ИННОВАЦИОННОЕ И ПРОМЫШЛЕННОЕ РАЗВИТИЕ

УДК 338.47 *EDN: WOTVUJ*

Е.С. Митяков[1], Т.В. Абраменко[2]

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ СФЕРЫ ТЕЛЕКОММУНИКАЦИЙ

[1]МИРЭА – Российский технологический университет
Москва, Россия
[2]ПАО «Ростелеком»
Москва, Россия

Рассматриваются ключевые теоретические аспекты экономической безопасности в телекоммуникационном секторе России: анализируются угрозы, вызовы и риски, с которыми сталкивается данная сфера. Основная цель работы – формирование целостного понимания вызовов, угроз и рисков экономической безопасности телекоммуникационного сектора. Подчеркивается необходимость глубокого анализа и систематизации понятий экономической безопасности в контексте телекоммуникаций, обозначается недостаток внимания к этим вопросам в существующих исследованиях. Даны определения национальных интересов, вызовов, угроз, рисков экономической безопасности в телекоммуникационной сфере. Национальные интересы включают ключевые потребности в телекоммуникациях, способствующие реализации стратегических приоритетов страны. Показано, что для обеспечения экономической безопасности телекоммуникационной сферы необходимо комплексное применение политических, организационных, социально-экономических, информационных и правовых мер. Они должны реализовываться через взаимодействие государственных структур, местных органов управления, финансовых институтов и гражданского общества. Предложена авторская типология вызовов, угроз и рисков для экономической безопасности телекоммуникационного сектора России.

Ключевые слова: сфера телекоммуникаций; экономическая безопасность; вызовы; угрозы; риски; типология; обеспечение экономической безопасности.

Введение. Телекоммуникационный сектор – один из наиболее активно развивающихся секторов экономики РФ. Он играет ключевую роль, предлагая услуги частным лицам, бизнесу и государственным учреждениям,

выступает ключевым для российской экономики, поскольку поддерживает работу других сфер народного хозяйства и всего государства в целом.

В настоящее время рынок телекоммуникаций демонстрирует активное развитие. Растет не только число пользователей, но и доходы от оказания телекоммуникационных услуг. Основные операторы в России постепенно выходят за рамки традиционных телекоммуникаций и формируют многофункциональные экосистемы. В 2023 г. на этом рынке выделяются такие крупные игроки, как «Ростелеком», МТС, «Вымпелком», «Мегафон» и «Эр-Телеком». По информации Росстата, в 2023 г. доход этих компаний увеличился на 9,7 %, составив рекордные 2,6 трлн руб. [1]. Наблюдается и встречная тенденция, когда на рынке телекоммуникаций появляются нетипичные для него игроки. Кроме ИТ-компаний (ВК, Яндекс, Авито), на рынок активно выходят банки. Сбер, ВТБ, Тинькофф уже создали MVNO-оператора под своим брендом. Все это привело к тому, что, согласно данным «ТМТ Консалтинг», в 2023 г. российский рынок услуг связи увеличился на 5,1 %, достигнув объема более 1,9 трлн руб. Это стало наивысшим показателем роста рынка за последние десять лет [2].

Хотя сфера телекоммуникационных услуг в стране уже достигла определенной зрелости, он продолжает претерпевать значительные изменения ввиду разнообразных факторов экзогенного и эндогенного характера. Сектор телекоммуникаций перманентно сталкивается с разнообразными угрозами и вызовами его экономической безопасности, которые могут повлиять на его стабильность и дальнейший рост.

В текущих условиях важно усилить технологический суверенитет, поддержать спрос на отечественные разработки, перейти на российское оборудование и программное обеспечение, сохраняя высокий уровень услуг, конкурентную среду и развивая новые технологии связи. Это будет не только способствовать экономическому росту, но и станет играть ключевую роль в обеспечении экономической безопасности страны, минимизируя зависимость от зарубежных технологий и укрепляя позиции отечественных производителей. В свою очередь, экономическая безопасность телекоммуникационного сектора России имеет важное значение для стабильности и развития национальной экономики, поскольку он обеспечивает инфраструктуру для передачи данных и коммуникации, что является основой функционирования большинства других отраслей.

