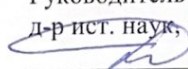


Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Наименование учебного структурного подразделения

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК

Руководитель ООП

д-р ист. наук, профессор

 Л.В. Дериглазова

подпись

« 15 » июне 20 23 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА МАГИСТРА
(МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

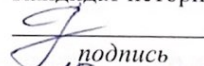
ПРОБЛЕМЫ ПЕРЕХОДА НА 5G В ЕС: ТЕХНОЛОГИЧЕСКИЕ И ПОЛИТИЧЕСКИЕ
АСПЕКТЫ

по направлению подготовки 41.04.05 «Международные отношения»
направленность (профиль) «Исследования Европейского Союза»

Собиров Сарварбек Соибжон угли

Руководитель ВКР

Кандидат исторических наук

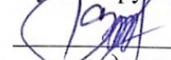
 О.В. Устюжанцева

подпись

« 15 » июне 20 23 г.

Автор работы

студент группы № 032129

 С.С. Собиров

подпись

« 15 » июне 20 23 г.

Министерство науки и высшего образования Российской Федерации.

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Наименование учебного структурного подразделения

УТВЕРЖДАЮ

Руководитель ООП

д-р. ист. наук, профессор



Л.В. Дериглазова

подпись

« 15 » марта 20 23 г.

ЗАДАНИЕ

по выполнению выпускной квалификационной работы бакалавра / специалиста / магистра
обучающегося

Собиров Сарварбек Соибжон угли

Фамилия Имя Отчество обучающегося

по направлению подготовки Код Наименование направления подготовки, направленность
(профиль) «Наименование образовательной программы»

1 Тема выпускной квалификационной работы

Проблемы перехода на 5g в ЕС: технологические и политические аспекты

2 Срок сдачи обучающимся выполненной выпускной квалификационной работы:

а) руководитель ООП

За 5 дня до защиты

б) в ГЭК –

За 2 дня до защиты

3 Исходные данные к работе:

Объект исследования – Технологическая политика ЕС.

Предмет исследования – Проблемы перехода на 5G в Европейском союзе с учетом
технологических и политических аспектов

Цель исследования – Цель данной диссертации заключается в исследовании проблем,
связанных с переходом на технологию 5G в Европейском Союзе,
с учетом технологических и политических аспектов.

Задачи:

1. Изучить регулирование для обеспечения полного покрытия 5G в ЕС;
2. Проанализировать проблемы, которые обсуждаются в ЕС в связи с переходом на 5G в ЕС;
3. Выявить, каким образом обсуждаемые проблемы влияют на процесс обеспечения полного покрытия 5G в ЕС;

Методы исследования:

Общенаучные методы сравнения, анализа, синтеза и индукции.

Политологические методы системного и сравнительного анализа.

Экспликативные методы контент-анализа.

Организация или отрасль, по тематике которой выполняется работа, –

Европейский союз

4 Краткое содержание работы

Работа состоит из введения, двух глав, заключения, списка использованных источников
и литературы, а так же приложения.

Во введении обосновывается актуальность темы исследования, приводятся цель, задачи, проблема, гипотеза, методология, а также проводится обзор источников и литературы. В теоретической части работы приведен детальный анализ регуляторных органов ЕС по вопросам 5G и стратегии и реализованные проекты в ЕС, с ними можно ознакомиться в первой главе "Регулирование 5G в Европе: Исследование Полного Покрытия". Вторая глава посвящена на анализу технологических и политических аспектов.

Руководитель выпускной квалификационной работы
канд. ист. наук, НИ ТГУ

должность, место работы



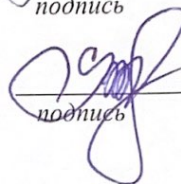
подпись

/ О. В. Устюжанцева

И.О. Фамилия

Задание принял к исполнению
магистрант, НИ ТГУ

должность, место работы



подпись

/ С. С. Собиров

И.О. Фамилия

АННОТАЦИЯ

Работа магистра посвящена изучению проблем и вызовов, с которыми сталкиваются страны Европейского Союза при переходе на пятое поколение сетей связи. Она охватывает как технологические, так и политические аспекты этого перехода, исследуя роль новых технологий, требования к безопасности данных, и влияние этих аспектов на политику ЕС. Главной задачей исследования будет попытка сформулировать комплексное понимание динамики перехода на 5G в ЕС и возникающих при этом проблем.

Основные задачи исследования:

1. Изучить регулирование для обеспечения полного покрытия 5G в ЕС.
2. Проанализировать проблемы, которые обсуждаются в ЕС в связи с переходом на 5G в ЕС.
3. Выявить, каким образом обсуждаемые проблемы влияют на процесс обеспечения полного покрытия 5G в ЕС.

Работа выполнена на тему, которая охватывает одну из ключевых областей современных телекоммуникаций и геополитики - переход на технологию 5G в странах Европейского Союза. Эта тема представляет собой сложное пересечение технологических и политических вопросов и оказывает влияние на различные сферы: от цифровой экономики и безопасности до геополитики и международных отношений.

Данная диссертация представляет собой исследование внедрения технологии 5G в Европейском Союзе (ЕС) с учетом технологических и политических аспектов. В работе освещаются различные аспекты этого процесса, включая регулирующие органы, механизмы финансирования и текущее состояние инфраструктуры по 5G в ЕС. Анализируются роли и функции регуляторных органов, таких как Европейская комиссия, их стратегии и политики, направленные на успешное внедрение 5G. Также рассматриваются механизмы финансирования и инвестиций, используемые для развития 5G-инфраструктуры в ЕС. В работе уделяется особое внимание возникающим технологическим и политическим проблемам, связанным с внедрением 5G, включая влияние торговой войны между США и Китаем на ЕС. Исследуется влияние ограничений и последствий, возникающих в результате этой торговой войны, на процесс внедрения и развитие 5G в ЕС.

В диссертационной работе изложены материалы, облегчающие понимание сложного процесса внедрения 5G в ЕС. В магистерском исследовании было использовано

в общей сложности 95 источников, включая академические работы, законодательные акты ЕС, стратегические материалы, отчеты регуляторных органов и мнения экспертов. В теоретической части работы приведен детальный анализ регуляторных органов ЕС по вопросам 5G и стратегии и реализованные проекты в ЕС, с ними можно ознакомиться в первой главе “Регулирование 5G в Европе: Исследование Полного Покрытия”. Вторая глава посвящена на анализ технологических и политических аспектов.

