Электронный научный журнал «Век качества» ISSN 2500-1841 http://www.agequal.ru

2024, №1 http://www.agequal.ru/pdf/2024/AGE_QUALITY_1_2024.pdf

**Ссылка для цитирования этой статьи:**

Кузовкова Т.А., Салютина Т.Ю. Риски цифровой трансформации экономики и общества и инструментарий управления экономической безопасностью бизнеса в цифровой среде // Электронный научный журнал «Век качества». 2024. №1. С. 63-87. Режим доступа: http://www.agequal.ru/pdf/2024/124005.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 338

# Риски цифровой трансформации экономики и общества и инструментарий управления экономической безопасностью бизнеса в цифровой среде

***Кузовкова Татьяна Алексеевна,***
*профессор, доктор экономических наук,*
*профессор кафедры «Цифровая экономика, управление и бизнес-технологии»,*
*Московский технический университет связи и информатики,*
*111024, г. Москва, ул. Авиамоторная, д. 8а*
*t.a.kuzovkova@mtuci.ru*

***Салютина Татьяна Юрьевна,***
*доцент, доктор экономических наук,*
*зав. кафедрой «Цифровая экономика, управление и бизнес-технологии», Московский технический университет связи и информатики,*
*111024, Россия, г. Москва, Авиамоторная ул., дом 8А*
*t.i.salutina@mtuci.ru*

В условиях значительной неопределенности последствий цифрового развития и политической нестабильности мировой экономики актуальны теоретические и практические вопросы экономической безопасности бизнеса, выявления угроз и оценки рисков, совершенствование принципов и компонентов управления безопасностью в цифровой среде. В статье раскрываются влияние цифровой трансформации экономики и социума на экономическую безопасность бизнеса, источники внешних и внутренних угроз, сущность рисков цифровой и информационной безопасности. Особое внимание уделяется рискам цифровой безопасности, обосновываются возможности и риски, а также особенности рисков цифровых технологий. В качестве системного инструментария управления экономической безопасностью бизнеса в цифровой среде предлагается интеграция процессов

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

управления рисками и планирования развития на примере инфокоммуникационного бизнеса.

**Ключевые слова:** экономическая безопасность, риски цифровых технологий, цифровая трансформация экономики, инструментарий управления рисками, интегральная система управления рисками.

## Введение

Во второй половине XX века человечество вступило в эпоху глобальных перемен, перешло к следующей стадии своего развития – информационному обществу, которое основано на превращении информации в приоритетный фактор производства товаров и услуг. Данный переход выражается в кардинальных социально-экономических преобразованиях экономики и общества, политической системы и институтов национальной безопасности, трендов и масштабов цифрового развития, в которых системообразующую и каталитическую роль играют высокотехнологичные инфокоммуникационные и цифровые технологии [1-3].

Цифровое производство товаров и услуг стирает границы предприятий и государств, трансформирует факторы производства, меняет потребительские предпочтения, формируя виртуально-электронную среду потребления. Цифровая экономика характеризуется «изменением изнутри» внешней и внутренней среды как производства, так и потребления. Технологическая особенность развития цифровой экономики состоит в том, что инфокоммуникационные элементы быстро развиваются в традиционных отраслях и становятся квазиинформационным производством внутри неинформационных производств, что обусловливает приоритет информационно-коммуникационных технологий (ИКТ) по сравнению со своими ресурсами [4-5].

Информация и знания являются специфическим ресурсом, обладающим свойством проникновения через все границы и преграды, и поэтому служат проводником процессов глобализации и цифровизации. Границы между отдельными отраслями все более стираются, образуются

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

единые межотраслевые производственно-обслуживающие системы и комплексные отрасли, интегрированные по конечному потреблению. В конечном счете структура экономики приобретает сетевой характер, а ее эффективность – сетевой эффект [6]. Формируемые в результате модернизации экономики «большие данные», наряду с системными технологиями их анализа, становятся одним из ведущих активов государства, бизнеса и гражданского общества. При этом отсутствие физических границ в цифровом пространстве открывает доступ к существенному массиву данных многочисленных участников глобального экономического пространства [4, 7].

Анализ эволюции общемировой экономики показал, что среди факторов, определяющих эффективность и конкурентоспособность современной социально-экономической системы, ведущими становятся информационные ресурсы, знания, большие данные, цифровые платформы, интернет вещей, искусственный интеллект, которые напрямую определяют экономическую безопасность бизнеса [8-9].

## Влияние цифровой трансформации экономики и социума на экономическую безопасность бизнеса

Глобализация политических, экономических, социальных процессов в ходе информатизации обостряет конкуренцию, делает информацию доступной для конкурентов, а субъекты предпринимательской деятельности – более зависимыми и уязвимыми [10-11]. Разнообразие источников внешних и внутренних угроз экономической безопасности бизнеса в условиях цифровой трансформации потребовало их классификации (рис. 1).

К значимым внешним угрозам безопасного бизнеса относятся кризисные явления в мировой экономике и политика санкций, неблагоприятная экономическая политика государства, недобросовестная конкуренция, а также переход к новому технологическому укладу и цифровой

трансформации экономики и общества, создающий новые цифровые угрозы и риски [3-5, 7]. Для эффективной защиты национальной экономики от внешних и внутренних угроз необходимо учитывать происходящие процессы цифрового развития и формирование единого информационного пространства и создавать адекватную систему обеспечения безопасности государства и бизнеса.