Данная статья направлена на формирование комплексного представления об угрозах, вызовах и рисках экономической безопасности сектора телекоммуникаций в России.

Обзор литературы. В экономической литературе существуют различные подходы к анализу экономической безопасности телекоммуникационной сферы в РФ. В исследованиях подчеркивается разнообразие угроз и вызовов, с которыми сталкивается сектор телекоммуникаций.

Так, в статье [3] показано, что ключевую роль в надлежащем функционировании сферы телекоммуникаций играет регулирование сферы и политика привлечения прямых иностранных инвестиций. Исследования показывают, что для обеспечения экономической безопасности требуется улучшение нормативной базы и создание благоприятных условий для иностранных инвесторов. Вместе с тем, на наш взгляд, в условиях ограниченного доступа к международным финансовым и технологическим ресурсам, необходимо искать внутренние резервы для обеспечения устойчивости и дальнейшего развития телекоммуникационного сектора в РФ.

Анализ, проведенный Организацией экономического сотрудничества и развития (OECD), указывает на структурные изменения в отрасли, включая тенденцию к консолидации и инновационное развитие. Эти изменения связаны с необходимостью удовлетворять более высокие требования общества и адаптироваться к новым технологиям и экономическим условиям [4].

В статье [5] рассмотрены проблемы экономической безопасности телекоммуникационных компаний, уделяется особое внимание информационной безопасности и увеличению киберугроз. Предложены рекомендации по улучшению ситуации. Статья [6] посвящена методическим подходам к использованию индикаторов экономической безопасности в системе сбалансированных показателей организаций телекоммуникационной сферы. В статье изложена методика формирования системы показателей для принятия управленческих решений стратегического и оперативного характера. Особое внимание уделено инновационному развитию сектора телекоммуникаций. В работе [7] показано влияние санкций, введенных после начала Специальной военной операции, которые серьезно сказались на телекоммуникационном секторе в стране. Санкции привели к увеличению расходов операторов связи, что побудило их перекладывать эти затраты на конечных пользователей. Операторы, ранее имевшие высокую конкурентоспособность, начали обсуждать совместное использование базовых станций для сохранения оборудования. Проблемы с привлечением капитала из-за вынужденного ухода с основных западных бирж также способствуют неопределенности в будущем развития сферы.

В исследовании [8] подчеркивается важность долгосрочной стратегии для обеспечения устойчивости сектора телекоммуникаций, показано, что в условиях продолжающихся санкций и экономической нестабильности российский телекоммуникационный сектор должен разработать меры по защите от внешних и внутренних угроз, включая обеспечение безопасности данных и устойчивость к кибератакам. В статье [9] рассматриваются особенности реализации концепции устойчивого развития в условиях цифровизации с фокусом на стратегии устойчивого развития телекоммуникационных предприятий. Авторы отмечают необходимость создания инфраструктуры для высокоскоростной связи с учетом экологических проблем. Обсуждаются экологические, социальные и экономические аспекты, а также инициативы

операторов связи в борьбе с климатическими проблемами и финансовыми вызовами. Автор предлагает стратегии для достижения устойчивого развития, включая внедрение возобновляемых источников энергии. Также отмечена роль пятого поколения мобильной связи в улучшении качества услуг.

В заключении далеко не исчерпывающего обзора научной литературы по тематике исследования следует отметить важность учета экономической безопасности в телекоммуникационной сфере России. Вместе с тем, наблюдается недостаточное внимание к понятийному аппарату, угрозам и вызовам, связанным с экономической безопасностью данного сектора. Несмотря на акцент на киберугрозах и зависимости от зарубежных технологий, требуется более тщательная проработка определения и систематизации понятий экономической безопасности.