Исследование было проведено с использованием общенаучные методы сравнения, анализа, синтеза и индукции, а также политологические методы системного и сравнительного анализа. Кроме того, были использованы экспликативные методы контент-анализа. В основе исследования лежит анализ обширного объема нормативных и информационных источников с последующим их исследованием. Применение системного подхода позволило рассмотреть предмет и объект исследования в комплексе и установить взаимосвязь между политическими и технологическими аспектами внедрения 5G в ЕС.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
Глава 1. Регулирование 5G в Европе: Исследование Полного Покрытия	8
1.1 Безопасность для обеспечения конфиденциальности и целостности данных	8
1.2 Регуляторная надзорная структура	14
1.3 Роль финансирующих организаций в развитии 5G инфраструктуры в Европейском Союзе.....	16
1.4 Регулирование спектра в ЕС	21
1.5 Вклад национальных регуляторных органов в странах ЕС	26
1.6 Общая характеристика регулирования 5G в Европейском Союзе.....	28
Глава 2. Анализ проблем и вызовов при переходе на 5G в ЕС	31
2.1 Технологические аспекты перехода на 5G в ЕС	31
2.2 Проблемы со спектром.	34
2.3 Стоимость развертывания.	36
2.4 Проблемы безопасности.....	39
2.4.1 Мобильные виртуальные операции.	41
2.4.2 Телекоммуникационный мошенничество	43
2.4.3 Проблемы IoT.	44
2.4.4 Сетевые атаки	45
2.4.5 Конфиденциальность пользователя в рамках 5G.	46
2.4.6 Уязвимости безопасности сети, коммуникация	47
2.5 Политические аспекты и проблемы безопасности при переходе на 5G в ЕС	48
ЗАКЛЮЧЕНИЕ.....	58
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ.....	61
ПРИЛОЖЕНИЕ А Национальные регуляторные органы стран ЕС.....	71
ПРИЛОЖЕНИЕ Б Иллюстрация покрытия и емкости по сравнению с частотой	75
ПРИЛОЖЕНИЕ В Обзор 5G в странах ЕС: частоты, стоимость, операторы, поставщики, уровень внедрения	76

ВВЕДЕНИЕ

Исследование предоставляет обзор проблем и возможностей, связанных с переходом к сетям 5G в Европейском Союзе. Развитие и расширение сетей 5G является стратегическим приоритетом в области информационных и коммуникационных технологий и имеет значительное влияние на различные отрасли и сферы деятельности в ЕС. В рамках данного исследования проводится анализ технологических и политических аспектов, связанных с переходом к 5G в ЕС. Оно направлено на расширение знаний и понимания о проблемах и перспективах внедрения сетей 5G, а также может быть полезным для исследователей, которые стремятся провести более глубокий анализ проблем, связанных с этим переходом.

Вопросы, связанные с переходом на 5G, затрагивают множество заинтересованных сторон, и эти вопросы могут быть подняты как правительственными органами, так и частными компаниями и организациями, которые заинтересованы в успехе 5G. Они также могут привлечь внимание общественных организаций, экспертов и активистов, которые обеспокоены влиянием 5G на здоровье людей и окружающей среды. Кроме того, переход на 5G является важной стратегической и экономической задачей для ЕС. 5G может способствовать созданию новых рабочих мест и увеличению экономического роста, а также повышению конкурентоспособности европейских компаний. Развитие 5G-технологий открывает новые возможности для создания более эффективных и инновационных систем в различных областях. Например, в автономной технике, более быстрая и надежная связь между транспортными средствами и инфраструктурой может повысить безопасность дорожного движения и уменьшить количество аварий. В умных городах 5G может помочь в более эффективном управлении городской инфраструктурой, такой как уличное освещение, транспортная инфраструктура и т.д. В медицине 5G-технологии могут использоваться для создания более быстрых и надежных систем телемедицины, которые позволят удаленно обследовать и диагностировать пациентов, а также обмениваться данными между медицинскими учреждениями¹.

Разработка и внедрение новых технологий связи, таких как 5G, является одной из ключевых областей в настоящее время, особенно в Европейском Союзе (ЕС), который стремится обеспечить конкурентоспособность своих экономик на мировой арене. Однако переход на новые технологии связи также связан с рядом проблем и вызовов, которые могут повлиять на их успешную реализацию и использование.

¹ 5G Action Plan // An official website of the European Commission. [Б.м.], 2023. URL: <https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan> (дата обращения: 13.03.2023).

Сторонники сетей 5G утверждают, что они приведут к росту экономики и инноваций, а также откроют новые возможности в таких областях, как здравоохранение, транспорт и "умные города". Противники сетей 5G выражают опасения по поводу потенциальных рисков для здоровья, связанных с воздействием электромагнитного излучения, а также опасения по поводу конфиденциальности и кибербезопасности, связанных с большим объемом данных, которые будут генерировать сети 5G. Например, председатель Еврокомиссии, Урсула фон дер Ляйен выразила свою поддержку внедрению 5G в Европе в ходе своего выступления на Европейском цифровом саммите в 2019 году. Она отметила, что 5G может стать ключевым фактором для развития новых технологий и создания рабочих мест в Европе. Она также подчеркнула важность обеспечения безопасности и надежности 5G-сетей, чтобы предотвратить возможные угрозы для национальной безопасности и частной жизни людей. Другие поднимают вопросы о стоимости внедрения сетей 5G, а также о возможности возникновения цифрового разрыва между сообществами, имеющими доступ к 5G, и сообществами, не имеющими такого доступа. Некоторые политики выражают обеспокоенность геополитическими последствиями внедрения 5G, включая возможность получения иностранными государствами доступа к конфиденциальным данным и влияние на национальную безопасность. Таким образом, переход на 5G в Европейском союзе является важной и сложной задачей, которая требует внимания и участия многих заинтересованных сторон.

Все эти причины делают внедрение 5G в ЕС актуальной проблемой, требующей внимания и дальнейших исследований. Исследование данной проблемы является актуальным и важным, поскольку позволит более глубоко понять риски и препятствия, связанные с переходом на 5G в ЕС.

Основной исследовательский вопрос:

Какие проблемы связаны с переходом на технологию 5G в Европейском союзе, и как технологические и политические факторы влияют на достижение полного покрытия 5G в ЕС?

Цель исследования — Цель данной диссертации заключается в исследовании проблем, связанных с переходом на технологию 5G в Европейском Союзе, с учетом технологических и политических аспектов.

Задачи исследования:

1. Изучить регулирование для обеспечения полного покрытия 5G в ЕС.
2. Проанализировать проблемы, которые обсуждаются в ЕС в связи с переходом на 5G в ЕС.

3. Выявить, каким образом обсуждаемые проблемы влияют на процесс обеспечения полного покрытия 5G в ЕС.

Методологическая основа данного исследования состоит из общенаучных методов сравнения, анализа, синтеза и индукции, а также политологических методов системного и сравнительного анализа. Для проведения исследования также использовались экспликативные методы контент-анализа. Основой исследования является анализ большого объема нормативных и информационных источников, а также их дальнейшее исследование. Применение системного подхода позволило рассмотреть предмет и объект исследования в комплексе и установить взаимосвязь между политическими и технологическими аспектами внедрения 5G в ЕС.

Степень изученности темы.

Изучением описанных проблем 5G в Европейском Союзе занимаются различные организации и институты, включая Европейскую комиссию, национальные регуляторные органы связи, академические и научные учреждения, а также представители промышленности и бизнеса. Например, Европейская комиссия финансирует множество исследовательских проектов в области 5G через программы, такие как Horizon 2020 до 2020 года, после через Horizon Europe. Это флагманская программа Европейского Союза по исследованиям и инновациям, являющаяся частью долгосрочной многолетней финансовой программы ЕС (MFF) с бюджетом в 95,5 млрд. евро (включая 75,9 млрд. евро из MFF и 5 млрд. евро из Европы следующего поколения) в течение семилетнего периода (2021-2027 гг.).