Источник: составлено авторами

Рис. 1. Классификация источников внешних и внутренних угроз экономической безопасности бизнеса

В цифровой среде существенно увеличиваются угрозы бизнесу, меняется характер рисков и растет вероятность турбулентности и нестабильности рынка [8-9]. Новые вызовы и угрозы безопасности,

связанные с цифровой трансформацией экономики и общества, многократным ростом объемов передаваемых и обрабатываемых данных, защитой корпоративных и персональных данных, исчезновением ряда профессий и отраслей, региональными диспропорциями, могут сказываться на независимости бизнеса и конкурентоспособности предприятий [10-12].

Поскольку стратегической целью обеспечения устойчивого бизнеса является сбалансированное развитие по трем основным аспектам – экономическому, социальному и экологическому, то современные угрозы можно разделить на три группы (рис. 2).


Источник: составлено авторами

Рис. 2. Классификация рисков и угроз экономической безопасности бизнеса

В зависимости от значимости для достижения целей бизнеса и сложности управления риски организации подразделяют на четыре основные категории:

– ***стратегические риски*** связаны с невозможностью четкой формулировки и/или выполнения успешной бизнес-стратегии, например, по

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

выходу на новые рынки, внедрению новых услуг, новых цифровых платформ, слияниям и поглощениям, применению новых бизнес-моделей, экосистем, а также отказу от оказания невостребованных услуг;

– ***операционные риски*** связаны с недостижением производственных целей, неэффективным использованием трудовых ресурсов, активов, процессов и систем, поддерживающих деятельность;

– ***риски отчетности*** возникают вследствие возникновения искажений в финансовой, управленческой и прочей отчетности, несвоевременного или неполного предоставления информации заинтересованным сторонам;

– ***риски несоответствия*** деятельности компании требованиям общества, инвесторов и акционеров, регулирующих органов, законодательства, применяемых правил и стандартов [3].

## Сущность, угрозы и риски цифровой и информационной безопасности

Применение высокотехнологичных технологий, являющееся фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы и риски [13]. Тренды трансграничности, цифровизации и открытости экономических субъектов делают национальный сегмент экономики более уязвимым для:

1) негативного информационно-технического воздействия со стороны ряда зарубежных стран на инфокоммуникационную инфраструктуру экономики в политических, экономических и военных целях, а также снижения конкурентоспособности отечественных производителей;

2) информационно-технической разведки в отношении государственных, национальных коммерческих, научных организаций и предприятий оборонно-промышленного комплекса;

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

3) информационно-психологического воздействия на экономические субъекты посредством манипулирования спросом и предложением экономики, биржевыми котировками.

Возрастают масштабы компьютерной преступности, особенно в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека при обработке персональных данных с использованием ИКТ. Человек становится полностью уязвимым перед глобальными платформами, получающими полный доступ к персональной информации. Повышается сложность и увеличиваются масштаб и количество скоординированных компьютерных атак на объекты критической информационной инфраструктуры. Данные риски увеличиваются с распространением искусственного интеллекта и индустриального интернета [8-9, 13].

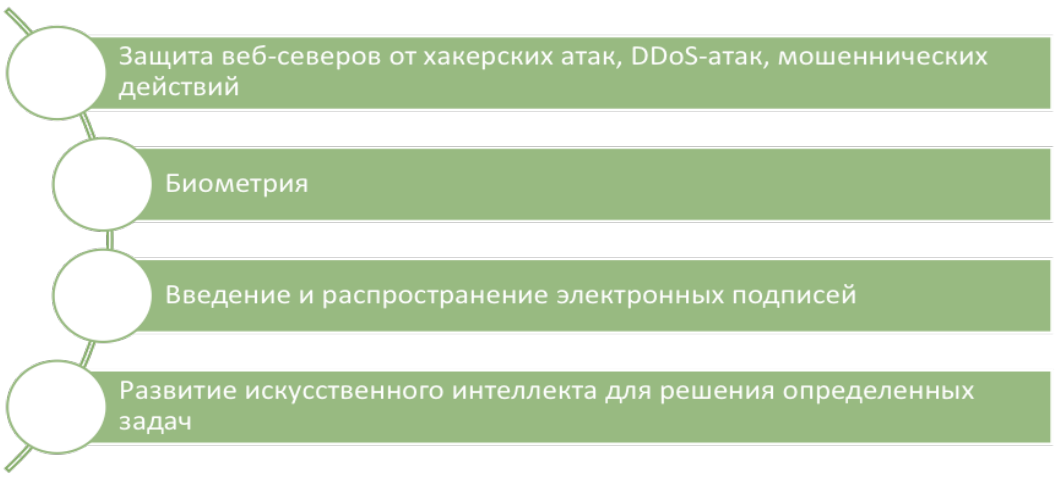
Существующее распределение ресурсов между странами по обеспечению безопасного и устойчивого функционирования сети интернет не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационной среде, механизмов и процедур их применения с учетом специфики ИКТ и цифровых технологий, затрудняет формирование системы международной информационной безопасности, способствующей стратегической стабильности и равноправному партнерству [14].