Экономическая безопасность российской сферы телекоммуникаций: ключевые понятия. Экономическую безопасность социально-экономических систем следует рассматривать с точки зрения следующих подуровней: индивидуального, в отношении организаций, отраслевого, регионального, национального (государственного), межгосударственного и межнационального (мирового). Все они взаимосвязаны [10].

Сфера коммуникаций играет критическую роль на каждом уровне экономической безопасности, поскольку она связывает и поддерживает все аспекты функционирования как отдельных организаций, так и широких социально-экономических систем. Например, стабильная и безопасная работа телекоммуникаций в отдельной компании может существенно повлиять на ее операционные возможности и конкурентоспособность. На уровне региона и на уровне национальной экономики телекоммуникации обеспечивают ключевые инфраструктурные функции, которые влияют на бизнес-среду, государственное управление и общую социальную устойчивость. В глобальном масштабе развитие и безопасность телекоммуникационных сетей и технологий также имеют значение для международного сотрудничества и конкурентоспособности страны на мировом рынке. С другой стороны, социально-экономические процессы на всех иерархических уровнях оказывают значительное воздействие на сферу коммуникаций, стимулируя ее развитие и определяя приоритетные направления. Индивидуальный спрос на связь, инновации в компаниях, отраслевые потребности, региональные инвестиции, национальные стратегии и международное сотрудничество – все это влияет на инфраструктуру, технологии и регулирование телекоммуникационной сферы, способствуя ее развитию и укрепляя экономическую безопасность в целом. В табл. 1 показана взаимосвязь экономической безопасности систем различных иерархических уровней и сферы телекоммуникаций.

Таблица 1.

Взаимосвязь экономической безопасности систем различных иерархических уровней и сферы телекоммуникаций

Уровень	Влияние сферы телекоммуникаций на экономическую безопасность		Влияние уровня экономики на экономическую безопасность сферы телекоммуникаций	
	+	–	+	–
Уровень индивида	Доступ к информации и образованию, возможности для дистанционной работы, социальные коммуникации	Киберпреступления, мошенничество, зависимость от цифровых технологий	Спрос на телекоммуникационные услуги, повышение осведомленности о безопасности в цифровом пространстве	Фишинг, мошенничество, дезинформация, кибербуллинг и др.
Уровень организации	Повышение эффективности бизнес-процессов, коммуникации и координации	Риски кибератак и утечки данных, зависимость от поставщиков телекоммуникационных услуг	Инновации и развитие новых технологий в сфере телекоммуникаций, создание новых рабочих мест	Риски кибератак и утечки данных в компаниях
Отраслевой уровень	Развитие новых отраслей, повышение конкурентоспособности, создание новых рабочих мест	Неравномерное развитие, угроза монополизации телекоммуникационных рынков	Развитие инфраструктуры, автоматизация производства	Риски монополизации, недостаток инвестиций, правовые ограничения
Региональный уровень	Стимулирование экономического роста, развитие инфраструктуры	Цифровой разрыв между регионами, риск оттока населения в развитые регионы	Развитие цифровых инфраструктур, привлечение инвестиций в отрасль, создание новых рабочих мест	Недостаток инвестиций в телекоммуникационную инфраструктуру
Национальный уровень	Укрепление национальной безопасности, стимулирование инноваций и технологического развития, рост конкурентоспособности на мировом рынке	Кибератаки, пропаганда, угроза суверенитета в сфере телекоммуникаций, зависимость от иностранных технологий	Развитие телекоммуникационной инфраструктуры, создание национальных телекоммуникационных стандартов, стимулирование инноваций	Риски кибератак на национальном уровне, политические ограничения и цензура в сфере телекоммуникаций
Мировой уровень	Развитие международного сотрудничества, международной торговли, ускорение глобальной интеграции	Конфликты в сфере телекоммуникаций, риски для международной безопасности	Усиление глобальной взаимосвязи и интеграции, создание глобального информационного пространства	Угрозы глобальной безопасности, контроль и манипуляции информацией на глобальном уровне и др.