Одним из ключевых механизмов для развития 5G до 2020 года был публично-частный партнерский проект 5G (5G PPP), который создан в рамках инициативы Европейского Союза по формированию стратегического исследовательского плана. Этот проект, который был активен в рамках Horizon 2020, объединил усилия промышленности, организаций исследований и Европейской комиссии для преобразования 5G в реальность. После 2020 года, в рамках программы Horizon Europe была запущена инициатива Smart Networks and Services (SNS), или "Умные сети и услуги". Целью этой инициативы является разработка и развертывание умных сетей следующего поколения, включая 6G, при сотрудничестве между промышленностью и научной общественностью. SNS сфокусирована на поиске решений, которые могут ускорить внедрение цифровых и

зеленых технологий, с тем, чтобы обеспечить европейскому обществу лучший доступ к усовершенствованным сетевым услугам².

Программа Horizon Europe также финансировала исследования и разработки в области 5G, и другие связанные проекты, которые способствовали развитию технологий 5G и их внедрению в различных секторах экономики, таких как умные города, здравоохранение, транспорт и многие другие.

В научной литературе часто изучаются следующие аспекты:

- Развитие новых технологий и стандартов для эффективного использования 5G³
- Разработка новых методов и алгоритмов для обработки и анализа больших объемов данных, которые могут быть собраны в сетях 5G⁴
- Оценка возможных рисков и проблем безопасности, связанных с использованием 5G, таких как кибератаки и проблемы конфиденциальности⁵
- Исследование социальных и экономических последствий перехода на 5G, включая анализ воздействия на экономику, занятость и повседневную жизнь людей⁶.

В шестом выпуске журнала European 5G Annual Journal более подробно рассматривается развитие 5G в ЕС. Журнал охватывает широкий спектр тем, связанных с развитием 5G в Европе, таких как стандарты 5G, развертывание сетей, применение 5G в разных отраслях, проблемы кибербезопасности, энергоэффективность и устойчивость 5G, государственно-частное партнерство для развития 5G, испытания и испытательные стенды 5G в Европе. В журнале подчеркивается необходимость инвестиций в инфраструктуру 5G, устранения рисков кибербезопасности и сотрудничества между различными заинтересованными сторонами для успешного внедрения технологии 5G.

²Call for future Clean Aviation partnership // official web site of European commission. [Б.м.], 2023. URL: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/call-future-clean-aviation-partnership-2020-08-26_en (дата обращения: 13.03.2023).

³Quliyev N. 5G TECHNOLOGIES ARE CREATING A NEW WORLD ORDER // Norwegian Journal of Development of the International Science. [Б.м.], 2023. URL: <https://cyberleninka.ru/article/n/5g-technologies-are-creating-a-new-world-order> (дата обращения: 13.03.2023).

⁴SURVEY ON ARTIFICIAL INTELLIGENCE TECHNIQUES IN 5G NETWORKS A. Abdellah1, A. Koucheryavy. [Б.м.], 2023. URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2020_1/1-10.pdf (дата обращения: 13.03.2023).

⁵Batalla, Jordi Mongay, et al. "Security risk assessment for 5G networks: National perspective." IEEE Wireless communications 27.4 (2020): 16-22. [Б.м.], 2023.

⁶Allam, Zaheer, and David S. Jones. "Future (post-COVID) digital, smart and sustainable cities in the wake of 6G: Digital twins, immersive realities and new urban economies." Land use policy 101 (2021): 105201.

Также рассказывается о влиянии COVID-19 на отрасль 5G и о том, как он повлиял на внедрение технологии 5G.

Данный журнал не делает окончательных выводов, но представляет мнения и обзоры экспертов и представителей отрасли, которые предлагают свои рекомендации по дальнейшему развитию технологии 5G в Европе. Однако можно выделить некоторые общие темы и вызовы, связанные с 5G, выявленные в публикациях данного журнала:

- Необходимость инвестирования в инфраструктуру 5G, включая поддержку развертывания сетей и устранение ограничений на спектр
- Увеличение устойчивости и энергоэффективности 5G сетей
- Решение проблем кибербезопасности 5G и защита данных пользователей
- Сотрудничество и согласование между заинтересованными сторонами для успешного развертывания технологии 5G в Европе
- Потенциал 5G для различных отраслей, таких как здравоохранение, автомобилестроение, транспорт и производство.

В целом, подчеркивается важность 5G для будущих инноваций и экономического роста в Европе, но также указывается необходимость продолжения работы над решением технических, экономических и регуляторных вызовов для достижения полного потенциала технологии⁷.

⁷The European 5G Annual Journal 2021. [Б.м.], 2023. URL: <https://bscw.5g-ppp.eu/pub/bscw.cgi/d424095/5G%20European%20Annual%20Journal%202021.pdf> (дата обращения: 13.03.2023).

Глава 1. Регулирование 5G в Европе: Исследование Полного Покрытия

Европейский союз (ЕС) - международная организация, которая осуществляет только те полномочия, которые ей предоставляют члены международной организации. Государства-члены являются основными обладателями этих полномочий. ЕС не обладает общими или неограниченными полномочиями, а лишь может осуществлять те функции, которые ему предоставлены в договорах. Распределение полномочий между ЕС и государствами-членами основано на принципе, согласно которому ЕС осуществляет в определенных областях, а другие полномочия остаются в компетенции членов Евросоюза. ЕС не имеет права осуществлять то что, не прописаны в Европейских Договорах⁸. Кроме того, существуют различные категории компетенций. Договор о функционировании ЕС устанавливает правовую систему компетенций в статьях с 2 по 6. Согласно этим правилам, у ЕС есть исключительные компетенции (ст. 2.1 и 3), совместные компетенции (ст. 2.2 и 4), координирующие компетенции (ст. 2.3 и 5) и поддерживающие, поощряющие или дополнительные компетенции (ст. 2.5 и 6). Различия между ними существенны.

1.1 Безопасность для обеспечения конфиденциальности и целостности данных

Безопасность в сетях 5G является одной из важных областей, которая затрагивает компетенцию Европейского союза (ЕС) и государств-членов. Хотя она не определена явно как отдельная компетенция в Договорах ЕС, ЕС обладает полномочиями в области регулирования электросвязи, информационных технологий и кибербезопасности, которые косвенно влияют на безопасность сетей 5G.

В рамках своих полномочий, ЕС разрабатывает и принимает нормативные акты, такие как директивы и регламенты, которые направлены на обеспечение безопасности сетей 5G. Например, Директива о сетях и информационной безопасности (Network and Information Security Directive) устанавливает требования к безопасности сетей и информационных систем в ЕС, включая сети 5G. Кроме того, ЕС имеет полномочия в области регулирования внутреннего рынка, включая электросвязь, и устанавливает правила и стандарты для обеспечения безопасности и конкурентоспособности сетей 5G внутри единого рынка.