Понятие информационной безопасности многогранно и в условиях цифровой трансформации экономики претерпевает определенные изменения. В широком смысле под информационной безопасностью (ИБ) понимают определенное состояние, обеспечивающее защиту национальных интересов страны в информационном секторе, которые определяются совокупностью трех сбалансированных элементов: государство; общество; личность [3-4, 13]. В более узком смысле ИБ отождествляют с защищенностью информации

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

и ее поддерживающей сетевой инфраструктуры от воздействий, способных привести к неприемлемому ущербу субъектов отношений, включая владельцев и пользователей информации.

К информационным угрозам, несущим в себе нарушение информационной безопасности, относятся: непрофессиональные и преднамеренные действия, шпионаж, терроризм, преступные действия группы лиц, хакеров, стихийные действия и аварии, сбои и отказы технического обеспечения системы, нелегальное копирование и использование информации, заражение вирусами информационных систем. По сути, ИБ предполагает обеспечение целостности и устойчивости функционирования информационных систем и непосредственно связана с защитой информационной среды от внутренних и внешних угроз. Наиболее важные технологии и инструменты информационной защиты в цифровой среде представлены на рис. 3.




Источник: составлено авторами

Рис. 3. Инструменты обеспечения информационной безопасности цифровой экономики

Ярким примером обеспечения ИБ в цифровой сфере выступают биометрические технологии защиты, когда касанием пальца идентифицируется и подтверждается личность человека; распознавание личности клиента по голосу, позволяющее внедрить систему кредитования, в

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

которой личность клиента и кредитная история находятся в единой базе данных; криптография, позволяющая реализовать следующие процессы информационной защиты: идентификацию и аутентификацию объекта или субъекта сети связи или информационной системы; контроль или разграничение доступа к ресурсам локальной сети или внесетевым сервисам; обеспечение и контроль целостности данных. Другим инструментом является использование электронных цифровых подписей, содержащих в себе определенный цифровой код, для проведения государственных закупок, электронных торгов, при сдаче отчетности в контролирующие органы.

Переход на российское шифровальное программное обеспечение является одним из ключевых инструментов защиты информации в цифровом пространстве нашей страны. В современном мире функционируют две школы шифрования - России и США, к которым присоединяется Китай. Российские алгоритмы, одобренные специальным комитетом Международной организации по стандартизации (ISO), очень надежны [8]. На данный момент шифрование данных осуществляется по американским сертификатам безопасности. В этой ситуации российские пользователи оказываются под угрозой рассекречивания своих данных, которые хранятся на различных сайтах, в случае отзыва этих сертификатов их владельцами.

Еще одним фактом, представляющим опасность для российских пользователей сети, является тот факт, что свыше 60% информации, передающейся внутри российского пространства, проходит через серверы других государств, что повышает возможность ее доступности сторонним лицам [11]. Для поддержания ИБ особенно важны программно-технические меры и средства, поскольку основные угрозы компьютерным системам находятся в них и связаны со сбоями оборудования, с ошибками программного обеспечения, промахами пользователей и администраторов и т.п.

Не менее важны национальные стандарты киберфизических систем, контроль обработки и доступа к персональным данным, большим

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации. Создание национального и региональных центров реагирования на компьютерные инциденты также обеспечит высокий уровень информационной безопасности.

*Риск цифровой безопасности* связан с использованием и развитием цифровых технологий в процессе экономической деятельности, носит динамичный характер и включает в себя аспекты, связанные с цифровой, экономической и социальной средой, а также с деятельностью людей, вовлеченных в процессы цифровизации экономики и общества [5, с. 35]. Возможности и риски внедрения цифровых технологий представлены в таблице 1 [8], а основные классы и особенности рисков – в таблице 2 [5, с. 38].

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

*Таблица 1*

Возможности и риски внедрения цифровых технологий

| **Возможности цифровых технологий** | **Риски внедрения цифровых технологий** |
|---|---|
| Новые технологии, прорыв в ИИ, Интернете вещей, финтехе, анализе больших данных | Быстрое навязывание и заимствование западных технологий, деградация собственных компетенций |
| Новые функции, возможности общения, ускорение коммуникаций и платежей, новый уровень комфорта | Новые уязвимости, закладки, слежка, утечки персональных данных, потеря тайны личной жизни |
| Новые рынки, бизнес-модели, большие компании, массовые сервисы и информационные услуги | Риск быстрого захвата новых рынков транснациональными компаниями |
| Рост производительности труда, рост эффективности, внедрение ИИ, интеллектуализация, роботизация | Потеря рабочих мест, безработица, социальная напряженность, возникновение слоя тунеядцев |
| «Экономика обмена», исчезновение посредников, повышение скорости и стандартизации услуг, уберизация медицины, образования, транспорта, сферы услуг | Юридическая неопределенность, этические проблемы, рост мошенничества, снижение качества и ответственности, «роботизация» людей, рост социального отчуждения |
| Большие данные, анализ персональных данных, электронная идентификация и аутентификация личности, электронный двойник гражданина | Исчезновение приватности, навязчивая реклама, новый цифровой тоталитаризм, утечка персональных данных граждан за границу к мощным иностранным игрокам |
| Инвестиции, стартапы, новые деньги, новые индустрии, «перелицовка» традиционных индустрий | Захват экономики более сильными и богатыми иностранными игроками. Внешнее управление глобальной экономикой |