Источник: составлено авторами

В *Стратегии экономической безопасности Российской Федерации на период до 2030 года* определены ключевые понятия экономической безопасности национальной экономики [11]. В данной работе определения адаптированы к сфере телекоммуникаций, чтобы отразить специфические особенности данного сектора в контексте обеспечения экономической безопасности.

Экономическая безопасность телекоммуникационной сферы представляет собой состояние защищенности российской телекоммуникационной инфраструктуры от внешних и внутренних угроз, при котором обеспечивается ее способность поддерживать экономический суверенитет страны, единство и устойчивость телекоммуникационного пространства на всех уровнях. Это состояние также гарантирует, что телекоммуникационная сфера способствует реализации стратегических национальных приоритетов и поддерживает экономическую безопасность различных уровней, от индивидуальных организаций до региональных и национальных систем.

Национальные интересы в телекоммуникационной сфере включают в себя ключевые потребности страны в области телекоммуникаций, удовлетворение которых способствует реализации стратегических национальных приоритетов как в этой сфере, так и в более широком контексте обеспечения устойчивого развития и безопасности страны в целом.

Вызовы экономической безопасности в телекоммуникационной сфере – факторы, которые при определенных условиях могут привести к угрозам экономической безопасности телекоммуникационной сферы, такие как развитие новых технологий, изменения в международной политике и экономические санкции.

Угроза экономической безопасности в телекоммуникационной сфере – совокупность условий и факторов, создающих возможность нанесения ущерба национальным интересам России в секторе телекоммуникаций.

Риск экономической безопасности в телекоммуникационной сфере – возможность нанесения ущерба национальным интересам России в телекоммуникационной сфере в результате реализации угроз экономической безопасности, например, через кибератаки или нарушение поставок технологического оборудования.

Обеспечение экономической безопасности телекоммуникационной сфере включает в себя осуществление комплекса политических, организационных, социально-экономических, информационных, правовых и иных мер, направленных на защиту телекоммуникационной сферы от вызовов и угроз, а также на обеспечение ее устойчивости и независимости. Эти меры реализуются в рамках взаимодействия государственных структур, местных органов управления, финансовых институтов и гражданского общества.

Стратегия развития отрасли связи России до 2035 года ставит цель усиления технологического суверенитета, что подразумевает контроль государства над сетями связи и всеми устройствами, передающими информацию, на территории страны.

Исследование нормативных правовых актов, стратегических планов и значительного количества научных публикаций позволяет предложить определенную последовательность рассматриваемых понятий: «Вызов → Угроза → Риск» [12]. Вызовы экономической безопасности создают условия, при которых могут возникать угрозы. Например, развитие новых технологий (вызов) может привести к кибератакам (угроза). В свою очередь, угрозы представляют конкретные ситуации, которые могут реализоваться в условиях вызовов и нанести ущерб. Например, кибератака (угроза) может реализоваться при недостаточной защите инфраструктуры. Наконец, риски экономической безопасности отражают вероятность и потенциальные последствия реализации угроз. Так, кибератака (угроза) может привести к утечке данных и финансовым потерям (риск). При этом негативные последствия реализации риска предполагают сохранение угрозы, позитивные последствия – ее нейтрализацию [13].

Экономическая безопасность российской отрасли телекоммуникаций: типология вызовов, угроз и рисков. Основные вызовы и угрозы национальной безопасности и экономики России отражены в стратегических документах, включая Доктрину информационной безопасности [14], *Стратегию национальной безопасности* [15] и *Стратегию экономической безопасности Российской Федерации* [11]. Эти документы подчеркивают важность обеспечения защиты критической инфраструктуры, включая телекоммуникации, от угроз и рисков. В представленных документах подчеркиваются ключевые вызовы и угрозы, с которыми сталкивается Россия, в том числе, с теми, которые имеют прямое отношение к сектору телекоммуникаций.