⁸Garben, Sacha, and Inge Govaere, eds. The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future. Bloomsbury Publishing, 2017. [Б.м.], 2023. URL: https://books.google.ru/books?hl=en&lr=&id=XwMzDwAAQBAJ&oi=fnd&pg=PR5&ots=ENflu98uY7&sig=tEtDE13oNelW8Hpyc_WUBkEmpEo&redir_esc=y#v=onepage&q&f=false (дата обращения: 13.03.2023)

Основываясь на этих компетенциях, ЕС сотрудничает с государствами-членами и другими заинтересованными сторонами для разработки стратегий по обеспечению безопасности сетей 5G и предотвращения угроз. Фактически, безопасность 5G материально и поперечно затрагивает различные области, в которых ЕС имеет компетенцию, а также области, которые попадают в компетенцию государств-членов. Она особенно влияет на основное ядро деятельности ЕС, внутренний рынок, в трех основных областях:

- 1) правовой режим электронных коммуникаций.
- 2) положения о безопасности сетей и информационных систем.
- 3) последние нормативные акты о кибербезопасности.

Эти нормативные акты в настоящее время являются основой для действий ЕС в области 5G.

Анализ положений договоров и актов, принятых для их применения в этой конкретной сфере, показывает, что европейская политика в области безопасности сетей 5G не является результатом автономной политики, а является результатом сочетания этих трех регулятивных столпов. Однако каждый из этих столпов порождает свой собственный набор проблем.

Правовой режим электронных коммуникаций в настоящее время закреплён в Директиве (ЕС) 2018/1972, устанавливающей Европейский кодекс электронных связей (ЕЕСС)⁹. Это основной законодательный акт, касающийся внедрения 5G в Европейском Союзе (ЕС), он вступил в силу 11 декабря 2018 года. Европейский кодекс электронных связей (ЕЕСС) представляет собой унифицированный регулятивный инструмент для рынка электронных связей в Европейском Союзе (ЕС), который обновляет и заменяет ранее существовавшие регулятивные рамки. ЕЕСС устанавливает правила и рекомендации, касающиеся внедрения 5G, с целью развития единого цифрового рынка и стимулирования инноваций в области связи. ЕЕСС предоставляет ряд важных мер по защите прав потребителей. Эти меры направлены на обеспечение высокого качества услуг, прозрачности информации и гарантии, пользовательских прав, что является ключевым фактором для укрепления доверия потребителей к новым технологиям и стимулирования конкуренции на рынке. Одним из основных принципов защиты прав потребителей в рамках 5G является обеспечение высокого качества услуг. ЕЕСС требует от операторов предоставления надежных и быстрых услуг связи с минимальными

⁹European Electronic Communications Code // An official website of Body of European Regulators for Electronic Communications. [Б.м.], 2023. URL:<https://www.berec.europa.eu/en/berec/european-electronic-communications-code> (дата обращения: 16.03.2023).

задержками и потерями данных. Операторы должны регулярно мониторить и сообщать о своих показателях качества, обеспечивая прозрачность и возможность сравнения для потребителей. А также ЕЕСС обязывает операторов предоставлять понятную и полную информацию о своих услугах, тарифах и условиях использования, включая возможные ограничения и условия обслуживания. Это позволяет потребителям делать осознанный выбор при заключении договора и в дальнейшем контролировать качество услуг и стоимость их предоставления. В рамках ЕЕСС, потребители имеют право на перенос своего номера телефона при смене оператора, а также на прекращение договора без штрафных санкций и объяснения причин. Это обеспечивает гибкость и свободу выбора для потребителей и стимулирует операторов предлагать более выгодные условия и качественные услуги. ЕЕСС также предусматривает специальные меры защиты интересов уязвимых групп потребителей, таких как малоимущие домохозяйства, пожилые люди и люди с ограниченными возможностями. Операторы должны предоставлять специальные услуги и тарифы, обеспечивая доступность и доступ к сетям 5G для этих групп пользователей.

Согласно отчету о реализации¹⁰, включая Рекомендацию Европейской комиссии 2019/534 о кибербезопасности сетей 5G, действия Европейского союза вписываются в более широкую европейскую правовую базу для защиты сетей электронных коммуникаций и их экосистемы. Европейский кодекс электронных связей требует от всех поставщиков услуг электронных коммуникаций принимать соответствующие меры безопасности¹¹. Это означает, что ЕС определяет и устанавливает обязательные меры безопасности, которые должны принимать поставщики услуг электронных коммуникаций, включая сети 5G. Правовая база, предоставленная Европейским кодексом электронных коммуникаций, обеспечивает регулятивную рамку и требования для обеспечения безопасности сетей электронных коммуникаций в Европейском союзе.

В качестве правовой основы политики ЕС в отношении 5G, ЕЕСС поднимает два основных вопроса. Во-первых, это использование самой директивы в качестве регулирующего инструмента¹². В отличие от регламента ЕС, он оставляет за Штатами широкую свободу действий. Что наиболее важно, это подразумевает, что права и

¹⁰ Official Journal of the European Union. [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:321:FULL&from=IT> (дата обращения: 16.03.2023).

¹¹ Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks. [Б.м.], 2023. URL: https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf (дата обращения: 16.03.2023).

¹² Tsilikas, Haris. "Huawei v. ZTE in context—EU competition policy and collaborative standardization in wireless telecommunications." IIC-International Review of Intellectual Property and Competition Law 48.2 (2017): 151-178. [Б.м.], 2023. URL: <https://link.springer.com/article/10.1007/s40319-017-0560-7> (дата обращения: 16.03.2023).

обязанности физических и юридических лиц, компаний или пользователей предоставляется из внутреннего правила транспонирования, а не непосредственно из европейского, что может привести к различиям в условиях регулирования между разными государствами-членами. Вторая проблема норматива ЕЕСС заключается в том, что большинство государств-членов еще не перенесли эту директиву, не смотря на то что срок истек в 21 декабря 2020 года. В 6 апреля 2022 года Комиссия подала в суд, поскольку они не соблюдали свои обязательства и не транспонировали данный Европейский кодекс, что привело к нарушению прав многих из них. Эта ситуация создает значительную правовую неопределенность в ключевой момент для политики 5G¹³.

Законодательство, принятое в рамках Европейской Директивы 2016/1148 (известной как Директива NIS), направлено на создание безопасности информационных систем и сетей в Европейском Союзе¹⁴. Директива NIS устанавливает правила, которые должны следовать операторы основных услуг и поставщики цифровых услуг. Она сосредоточена на требованиях к безопасности и отчетности об инцидентах.

Вот только при попытке применить эти правила к технологии 5G возникают две проблемы. Во-первых, сейчас идет процесс пересмотра Директивы NIS, и текущие правила могут измениться. Это создает неуверенность в регулировании этой сферы.

Вторая проблема связана с тем, что в Директиве NIS говорится, что ее положения не применимы к компаниям, которые работают в сфере электронных коммуникаций. Это ставит под сомнение возможность применения требований Директивы NIS к сфере 5G, поскольку сама Директива исключает такую возможность. Так что здесь возникает юридический вопрос, который требует решения.