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

*Таблица 2*

Характерные особенности рисков цифровых технологий

| **Риски** | **Характерные особенности рисков цифровых технологий** |
|---|---|
| Операционные | Плохо разработанные цифровые технологии могут увеличить ошибки обработки. Неэффективные процедуры надзора могут привести к эксплуатационным сбоям. Входные данные, представленные разработчиками для обучения алгоритмов, используемых для цифровых технологий, могут быть устаревшими. Распространение инновационных продуктов и цифровых сервисов может увеличить сложность предоставления финансовых услуг, что затрудняет управление и контроль операционного риска |
| Финансовые | Неправильная реализация технологий может привести к финансовым и репутационным потерям организации. Стандарты и правила конфиденциальности данных могут подвергаться риску несоблюдения |
| Нормативные | Изменения в законодательстве или нормативных актах могут оказать существенное влияние на технологии. Некоторые строго регламентированные процессы (конфиденциальность данных) могут быть отключены в непредвиденные моменты. Неправильные и/или неполные нормативные документы, созданные с помощью технологий, могут привести к проблемам с регулированием и дорогостоящим штрафам. Технологии могут реализовываться способами, которые противоречат существующим законам |
| Организационные | Замена или перепрофилирование штатных сотрудников может негативно отразиться на их психологическом состоянии. Несоответствие между группами может привести к разрывам в ролях и подотчетности. Отсутствие стандартов по внесению изменений в технологии может помешать изменениям управленческих процессов. Одна технология может быть эквивалентной нескольким технологиям, что приводит к риску концентрации |
| Технологические | Влияние изменений планового технического обслуживания на существующие ИТ-платформы может потребовать регрессионное тестирование. Программному обеспечению могут потребоваться учетные данные для доступа к данным системы и приложения. Новые технологии могут быть использованы не по назначению (для выполнения очистки данных из приложений). Данные, представленные для освоения новых технологий, могут не иметь значения, что приведет к неверному результату |

Основными направлениями обеспечения цифровой безопасности являются:

– инновационное развитие средств, систем связи, среды передачи информации, ИКТ, ИТ, вычислительной техники и электронной промышленности;

– ликвидация зависимости российской промышленности от зарубежных ИТ и создание средств обеспечения ИБ за счет внедрения отечественных разработок, а также производства продукции и услуг на их основе;

– повышение конкурентоспособности российских компаний в сфере ИКТ, ИТ и электронной промышленности за счет создания благоприятных условий для развития отечественной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка и выхода на мировой рынок [14, с. 36-37].

## Интеграция процессов управления рисками и планирования развития инфокоммуникационного бизнеса

Научно-технический прогресс, конвергенция связи и информатики оказывают непосредственное воздействие на отраслевую специфику производства и потребления инфокоммуникационных услуг (ИКУ), организационную структуру и архитектуру сетевой инфраструктуры, экономические категории, модели бизнеса и экономическую безопасность [1, 15-17].

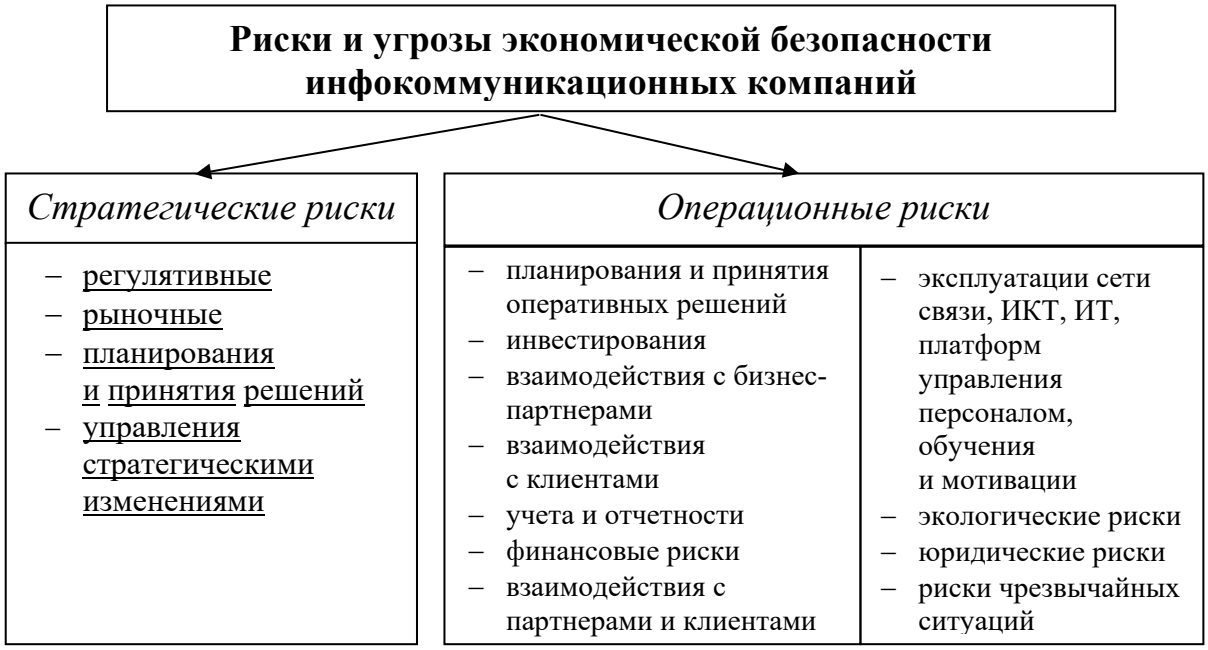
В условиях насыщения рынка услугами электросвязи для инфокоммуникационных компаний, включая ПАО «Ростелеком», наиболее обоснованной стратегией становится цифровая трансформация бизнеса с расширением спектра услуг и созданием цифровой экосистемы, что вызывает необходимость совершенствования инструментов управления рисками и экономической безопасности с учетом интеграции бизнеса и отраслевой специфики.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Невещественный характер и низкая материалоемкость продукта – информационно-коммуникационной услуги (ИКУ) - обуславливает более низкую потребность операторов связи в оборотных средствах и, как следствие, более низкий риск банкротства, а также специфичную политику управления оборотным капиталом операторов связи [18]. Эта политика состоит в обеспечении сбалансированности активов на основе соблюдения пропорций в объеме и структуре текущих финансовых ресурсов, источников их покрытия, а также соотношений между ними, достаточных для обеспечения эффективной производственной деятельности.