Одной из основных угроз, обозначенных в стратегических документах, выступает нарастание информационных атак на молодежную аудиторию, нацеленных на размывание традиционных духовно-нравственных ценностей России. Также в условиях активного использования информационных технологий возрастает число преступлений, связанных с нарушением конституционных прав и свобод человека, включая неприкосновенность частной жизни и обработку персональных данных. Данные нарушения подрывают права граждан и ставят под угрозу их безопасность.

В документах отмечается, что угрозы, связанные с применением информационных технологий, могут нанести серьезный ущерб государственному суверенитету и территориальной целостности. Кроме того, низкий уровень внедрения отечественных разработок и кадрового обеспечения в области информационной безопасности подчеркивает необходимость повышенного внимания к телекоммуникационному сектору. Внедрение отечественных технологий и создание устойчивой кадровой базы в сфере телекоммуникаций необходимы для снижения зависимости от внешних факторов и повышения общего уровня безопасности.

В данном разделе работы представлена авторская типология вызовов, угроз и рисков экономической безопасности отрасли телекоммуника-

ций в РФ. В научных исследованиях данные категории экономической безопасности классифицируются по различным критериям. Например, угрозы могут классифицироваться по происхождению (внутренние и внешние), степени опасности (от умеренно опасных до крайне опасных), вероятности возникновения, масштабу и характеру влияния, уровню ущерба и форме проявления. Также они могут затрагивать различные бизнес-процессы в социально-экономических системах, такие как снабжение, производство, сбыт, финансы и социально-экономические аспекты, а их природа может быть политической, экономической, социальной, техногенной, правовой, экологической и др.

Надлежащая типология указанных категорий экономической безопасности в сфере телекоммуникаций имеет важное значение по нескольким причинам. Она позволяет определить их характер, масштаб и потенциальное воздействие на экономику, что помогает в разработке стратегических мер защиты. Кроме этого, понимание различных видов угроз позволяет выделить ресурсы и усилия на наиболее значимые и опасные угрозы.

Типология современных вызовов экономической безопасности телекоммуникационной отрасли в России представлена на рис. 1.

Рис. 1. Типология вызовов экономической безопасности телекоммуникационной сферы

Источник: составлено авторами

Отметим, что представленные типы вызовов взаимодействуют друг с другом и могут усиливать взаимное влияние, создавая сложные условия для обеспечения экономической безопасности.

Типология угроз экономической безопасности телекоммуникационной отрасли в России представлена на рис. 2. Угрозы могут проявляться как по отдельности, так и в своем сочетании.

Рис. 2. Типология угроз экономической безопасности телекоммуникационной сферы
Источник: составлено авторами

Наконец, типология рисков экономической безопасности телекоммуникационной отрасли в России может быть представлена в виде рис. 3.

Рис. 3. Типология рисков экономической безопасности телекоммуникационной сферы
Источник: составлено авторами

Далее рассмотрим ряд цепочек «Вызов -> Угроза -> Риск», которые демонстрируют, как вызовы в телекоммуникационной отрасли могут привести к угрозам, а затем и к конкретным рискам для экономической безопасности (табл. 2). В таблице представлен далеко не полный перечень таких цепочек, использование которых позволяет структурировать информацию о потенциальных проблемах, их последствиях и связанных рисках, что помогает в стратегическом планировании и управлении рисками.

Таблица 2.