Закон о кибербезопасности - это законодательный акт, состоящий из двух частей. Первая часть связана с Европейским агентством по кибербезопасности, или ENISA (European Union Agency for Cybersecurity). Это агентство отвечает за укрепление кибербезопасности внутри Европейского Союза¹⁵.

Вторая часть связана с Европейской системой сертификации кибербезопасности. Это система, которая создает единые стандарты и процедуры для сертификации продуктов, процессов и услуг в области кибербезопасности в Европейском Союзе.

¹³ Commission opens infringement procedures against 24 Member States for not transposing new EU telecom rules // official web site of European commission [Б.м.], 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_206 (дата обращения: 16.03.2023).

¹⁴ OJEU, L 194, 19.07.2016, [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL> (дата обращения: 16.03.2023).

¹⁵ OJEU, L 151, 7.06.2019 [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2019%3A151%3ATOC> (дата обращения: 20.03.2023).

Тем не менее, в них есть два слабых места. Во-первых, она прогрессивная, что означает, что её реализация занимает много времени, так как она основана на постепенном усовершенствовании стандартов и процедур. Во-вторых, её добровольный характер означает, что участие в системе сертификации не является обязательным для компаний. Это может привести к тому, что некоторые компании могут выбрать не участвовать в системе, что в свою очередь препятствует созданию единых стандартов кибербезопасности на всей территории ЕС. В итоге, эти две проблемы не позволяют быстро достигнуть цели системы - создания единых, общепринятых стандартов кибербезопасности в Европейском Союзе.

На самом деле, из этих трех основных элементов, которые регулируют область кибербезопасности наиболее прочной правовой базой является Директива ЕЕСС, которая еще не была транспонирована во многих странах. Несмотря на то, что некоторые меры безопасности, предложенные в Директиве ЕЕСС, схожи с теми, что есть в Директиве NIS, они не являются идентичными. Например, критерии для определения серьезности инцидента, связанного с безопасностью, различны в этих двух директивах.

С точки зрения обеспечения безопасности, было бы полезно сделать требования этих двух директив более схожими, чтобы достичь максимального уровня безопасности и однородности требований во всех областях. Более того, хотя выполнение этих требований и обеспечение их соблюдения в обоих случаях имеют схожие механизмы, требования Директивы ЕЕСС строже. Тем не менее, текущая система законодательства ЕС в области кибербезопасности является недостаточной и сложной. К тому же, эти европейские законы не включают некоторые ключевые аспекты регулирования, которые характерны для технологии 5G. Но даже при этом, эти законы позволили создать европейский подход к безопасности 5G.

Стоит уделить внимание еще одному важному законодательному акту - Директиве по радиооборудованию (The Radio Equipment Directive, RED)¹⁶ Этот акт Европейского Союза, принятый в 2014 году и вступивший в силу 13 июня 2016 года, заменил предыдущую Директиву по радио и телекоммуникационному терминальному оборудованию (R&TTE Directive). В контексте 5G, Директива по радиооборудованию играет важную роль в обеспечении безопасности и надежности сетей нового поколения, а также защиты прав потребителей. Она гарантирует, что оборудование, используемое для развертывания 5G сетей, соответствует высоким стандартам безопасности, эффективности

¹⁶ Radio equipment // European Commission. [Б.м.], 2023. URL https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards/radio-equipment_en (дата обращения: 20.03.2023).

и экологической устойчивости, что в свою очередь способствует доверию пользователей к новым технологиям и услугам.

RED влияет на множество различных типов радиооборудования, от мобильных телефонов до Wi-Fi оборудования, радиоуправляемых игрушек и даже оборудования для 5G. Директива стремится обеспечить безопасное использование радиооборудования, защитить здоровье и безопасность пользователей, а также снизить воздействие на окружающую среду¹⁷. Производители радиооборудования, которые стремятся продавать свою продукцию в ЕС, должны убедиться, что их оборудование соответствует требованиям RED и проходит соответствующую процедуру оценки соответствия. В зависимости от типа оборудования и возможных рисков, процедура оценки может включать внутренний контроль производителя, испытания на соответствие стандартам или сертификацию со стороны уполномоченного органа.

Дополняя обсуждение регулирования в области кибербезопасности и связи в Европейском Союзе, стоит отметить Общий регламент защиты данных (General Data Protection Regulation, GDPR). Этот регуляторный инструмент, принятый в 2016 году и вступивший в силу 25 мая 2018 года, является ключевым в рамках обеспечения защиты личных данных граждан ЕС¹⁸. GDPR определяет правила обработки и передачи личных данных, предоставляя гражданам ЕС больше контроля над своей информацией и предусматривая серьезные штрафы для тех, кто нарушает эти правила¹⁹. В этом контексте, сети 5G представляют особый интерес, поскольку они обеспечивают возможность сбора и обработки огромного объема данных, включая личные данные пользователей. Развитие технологий, таких как интернет вещей (IoT), большие данные и машинное обучение, возможно благодаря 5G, что делает соблюдение GDPR еще более критически важным. Учитывая эти технологические новшества и масштабы обработки данных, необходимо гарантировать конфиденциальность и безопасность пользовательских данных в соответствии с требованиями GDPR.

GDPR устанавливает ряд принципов, которым должны следовать операторы и другие организации, обрабатывающие личные данные, такие как законность, справедливость, прозрачность, целевая ограниченность, минимизация данных, точность, ограничение хранения, целостность и конфиденциальность. А также требует, чтобы

¹⁷ DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL // Official Journal of the European Union. L 153/62. 22.5.2014. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=EN> (дата обращения: 20.03.2023).

¹⁸ О GDPR на русском // GDPR документы и материалы, на русском языке. [Б.м.], 2023. URL: <https://ogdpr.eu/ru> (дата обращения: 20.03.2023).

¹⁹ Data protection in the EU // European Commission. [Б.м.], 2023. URL: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (дата обращения: 20.03.2023).

пользователи были осведомлены о целях сбора и обработки их данных, а также имели возможность дать или отозвать свое согласие на такую обработку. Организации, обрабатывающие личные данные, должны применять соответствующие технические и организационные меры для обеспечения безопасности данных, а также защиты от случайных или неправомерных действий, таких как потеря, разглашение или искажение данных. Согласно Общему регламенту по защите данных (GDPR), на организации возлагается обязанность проведения оценки рисков. Это требование обусловлено необходимостью идентификации потенциальных угроз для защиты личных данных и определения мер, которые следует принять для минимизации этих рисков. Оценка рисков помогает организациям выявить уязвимые места в их системах защиты данных и разработать соответствующие стратегии для предотвращения нарушений конфиденциальности. В случае утечки данных, организации должны уведомить национальные органы по защите данных и затронутых пользователей в течение 72 часов после обнаружения инцидента²⁰.