Объективно существующая и принципиально неустранимая полностью неопределенность диктует необходимость управления рисками [18-21]. Для инфокоммуникационных компаний (операторов связи) с прямой зависимостью предложения услуг от спроса игнорирование риска может проявиться в различных нежелательных хозяйственных результатах: уменьшении спроса, доходов и прибыли; неэффективности материальных, трудовых и финансовых ресурсов; высоких сроках окупаемости инвестиций; уменьшении котировок акций и т.д.

Систематизированные риски и угрозы экономической безопасности инфокоммуникационного бизнеса во взаимосвязи с целями и задачами деятельности по масштабам последствий представлены на рис. 5.




Источник: составлено авторами

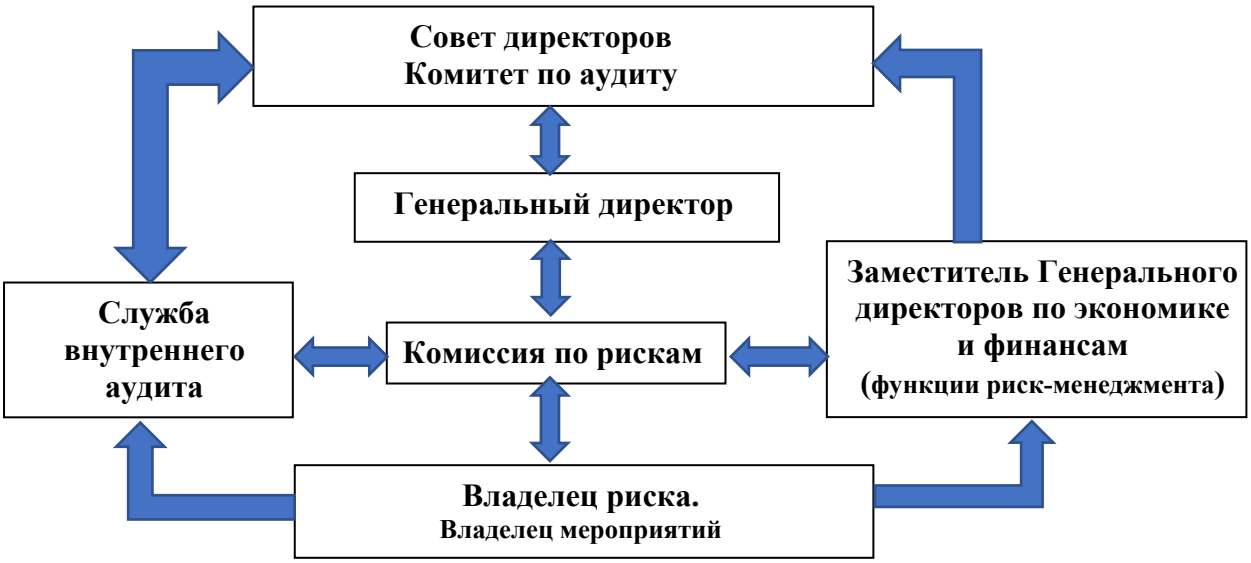
Рис. 5. Классификация рисков и угроз экономической безопасности бизнеса в сфере инфокоммуникаций

Стратегические риски характеризуют угрозы и возможности, возникающие на уровне принятия стратегических решений и обусловлены наращиванием масштабов бизнеса, внедрением новых цифровых продуктов, новых ИКТ, облачных сервисов, платформ, ИТ-систем, внесением качественных изменений в бизнес-модель компании и технологии. Операционные риски характеризуют угрозы осуществления постоянной операционной деятельности. Для компаний с сетевой инфраструктурой характерны особые риски эксплуатации сети связи, сетевого оборудования, ИКТ и ИТ-систем, экологические риски влияния деятельности операторов связи на окружающую природную среду.