Примеры цепочек «Вызов -> Угроза -> Риск» в контексте сферы телекоммуникаций

Вызов	Угроза	Риск
Быстрое развитие новых технологий (5G, IoT, AI)	Кибератаки на новейшую инфраструктуру	Утечка данных и компрометация информации
Обновление и устаревание оборудования	Несовместимость и уязвимость устаревшего оборудования	Нарушение работы сетевой инфраструктуры
Разработка и внедрение новых стандартов связи	Монополизация стандартов крупными игроками	Ограничение доступа к инновациям для отдельных участников рынка
Геополитическая нестабильность	Санкции и экономическая изоляция	Прекращение поставок критически важного оборудования
Торговые войны и санкции	Ограничение доступа к международным рынкам и финансам	Утрата позиций на международном рынке
Политические конфликты и изменения альянсов	Нарушение международных соглашений о сотрудничестве	Уменьшение инвестиционных возможностей
Колебания курсов валют	Удорожание импортного оборудования	Рост затрат на альтернативные источники и логистику
Изменения в налогообложении	Увеличение налогового бремени на компании	Финансовые потери и снижение рентабельности
Финансовые кризисы и рецессии	Снижение доступности кредитов и инвестиций	Срывы в работе из-за недоступности компонентов
Новые законодательные инициативы	Ужесточение требований по защите данных и конфиденциальности	Финансовые потери из-за необходимости адаптации к новым требованиям
Изменения в регулировании телекоммуникационной отрасли	Непредсказуемость правового поля	Ухудшение условий для бизнеса и снижение инвестиций

Окончание табл. 2

Ужесточение требований по защите данных и конфиденциальности	Повышенные затраты на соответствие требованиям	Снижение рентабельности и увеличение операционных расходов
Концентрация рынка в руках одного или нескольких крупных игроков	Злоупотребление рыночной властью для установления высоких цен	Увеличение затрат для потребителей и снижение доступности услуг
Ограничение конкуренции и инноваций	Снижение качества услуг из-за отсутствия конкурентного давления	Потеря гибкости и инновационности отрасли
Создание барьеров для входа новых участников на рынок	Ограничение доступа к рынку для новых участников	Увеличение зависимости от ограниченного числа поставщиков и операторов
Коррупция и злоупотребления	Недобросовестные действия сотрудников	Финансовые потери и ухудшение качества услуг и продукции
Недобросовестные действия сотрудников	Умышленное нарушение правил и стандартов	Потеря доверия пользователей и клиентов
Низкая квалификация и отсутствие профессиональных кадров	Ошибки в эксплуатации и управлении	Снижение качества услуг и увеличение аварийных ситуаций

Источник: составлено авторами

Заключение. Необходимо подчеркнуть значимость понимания и систематизации понятий, связанных с экономической безопасностью в телекоммуникационном секторе России. Учитывая постоянно меняющиеся вызовы, такие как развитие новых технологий и международные политические обстоятельства, становится очевидным, что эти факторы могут привести к реальным угрозам, представляющим опасность для национальных интересов. Важно отметить, что угрозы в этой сфере формируют условия, при которых возникают риски, связанные с потенциальным ущербом. Для эффективной защиты экономической безопасности телекоммуникационного сектора требуется комплексный подход, который включает в себя не только политические и правовые меры, но и активное взаимодействие различных государственных и частных институтов. Важно, чтобы эти меры были направлены на системное выявление и оценку угроз и рисков, а также на выработку стратегий, способствующих укреплению устойчивости сектора. Авторская типология вызовов, угроз и рисков, представленная в статье, предоставляет аналитический базис для дальнейшего исследования и разработки стратегий и механизмов обеспечения экономической безопасности в телекоммуникационной сфере. Правильная интерпретация и интеграция этих концепций помогут в структу-

рировании информации о потенциальных вызовах, что, в свою очередь, будет способствовать более эффективному стратегическому планированию и управлению рисками, обеспечивая безопасное и устойчивое функционирование телекоммуникационного сектора в России.

