. Проблемы внедрения риск-ориентированного подхода в деятельности организаций: проблемы теории и практики / А. И. Сазонов, А. А. Киселев // Экономика и предпринимательство. – 2024. – № 5 (166). – С. 964–967.

20. Спиридонова, А. А. Риск-ориентированный подход в системе менеджмента качества промышленного предприятия: проблема выбора методов управления рисками / А. А. Спиридонова, Е. Г. Хомутова // Организатор производства. – 2017. – Т. 2, № 2. – С. 93–94.

21. Титор, С. Е. Риск-ориентированный подход при организации государственного контроля (надзора) в сфере труда: итоги нескольких лет / С. Е. Титор // Вестник Московского университета МВД России. – 2022. – № 3. – С. 262–269.

22. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ : от 01.05.2022 №250. – URL: https://base.garant.ru/404561984/ (дата обращения: 05.10.2026). – Текст : электронный.

23. Что такое риск-ориентированный подход. Объясняем простыми словами. – URL: https://news.rambler.ru/disasters/47507181-chto-takoe-riskorientirovannyy-podhod-obyasnyaem-prostymi-slovami/ (дата обращения: 05.10.2026). – Текст : электронный.

24. Кваша, Е. Рынок информационной безопасности РФ / Е. Кваша, Р. Краснов // Фонд «Центр стратегических разработок» (ЦСР). – 2026. – URL:

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

https://www.csr.ru/upload/iblock/f97/00g0eegv8oocs0o7txx6bkwibcr0atlg.pdf (дата обращения: 05.10.2026). – Текст : электронный.

Киселев Александр Александрович – канд. пед. наук, профессор, профессор института экономики и менеджмента, Почетный работник высшего профессионального образования, ФГБОУ ВО «Ярославский государственный технический университет», Ярославль, Россия

Кораблева Ольга Николаевна – канд. хим. наук, доцент, доцент кафедры «Химическая технология органических веществ, Почетный работник высшего образования, ФГБОУ ВО «Ярославский государственный технический университет», Ярославль, Россия.

Городкова Варвара Игоревна – магистрант 3 курса института экономики и менеджмента, ФГБОУ ВО «Ярославский государственный технический университет», Ярославль, Россия.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)