В основе разработки стратегии управления рисками лежат два показателя: уровень существенности рисков и степень управляемости рисков, установление которых экспертным методом с учетом качественных критериев позволяет построить матрицу и выработать стратегию реагирования на риск. Наличие общих причин возникновения рисков и

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

причинно-следственных связей между ними обусловливает интегрированный подход к управлению рисками на основе унифицированных методик и алгоритмов. Интегрированная система управления рисками (ИСУР) представляет собой набор взаимосвязанных элементов, объединенных в единый процесс, в рамках которого руководство и работники участвуют в выявлении потенциальных негативных событий и управлении ими в целях роста конкурентоспособности и капитализации компании (рис. 6).




Источник: составлено авторами

Рис. 6. Типовая структура интегрированной системы управления рисками

При формировании такой системы необходимо решить задачи по определению организационной структуры, классификации и детальному описанию рисков, установлению этапов процесса управления рисками и обмена информацией о них, механизмам мониторинга системы и компании (в части управления рисками), взаимосвязи элементов с процессами планирования, бюджетирования и мотивации, а также критериев эффективности ИСУР.

Основой ИСУР являются: применение единообразных подходов к выявлению, оценке и управлению рисками; формирование механизма отслеживания качества управления рисками на основе четких и понятных критериев; оперативное реагирование на возникающие рисковые события,

отслеживание изменений внешней и внутренней среды; организация целенаправленной деятельности по управлению рисками с целью снижения их до приемлемого уровня либо передачи третьим сторонам (страхование, хеджирование); систематизация и накопление информации о рисках, повышение управляемости бизнеса.

Процесс функционирования ИСУР включает в себя совокупность процедур, представленных на рис. 7, которые логически следуют одна за другой, но хронологически осуществляются одновременно, в ходе выполнения одних и тех же мероприятий. Ключевыми процедурами функционирования интегрированной системы управления рисками компании являются:

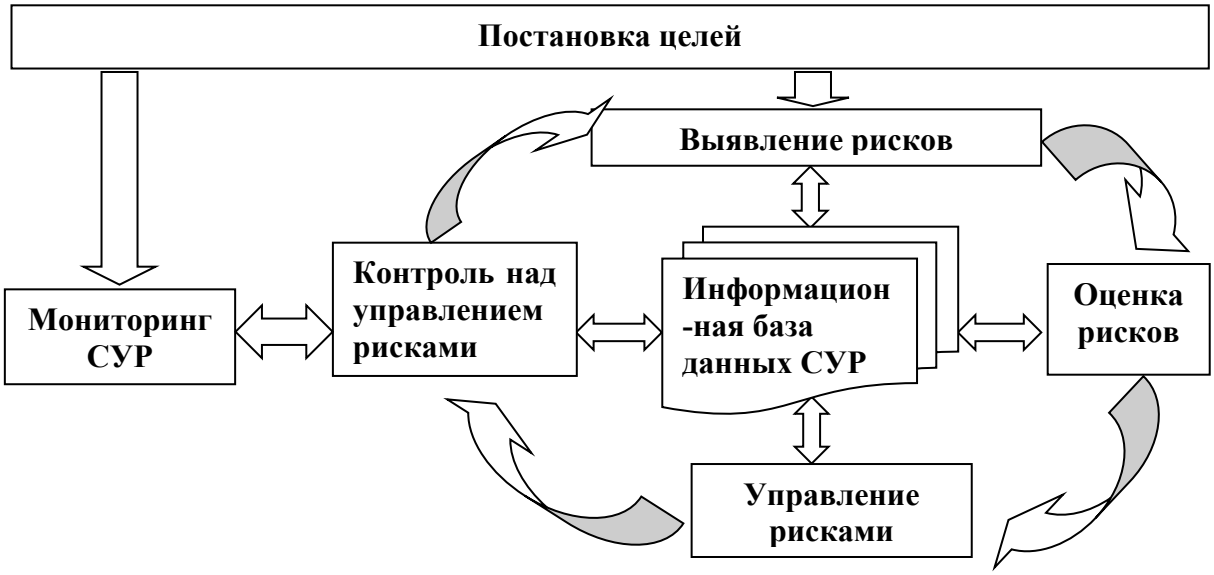
– выявление рисков, цель которого состоит в обнаружении рисков и включении их в регистр рисков компании;

– оценка рисков, позволяющая установить их существенность, произвести ранжирование и распределение по уровням управления компании;

– управление рисками, состоящее в разработке, согласовании и утверждении стратегий, планов действий и показателей эффективности управления рисками, а также определении необходимых ресурсов;

– контроль за управлением рисками, который позволяет установить своевременность и полноту реализации планов, выявить и разрешить возникшие в ходе выполнения планов проблемы.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru




Источник: составлено авторами

Рис. 7. Процесс функционирования системы управления рисками инфокоммуникационной компании

Интеграция процесса управления рисками в процесс планирования инфокоммуникационного бизнеса осуществляется на основе принципов, представленных на рис. 8. Управление рисками должно быть взаимосвязано с системой бюджетного планирования и контроля, программами инвестирования, выбором альтернативных планов развития. Выявленные риски и утвержденные способы реагирования на них могут и должны являться обоснованием при формировании бюджетных статей организации и его подразделений [17].