После успешного прохождения процедуры оценки соответствия, производитель должен разместить на своем оборудовании маркировку CE, которая является доказательством соответствия требованиям RED и других применимых директив ЕС. Кроме того, производитель должен составить и сохранять техническую документацию, которая подтверждает соответствие продукции RED и предоставить ее на запрос национальных регуляторных органов, такие как Ofcom в Великобритании или Bundesnetzagentur в Германии, несут ответственность за контроль и надзор за соблюдением требований RED на своих территориях. Они могут проводить проверки, требовать предоставления документации и, в случае обнаружения нарушений, применять санкции, вплоть до изъятия оборудования с рынка.

1.2 Регуляторная надзорная структура

Регуляторная надзорная структура в области электронных связей и 5G в ЕС является многоуровневой и сложной системой, которая включает в себя как европейские, так и национальные органы. Эта структура была создана для обеспечения consistente регулирования, поддержки конкуренции, развития инфраструктуры и защиты интересов, как потребителей, так и предприятий. В основе этой структуры находятся национальные регуляторные органы, которые играют важную роль в обеспечении соблюдения

²⁰ What does the General Data Protection Regulation (GDPR) govern? // European Commission. [Б.м.], 2023. URL: https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en (дата обращения: 20.03.2023).

требований универсального обслуживания в рамках 5G. Они обязаны регулярно проводить проверки выполнения обязательств операторами, а также принимать меры для исправления любых выявленных нарушений и улучшения качества предоставляемых услуг на их территориях²¹.

Национальные регуляторные органы отвечают за регулирование связи и телекоммуникаций в странах Европейского союза [см. приложения А]. Они могут заниматься широким спектром областей, таких как телекоммуникации, энергетика, транспорт, финансы, здравоохранение, окружающая среда и многое другое. Цель этих органов - обеспечить справедливую конкуренцию, защиту прав потребителей, устойчивость и безопасность отрасли, а также соблюдение законов и регулятивных норм ЕС. Так, например, национальные регуляторные органы, такие как Ofcom в Великобритании или Bundesnetzagentur в Германии, обеспечивают регулирование и контроль над деятельностью операторов связи, включая обеспечение доступа к сетям, управление радиочастотным спектром и защиту прав потребителей.

Некоторые национальные регуляторные органы в ЕС тесно взаимодействуют с европейскими регуляторами и органами. Например, Европейская ассоциация регуляторов электронной связи (BEREC) объединяет национальные регуляторные органы из 27 стран ЕС и дополнительно отвечает за координацию их действий на уровне ЕС. BEREC объединяет представителей национальных регуляторных органов всех стран-членов ЕС, и его главная задача – координация их деятельности, разработка общих подходов и обмен лучшими практиками в области регулирования электронных связей.

Работа национальных регуляторных органов не ограничивается рамками отдельных стран. Они также активно сотрудничают с другими международными и региональными организациями, такими как Международный союз электросвязи (ITU), Европейский комитет по радиосвязи (CEPT) и Европейское агентство по кибербезопасности (ENISA), чтобы обеспечить координацию и согласованность политики на международном уровне. В дополнение к этому, национальные регуляторные органы тесно сотрудничают с Европейской комиссией и другими организациями в области гармонизации и оптимизации использования радиочастот для 5G, включая выделение и присвоение спектра, проведение аукционов и лицензирование²².

²¹ Telecommunications national regulatory authorities // An official website of the European Commission. [Б.м.], 2023. URL: <https://digital-strategy.ec.europa.eu/en/policies/telecommunications-national-regulatory-authorities> (дата обращения: 24.03.2023).

²² Geoffrey Myers Spectrum Auctions // LSE Press. [Б.м.], 2023. URL: <https://press.lse.ac.uk/site/books/m/10.31389/lsepress.spa/> (дата обращения: 24.03.2023).

Регуляторная надзорная структура играет значительную роль не только в контроле и регулировании, но также в поддержке исследований и разработок в области 5G и связанных с ними технологий. Национальные регуляторные органы (NRAs) активно сотрудничают с академическими и научно-исследовательскими организациями, а также с промышленным сектором, чтобы стимулировать инновации и создание новых продуктов и услуг, максимально использующих потенциал 5G.

Одной из ключевых целей регуляторной структуры является обеспечение здоровой конкуренции на рынке электронных связей, особенно по внедрению 5G в ЕС. Для этого NRAs мониторят деятельность операторов, которые предоставляют 5G и других участников рынка, чтобы предотвратить антиконкурентное поведение и обеспечить равные условия для всех компаний.

Еще одно особое внимание в рамках регуляторной надзорной структуры уделяется обеспечению доступа к высокоскоростному интернету для всех граждан ЕС, включая сельские и отдаленные районы²³. Это основывается на одном из ключевых принципов Европейского кодекса электронных связей, согласно которому все виды интернет-трафика должны обрабатываться равным образом, без дискриминации, ограничения или преимущества для определенных видов контента, приложений, услуг или устройств.

NRAs имеет значительную роль в управлении радиоспектром, координируя его использование на национальном уровне и сотрудничая с другими странами ЕС и Европейской комиссией для обеспечения оптимального распределения частот. Стоит отметить, что национальные регуляторные органы (NRAs) не только стимулируют инновации и поддерживают равноправие в сфере электронных связей, но также стимулируют инвестиции и развитие 5G-инфраструктуры на национальном уровне. В сотрудничестве с Европейской комиссией и другими организациями, NRAs фокусируются на поддержке развертывания оптоволоконных сетей, малых базовых станций и других ключевых компонентов 5G-сетей.

1.3 Роль финансирующих организаций в развитии 5G инфраструктуры в Европейском Союзе.

Развитие инфраструктуры 5G требует значительных инвестиций со стороны государств-членов, операторов и частных инвесторов. Европейский союз предоставляет

²³ BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules [Б.м.], 2023. URL: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules (дата обращения: 24.03.2023).

финансовую поддержку и стимулирует инвестиции в развитие 5G инфраструктуры через различные инициативы и программы, такие как The Connecting Europe Facility (CEF), Recovery and Resilience Facility (RRF), European Structural and Investment Funds (ESIF) и другие.

Механизм соединения Европы (The Connecting Europe Facility, CEF)²⁴ представляет собой ключевую программу финансирования Европейского союза, разработанную с целью инвестирования в стратегически важные инфраструктурные проекты в области транспорта, энергетики и цифровых сетей. Цель CEF - стимулировать экономический рост и укрепить внутренний рынок ЕС, способствуя развитию сетей, которые объединяют и поддерживают все 27 стран-членов²⁵.

CEF поддерживает проекты, которые способствуют созданию единой и безопасной цифровой инфраструктуры в ЕС. Программа финансирует проекты, которые обеспечивают трансграничное сотрудничество и развитие сетей 5G между странами-членами, что способствует созданию единого рынка для электронных связей²⁶. Оно предоставляет финансирование для развития и модернизации инфраструктуры 5G, включая выделение средств на развертывание сетей, обновление существующих сетей и разработку новых технологий, которые обеспечат высокоскоростной доступ и низкую задержку для пользователей²⁷. CEF принес множество преимуществ для граждан всех стран-членов, сделав путешествия более простыми и устойчивыми, улучшил энергетическую безопасность в Европе, позволил расширить использование возобновляемых источников энергии и упростил международное сотрудничество между государственными учреждениями, предприятиями и гражданами.