Библиографический список

[1] Оборот телеком-операторов РФ в 2023 году вырос на 9,7%. [Электронный ресурс]. URL: https://www.interfax.ru/business/945050

[2] Российский рынок телекоммуникаций – 2023. [Электронный ресурс]. URL: mt-consulting.ru/wp-content/uploads/2023/12/TMT-телеком-2023.pdf

[3] Petuhova S., Vronetz A., Pfaffenberger W. (1999). Regulation of the Telecommunication Sector in Russia: Direct Foreign Investments and Options for Competition. In: Welfens, P.J.J., Yarrow, G., Grinberg, R., Graack, C. (eds) Towards Competition in Network Industries. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-60189-7_10

[4] Darryl Biggar, 2002. The Telecommunications Sector in Russia. OECD Journal: Competition Law and Policy, OECD Publishing, vol. 4(3), pages 223-230.

[5] Семенов К.О. Специфика и проблемы обеспечения экономической безопасности российских телекоммуникационных компаний // Вестник Московского финансово-юридического университета МФЮА. 2023. № 2. С. 118-127. DOI 10.52210/2224669X_2023_2_118.

[6] Куринов С.М. Инновационное развитие как элемент обеспечения экономической безопасности в телекоммуникационных компаниях // Бизнес в законе. Экономико-юридический журнал. 2015. № 2. С. 249-252.

[7] Kolomychenko Maria. The Impact and Limits of Sanctions on Russia's Telecoms Industry. *DGAP Analysis 3 (2024)*. German Council on Foreign Relations. March 2024. https://doi.org/10.60823/DGAP-24-40476-en.

[8] Ganichev N.A., Koshovets O.B. Rethinking Russian Digital Economy Development Under Sunctions. Studies on Russian Economic Development. 33, 645–655 (2022). https://doi.org/10.1134/S1075700722060041

[9] Давыдов А.А. Формирование стратегии устойчивого развития предприятий отрасли связи в условиях цифровой экономики // Вестник евразийской науки. 2023. Т.15. № s3. URL: https://esj.today/PDF/07FAVN323.pdf

[10] Компанейцева Г.А. Система экономической безопасности: уровни и механизмы оценки // Научно-методический электронный журнал «Концепт». 2016. Т. 17. С. 832-836. [Электронный ресурс]. URL: http://e-koncept.ru/2016/46342.htm.

[11] Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года». [Электронный ресурс]. [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71572608/

[12] Оганян В.А. Классификация вызовов и угроз экономической безопасности индивидуальных предпринимателей, использующих интеллектуальные активы // Фундаментальные и прикладные исследования кооперативного сектора экономики. 2022. № 1. С. 129-138.

[13] Сушкова И.А. Соотношение и взаимосвязь понятий "вызов", "опасность", "угроза", "риск" // Экономическая безопасность и качество. 2018. № 4 (33). С. 10-15. EDN SKSDSU.
[14] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: https://base.garant.ru/71556224/
[15] Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. URL: https://base.garant.ru/401425792/

E.S. Mityakov[1], T.V. Abramenko[2]

THEORETICAL ASPECTS OF ECONOMIC SECURITY IN THE RUSSIAN TELECOMMUNICATIONS SECTOR

[1]MIREA – Russian Technological University
Moscow, Russia
[2]Rostelecom
Moscow, Russia

Abstract. The article examines the key theoretical aspects of economic security in the telecommunications sector of Russia, focusing on the threats, challenges, and risks faced by this field. The primary objective of the study is to form a comprehensive understanding of the challenges, threats, and risks to the economic security of the telecommunications sector. The paper emphasizes the necessity of in-depth analysis and systematization of the concepts of economic security in the context of telecommunications, highlighting the lack of attention given to these issues in existing research. Definitions of national interests, challenges, threats, and risks to economic security in the telecommunications field are provided. National interests encompass key telecommunications needs that facilitate the realization of the country's strategic priorities. It is shown that ensuring economic security in the telecommunications sector requires a comprehensive application of political, organizational, socio-economic, informational, and legal measures. These measures must be implemented through the interaction of governmental structures, local authorities, financial institutions, and civil society. The article also presents an author's typology of challenges, threats, and risks to the economic security of the telecommunications sector in Russia.