Для наиболее эффективной интеграции процессов планирования и управления рисками частота циклов данных процессов должна совпадать, причем в целях обеспечения эффективности системы управления рисками в индивидуальные планы руководства и работников организации должны быть включены цели по управлению рисками в соответствии с их ролью в общем процессе экономической безопасности.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru


Источник: составлено авторами

Рис. 8. Принципы интеграции процессов управления рисками и планирования развития инфокоммуникационного бизнеса

Использование интегрированного подхода при формировании бюджета направлено на точное и обоснованное планирование показателей бюджета и эффективное использование ресурсов во взаимосвязи с допустимыми рисками и угрозами. Для конкретизации стратегии реагирования на риск разрабатывается карта рисков по степени их управляемости в текущем и перспективном периодах (таблица 4).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

*Таблица 4*

Фрагмент карты рисков ПАО «Ростелеком»

| **Текущий период** | | **Прогнозный период** | |
|---|---|---|---|
| **Риски** | **Меры реагирования** | **Риски** | **Планируемые меры** |
| ***Рыночные*** (управляемость средняя) | | | |
| 1. Отсутствие реконструкции рынка по ценам, по регионам.<br>2. Захват рынков конкурентами | Разработка новых продуктов и сервисов. Мероприятия по повышению лояльности клиентов, быстрому выводу на рынок новых продуктов с целью захвата рынка | 1. Отсутствие динамики прироста ARPU.<br>2. Усиление оттока абонентов.<br>3. Захват рынков конкурентами | Мероприятия по повышению клиентской лояльности. Развитие новых услуг и сервисов на базе продуктовых офисов |
| ***Информационные технологии*** (управляемость высокая) | | | |
| Нарушение целостности и достоверности информации | Обеспечение синхронизации разработки проектов управления непрерывностью бизнеса и комплексной системы информационной безопасности | Нарушение целостности и достоверности информации | Реализация проектов цифровой и информационной защиты сети и внутренних сервисов. Учет рисков, связанных сервисами и внешними услугами при планировании |
| ***Законодательные*** (управляемость низкая) | | | |
| Неблагоприятные изменения законодательства | Мониторинг изменений законодательства. Оценка потребности и инвестиций в оборудовании для реализации согласованных мероприятий | Неблагоприятные изменения законодательства | Мониторинг изменений законодательства. Взаимодействие с партнерами по рынку, участие в профильных рабочих группах |

В ходе анализа выявленных рисков по степени управляемости и разработка мер реагирования на основе внедрения современных инструментов управления рисками, автоматизации разрабатываемых панелей риск-индикаторов бизнес-процессов компания может системно осуществлять комплекс постоянных улучшений в каждом подразделении и бизнес-процессе.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

## Заключение

Предложенный инструментарий интегации систем управления рисками и планирования деятельности бизнеса позволяет руководителям компаний и специалистам не только объяснять существующий уровень устойчивости бизнеса, но и измерять и прогнозировать последствия реализации рисков и угроз, системно модернизировать управление безопасностью бизнеса с учетом стратегии развития и новых кибернетических угроз в цифровой среде.

Раскрытие принципов интеграции процессов управления рисками и планирования развития бизнеса, типовой структуры, процесса функционирования интегрированной системы управления рисками подтверждается практикой деятельности инфокоммуникационных компаний. Использование интегрированного подхода при формировании бюджета позволяет не только снизить риски и нейтрализовать угрозы безопасности, но и повысить обоснованность планирования показателей бюджета и эффективность использование ресурсов во взаимосвязи с допустимыми рисками и угрозами.

Разработанная ИСУР позволяет эффективно моделировать, оценивать и минимизировать риски, осуществлять механизм управления рисками при формировании бюджета и повышать эффективность работы компании. ИСУР инфокоммуникационного бизнеса служит инструментом принятия эффективных управленческих решений в области стратегического и бюджетного планирования, мониторинга существенности рисков, мотивации и оценки результатов работы, а также межфункционального взаимодействия различных подразделений.

## Список литературы

1. Абаимова К.В., Арутюнян Э.Р. Проблемы экономической безопасности предприятия в современных условиях // Экономика и бизнес: теория и практика. - 2015. - № 4. - С. 4-8.

2. Кузовкова Т.А., Тимошенко Л.С. Анализ и прогнозирование развития инфокоммуникаций. - М.: Горячая линия-Телеком, 2016. - 162 с.

3. Кузовкова Т.А., Салютина Т.Ю. Экономическая безопасность бизнеса. Безопасность инфокоммуникационного бизнеса в условиях цифровой экономики: учебное пособие / МТУСИ. - М., 2020. - 175 с.

4. Как обезопасить свой бизнес: стабильность, угрозы, риски / Т.А. Кузовкова, Т.Ю. Салютина. - Москва: Ай Пи Ар Медиа; Алматы: EDP Hub (Идипи Хаб), 2024. - 156 с.