Помимо грантов, CEF предлагает финансовую поддержку проектам с помощью инновационных финансовых инструментов, таких как гарантии и проектные облигации. Эти инструменты создают значительные рычаги для использования ими бюджета ЕС и действуют как катализатор для привлечения дополнительного финансирования из частного сектора и других субъектов государственного сектора.

²⁴ About the Connecting Europe Facility // An official website of the European Union. [Б.м.], 2023. URL:https://cinea.ec.europa.eu/programmes/connecting-europe-facility/about-connecting-europe-facility_en (дата обращения: 27.03.2023).

²⁵ Connecting Europe Facility // European Commission. [Б.м.], 2023. URL:<https://wayback.archive-it.org/12090/20221222151902/https://ec.europa.eu/inea/en/connecting-europe-facility> (дата обращения: 27.03.2023).

²⁶ Там же.

²⁷ CEF Telecom // INNOVATION AND NETWORKS EXECUTIVE AGENCY. [Б.м.], 2023. URL:<https://wayback.archive-it.org/12090/20221222152013/https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom> (дата обращения: 27.03.2023).

- Первое поколение программы Connecting Europe Facility (CEF-1) «Телеком» (2014–2020 гг.) способствовало трансграничному взаимодействию между государственными администрациями, предприятиями и гражданами путем развертывания, среди прочего, инфраструктуры цифровых услуг (DSI). С бюджетом около 1 миллиарда евро, предназначенным для трансъевропейских сетей в телекоммуникационном секторе, из которых 203 миллиона евро в настоящее время находятся в ведении Европейского исполнительного агентства по здравоохранению и цифровым технологиям European Health and Digital Executive Agency (HaDEA), программа поддерживала два типа цифровых услуг:

1. Цифровые услуги многократного использования, которые можно интегрировать или комбинировать с другими проектами, охватывая электронную идентификацию, электронную подпись, электронные счета и электронную доставку.

2. Конкретные инфраструктуры цифровых услуг, охватывающие такие области, как кибербезопасность, электронное здравоохранение, Европейская платформа цифровых рабочих мест и навыков, система взаимосвязи коммерческих регистров, Еуроореана, электронные закупки, электронный обмен информацией о социальном обеспечении, общедоступные открытые данные, европейский портал электронного правосудия, более безопасный Интернет и разрешение споров онлайн.

- Второе поколение программы Connecting Europe Facility (программа CEF-2), «Цифровое» направление (2021–2027 гг.), направлено на поддержку и стимулирование инвестиций в инфраструктуры цифровой связи, представляющие общий интерес. Общий бюджет программы составляет 2 065 миллиардов евро, из которых 1,7 миллиарда евро находятся под управлением HaDEA. Действия, которые предполагается поддерживать в рамках CEF-2 Digital, включают:

1. Развертывание/доступ к сетям очень высокой пропускной способности, включая системы 5G, способные обеспечить гигабитную связь в районах, где расположены социально-экономические факторы, такие как школы, университеты, больницы, транспортные узлы, государственные администрации и т. д.;

2. Бесперебойное покрытие системами 5G на всех основных транспортных путях, включая трансъевропейские транспортные сети;

3. Развертывание новых или значительная модернизация существующих магистральных сетей, включая подводные кабели, как внутри/между государствами-членами ЕС, так и третьими странами;

4. Внедрение инфраструктур цифровой связи, связанных с трансграничными транспортными и энергетическими проектами, и/или поддержка операционных цифровых платформ, непосредственно связанных с этими инфраструктурами.

В рамках Европейского кодекса электронных связей предусматриваются различные меры и стимулы для поддержки инвестиций в высокоскоростные сети, такие как оптоволоконные сети и сети 5G²⁸. Кодекс предоставляет долгосрочную стабильность регулирования для инвесторов и операторов, устанавливая прозрачные и предсказуемые правила, которые позволяют участникам рынка лучше планировать свои инвестиции и стратегии развития, облегчая использование инфраструктуры и ресурсов между операторами и инвесторами, что позволяет снизить затраты на развертывание сетей и улучшить качество предоставляемых услуг. Это стимулирует сотрудничество операторов в развертывании и совместном использовании инфраструктуры, включая мачты, антенны и другие элементы сети, для повышения эффективности и окупаемости инвестиций. ЕЕСС обеспечивает гибкость в регулировании инвестиций в сети, позволяя учитывать особенности национальных рынков и технологические изменения. Индивидуализированные подходы к лицензированию и различные формы финансовой поддержки и стимулирования инвестиций могут быть применены. В дополнение к этому, ЕЕСС способствует доступ к финансированию для инвестиций в высокоскоростные сети, включая 5G, через взаимодействие с различными финансовыми институтами и программами, включая Европейский инвестиционный банк (EIB) и Европейский фонд стратегических инвестиций (EFSI)²⁹. Инициатива запущена, чтобы помочь преодолеть текущий дефицит инвестиций в ЕС путем мобилизации частного финансирования для стратегических инвестиций. На сегодняшний день более 2,2 миллиарда для проектов Next Generation Access Network (NGA).

Далее рассмотрим еще один из основных инструментов государственного финансирования 5G. Фонд восстановления и устойчивости RRF был предложен Европейской комиссией в 2020 году в рамках пакета мер для восстановления экономики Евросоюза после пандемии COVID-19. Он является ключевым элементом плана (NGA), основной целью которого является поддержка восстановления, повышение устойчивости и содействие "зеленой" и цифровой трансформации экономики ЕС.

²⁸ Directive (eu) 2018/1972 of the European parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code [Б.м.], 2023. [URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217) (дата обращения: 27.03.2023).

²⁹ Directive (eu) 2018/1972 of the European parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code [Б.м.], 2023. [URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217) (дата обращения: 27.03.2023).

Удаленное здравоохранение является одним из основных вариантов использования 5G. В этом смысле коронавирус очень своевременен. Для этого требуется видео UHD/VR/AR в режиме реального времени, поддерживаемое 5G благодаря малой задержке, очень высокой скорости и очень большой емкости. Вот почему Комиссия и государства-члены определили 5G в качестве ключевой области для инвестиций в Фонд восстановления и устойчивости (RRF). В июле 2020 года государства-члены согласовали пакет мер по восстановлению для смягчения последствий кризиса. Пакет называется NextGenerationEU (NGEU). Он включает 750 миллиардов евро в виде кредитов и грантов для членов ЕС. NGEU инвестирует в RRF 672,5 млрд. евро, из которых 360 млрд. евро — кредиты, а 312,5 млрд. евро — гранты. Из них, 20% всего бюджета (130 млрд. евро) были направлены на цифровые технологии. Horizon Europe получил дополнительно 5 миллиардов евро. RRF дополнит стратегические инвестиции и инвестиции в исследования и разработки программы Connecting Europe Facility (CEF) и программы Digital Europe. Кроме того, многие страны определили 5G как ключевой рычаг восстановления после пандемии. Во Франции, 5G является частью «Plan de Relance» в качестве стратегического направления для страны. В Германии 5G рассматривается как ключевой инструмент для ускорения мобильного покрытия и сокращения белых пятен.