Keywords: telecommunications sector; economic security; challenges; threats; risks; typology; ensuring economic security.

References

[1] Telecom Operators' Turnover in Russia in 2023 Increased by 9.7%. [Electronic resource]. Available at: https://www.interfax.ru/ business/945050
[2] Russian Telecommunications Market – 2023. [Electronic resource]. Available at: https://mt-consulting.ru/wp-content/uploads/2023/12/TMT-телеком-2023.pdf

[3] Petuhova, S., Vronetz, A., Pfaffenberger, W. (1999). Regulation of the Telecommunication Sector in Russia: Direct Foreign Investments and Options for Competition. Towards Competition in Network Industries. Springer, Berlin, Heidelberg.

[4] Biggar, D. (2002). The Telecommunications Sector in Russia. OECD Journal: Competition Law and Policy, OECD Publishing. pp. 223-230.

[5] Semenov, K.O. (2023). [Specifics and Problems of Ensuring Economic Security of Russian Telecommunications Companies]. *Vestnik Moskovskogo finansovo-yuridicheskogo universiteta MFYuA* [Bulletin of the Moscow University of Finance and Law MFUA]. No. 2. pp. 118-127. (In Russ).

[6] Kurinov, S.M. (2015). [Innovative Development as an Element of Ensuring Economic Security in Telecommunications Companies]. *Biznes v zakone. Ekonomiko-yuridicheskiy zhurnal* [Business in Law. Economic and Legal Journal]. No. 2. pp. 249-252. (In Russ).

[7] Kolomychenko, M. (2024). The Impact and Limits of Sanctions on Russia's Telecoms Industry. DGAP Analysis 3. German Council on Foreign Relations.

[8] Ganichev, N.A., Koshovets, O.B. (2022). Rethinking Russian Digital Economy Development Under Sanctions. Studies on Russian Economic Development, 33. pp. 645-655.

[9] Davydov, A.A. (2023). [Formation of a Sustainable Development Strategy for the Telecommunications Industry in the Digital Economy]. *Vestnik evraziyskoy nauki* [Bulletin of Eurasian Science]. Vol. 15. (In Russ).

[10] Kompaniytseva, G.A. (2016). [System of Economic Security: Levels and Mechanisms of Evaluation]. *Nauchno-metodicheskiy elektronnnyy zhurnal «Kontsept»* [Scientific and Methodical Electronic Journal "Koncept"], Vol. 17. pp. 832-836. (In Russ).

[11] Presidential Decree of the Russian Federation No. 208 "On the Strategy of Economic Security of the Russian Federation for the Period Until 2030" dated May 13, 2017. [Electronic resource]. Available at: https://www.garant.ru/products/ipo/prime/doc/71572608/ (In Russ).

[12] Oganyan, V.A. (2022). [Classification of Challenges and Threats to the Economic Security of Individual Entrepreneurs Using Intellectual Assets]. *Fundamentalnye i prikladnye issledovaniya kooperativnogo sektora ekonomiki* [Fundamental and Applied Research of the Cooperative Sector of the Economy]. No. 1. pp. 129-138. (In Russ).

[13] Sushkova, I.A. (2018). [Correlation and Interconnection of the Concepts of "Challenge", "Danger", "Threat", "Risk"]. *Ekonomicheskaya bezopasnost i kachestvo* [Economic Security and Quality]. No. 4(33). pp. 10-15. (In Russ).

[14] Presidential Decree of the Russian Federation No. 646 "On the Approval of the Information Security Doctrine of the Russian Federation" dated December 5, 2016. [Electronic resource]. Available at: https://base.garant.ru/71556224/

[15] Presidential Decree of the Russian Federation No. 400 "On the National Security Strategy of the Russian Federation" dated July 2, 2021. [Electronic resource]. Available at: https://base.garant.ru/401425792/