5. Лев М.Ю., Лещенко Ю.Г. Цифровая экономика: на пути к стратегии будущего в контексте обеспечения экономической безопасности // Вопросы инновационной экономики. - 2020. - Т. 10. - № 1. - С. 25-43.

6. Кузовкова Т.А., Салютина Т.Ю. Методы комплексной оценки цифрового развития экономики и общества: учебное пособие. - М.: Ай Пи Ар Медиа, 2022. - 118 с. - URL: https://www.iprbookshop.ru/117861.html.

7. Писаренко А.О. Экономическая безопасность в России: современное состояние, угрозы и перспективы развития // Национальные интересы: приоритеты и безопасность. - 2018. - Т. 14. - № 5. - С. 927-940.

8. Касперская Н.И. Цифровая экономика и риски цифровой колонизации. - URL: https://ivan4.ru/news/traditsionnye_semeynye_tsennosti/the_digitaleconomyand_therisks_of_digitalcolonization_kasperskaya_developed_the- ses of the_spee/.

9. Урмин И.Б, Загеева Л.А. Big data: большие вызовы, огромные возможности // Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт. - 2017. - № 9. - С. 107-110.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

10. Управление бизнесом в цифровой экономике: вызовы и решения / под ред. И.А. Аренкова, Т.А. Лезиной, М.К. Ценжарик, Е.Г. Черновой. - СПб.: Изд-во СПб. ун-та, 2019. - 360 с.

11. Хочуева Ф.А., Шугунов Т.Л., Жуков А.З., Ингушев Ч.Х. Информационная безопасность сквозь призму цифровой экономики // Современные наукоемкие технологии. - 2018. - № 11-1. - С. 65-71.

12. Леухина В.И. Государственное воздействие на процессы обеспечения экономической безопасности // Гуманитарные научные исследования. - 2021. - № 2. - URL: https://human.snauka.ru/2021/02/40113.

13. Экономическая безопасность России в новой реальности: Коллективная монография / под общ. ред. А.Е. Городецкого, И.В. Караваевой, М.Ю. Льва. - М.: ИЭ РАН, 2021. - 325 с.

14. Развитие цифровой экономики в России. Программа до 2035 года. - М.: Центр изучения Цифровой (электронной) экономики, 2017. - 41 с. - URL: http://innclub.info/wp-content/uploads/2017/05/strategy.pdf.

15. Кузовкова Т.А., Салютина Т.Ю., Шаравова О.И. Отражение специфики экономической безопасности инфокоммуникационного бизнеса в обучении магистров экономики // Методические вопросы преподавания инфокоммуникаций в высшей школе. – 2021. - № 1. - С. 41-45.

16. Шаравова М.М. Выявление характера цифровой трансформации моделей инфокоммуникационного бизнеса // Экономика и качество систем связи. - 2021. - № 1 (19). - С. 3-12.

17. Цифровая экосистема экономики будущего. Отчет об устойчивом развитии 2018. - М.: Ростелеком, 2018. - 203 с.

18. Шаравова О.И. Анализ и диагностика финансово-хозяйственной деятельности: Учебное пособие. - М.: МТУСИ, 2020. - 55 с.

19. Пикфорд Дж. Управление рисками. - М.: Вершина, 2004. - 349 с.

20. Сергеев А.А. Экономическая безопасность предприятия: учебник и практикум для вузов. - М.: Юрайт, 2019. - 273 с.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

21. Тарасова Н.В., Попова В.М. Экономическая безопасность предприятий малого и среднего бизнеса // International Journal of Humanities and Natural Sciences. - 2020. - Vol. 2-2 (41). - С. 58-64.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

# Risks of digital transformation of the economy and society and tools for managing the economic security of business in the digital environment

***Kuzovkova Tatiana Alekseevna,***
*Professor, Doctor of Economics,*
*Professor of the Department "Digital Economy,*
*Management and Business Technologies",*
*Moscow Technical University of Communications and Informatics,*
*8a Aviamotornaya str., Moscow, 111024*
*t.a.kuzovkova@mtuci.ru*

***Salutina Tatiana Yurievna,***
*Associate Professor, Doctor of*
*Economics, Head of the Department "Digital Economy,*
*Management and Business Technologies"*
*Moscow Technical University of Communications and Informatics,*
*8A Aviamotornaya str., Moscow, 111024, Russia,*
*t.i.salutina@mtuci.ru*

In conditions of significant uncertainty of the consequences of digital development and political instability of the world economy, theoretical and practical issues of economic security of business, threat identification and risk assessment, improvement of the principles and components of security management in the digital environment are relevant. The article reveals the impact of the digital transformation of the economy and society on the economic security of business, the sources of external and internal threats, the essence of the risks of digital and information security. Special attention is paid to the risks of digital security, the possibilities and risks are justified, as well as the specifics of the risks of digital technologies. As a system tool for managing the economic security of a business in a digital environment, the integration of risk management and development planning processes is proposed using the example of an infocommunication business.

**Keywords:** economic security, risks of digital technologies, digital transformation of the economy, risk management tools, integrated risk management system.