Из основных инструментов финансирования в рамках ЕС, отметим важную роль Структурно-инвестиционных фондов ESIF. Они выделяют значительные суммы на поддержку различных сфер, в том числе 6 миллиардов евро на развитие цифровых сетей.

- Европейский региональный фонд (ERDF) - это один из этих фондов, который направлен на сокращение экономических и социальных различий между регионами ЕС. ERDF поддерживает региональное и городское развитие, финансируя проекты, направленные на повышение конкурентоспособности и улучшение качества жизни.

- Европейский сельскохозяйственный фонд развития сельских районов (EAFRD) - это фонд в рамках ESIF. EAFRD поддерживает стратегии ЕС в области сельского развития, включая поддержку устойчивого развития сельских территорий и улучшение эффективности аграрного сектора.

Европейское космическое агентство European Space Agency (ESA) и промышленные гиганты европейской космической сферы скооперировались для того, чтобы работать над созданием спутниковых систем для поддержки сетей 5G. Цель этих усилий - разработать и продемонстрировать ценность, которую спутниковые системы могут добавить в контексте 5G. Очевидно, что спутники могут дополнительно облегчить общеевропейское и глобальное покрытие, устойчивость, мобильность и безопасность для

предоставления услуг 5G, а также служить инструментом для реализации инновационной инфраструктуры и услуг. С учетом этого, приоритет будет отдан тем областям, где спутники могут внести значительный вклад, включая транспорт, средства массовой информации и развлечения, общественную безопасность, не исключая и другие подходящие области, и сценарии использования. Инициатива ESA Satellite 5G принимает активное участие в двух основных направлениях деятельности:

1. Разработка технологий, продуктов и проведение валидационных испытаний. Этот аспект работы ориентирован на создание интегрированной спутниковой наземной системы 5G или ее составляющих.

2. Разработка приложений и реализация вертикальных пилотных проектов. Этот сегмент деятельности направлен на создание и демонстрацию приложений и услуг, основанных на 5G и космических системах, в рамках пилотных проектов с участием потенциальных пользователей.

Помимо этих ключевых инструментов сотрудничество ЕС с международными партнерами, такими как International Telecommunication Union (ITU), European Conference of Postal and Telecommunications Administrations (CEPT) и другими организациями, для обмена опытом и знаниями в области инвестиций и развития сетей 5G. Это позволяет ЕС получать доступ к передовым мировым решениям и технологиям, а также сотрудничать с партнерами по разработке международных стандартов и стратегий для 5G и других технологий, включая регулирование радиочастотного спектра. Так как, Спектр - это ограниченный ресурс, который должен быть эффективно и справедливо распределен между странами и операторами связи. ITU играет центральную роль в международном координационном процессе, определяя международные правила использования спектра и нормы для беспроводных технологий.

1.4 Регулирование спектра в ЕС

Спектр радиочастот является одним из ключевых аспектов внедрения 5G, поскольку он определяет качество, пропускную способность и доступность беспроводных услуг. В Европейском кодексе электронных связей спектр радиочастот рассматривается как стратегический ресурс, который необходимо оптимизировать и эффективно использовать для обеспечения успешного внедрения 5G и развития единого цифрового рынка в ЕС.

Некоторые ключевые аспекты спектра, которые регулируются в рамках ЕЕСС:

1. Гармонизация спектра: ЕЕСС предусматривает гармонизацию радиочастотного спектра на уровне ЕС, что позволяет обеспечить более эффективное использование спектра и содействует созданию общего рынка для 5G-услуг. Гармонизация спектра означает согласованное использование определенных частотных диапазонов для 5G во всех странах-членах ЕС, что упрощает разработку и выпуск оборудования, снижает затраты и облегчает координацию между операторами.

2. Целевые частотные диапазоны: В соответствии со статьей 54 Европейской комиссии, государства-члены должны до 31 декабря 2020 года принять соответствующие меры для обеспечения развертывания 5G, включая реорганизацию и разрешение использования диапазона 3,4-3,8 ГГц и, по крайней мере, 1 ГГц диапазона 24,25-27,5 ГГц, при наличии рыночного спроса и отсутствии ограничений для миграции пользователей или расчистки диапазона. Эти диапазоны были выбраны из-за их способности предоставлять, высокую пропускную способность, низкую задержку и широкое покрытие. Целью является освобождение этих диапазонов во всех странах-членах ЕС к 2023 году для обеспечения широкомасштабного внедрения 5G.

3. Лицензирование и аукционы: ЕС разрабатывает общие подходы к лицензированию и аукционам спектра с целью обеспечения справедливого и эффективного распределения частотных ресурсов между операторами. ЕЕСС предусматривает прозрачные, недискриминационные и объективные процедуры для аукционов и лицензирования, что способствует конкуренции и обеспечивает равный доступ к радиочастотному спектру для всех участников рынка.

4. Эффективное использование спектра: ЕЕСС делает акцент на эффективное использование радиочастотного спектра, что включает в себя определение условий и технических характеристик для использования спектра, а также меры по предотвращению помех и оптимизации использования частот. Это может включать в себя совместное использование частот, динамическое распределение спектра и временное использование свободных частот для предоставления услуг 5G³⁰.

5. Продление и обновление лицензий: ЕЕСС предусматривает механизмы для продления и обновления лицензий на использование спектра, что позволяет операторам и инвесторам лучше планировать свои инвестиции в инфраструктуру и развитие сетей. Кодекс также предоставляет регуляторам возможность адаптировать условия лицензирования в соответствии с развитием технологий и изменениями на рынке.

³⁰ Directive (eu) 2018/1972 of the European parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code [Б.м.], 2023. [URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217) (дата обращения: 27.03.2023).

Управление спектром радиочастот в рамках Европейского кодекса электронных связей направлено на обеспечение эффективного и согласованного использования радиочастотного спектра для 5G в ЕС.

Европейский кодекс электронных коммуникаций устанавливает общие принципы управления использованием радиочастотного спектра. Государства-члены должны способствовать гармонизации спектра и обеспечивать его эффективное и действенное использование. В этом контексте трансграничная координация использования радиочастотного спектра между Государствами-Членами является ключевым элементом эффективного управления радиочастотным спектром и необходима для надлежащего функционирования внутреннего рынка.

Европейская комиссия отвечает за разработку и внедрение политики ЕС в области электронных связей, включая 5G. Она также тесно сотрудничает с национальными регуляторными органами, разрабатывая общие правила, и координирует работу по гармонизации спектра и использованию радиочастот. Чтобы помочь Комиссии, были созданы два взаимодополняющих органа для содействия консультациям, а также для разработки и поддержки политики ЕС в отношении радиочастотного спектра:

- Группа политики в отношении радиочастотного спектра (RSPG) представляет собой группу высокопоставленных национальных правительственных экспертов, помогающих Комиссии в разработке общей политики в отношении радиочастотного спектра на уровне ЕС.
- Комитет по радиочастотному спектру (RSC) помогает Комиссии в разработке технических мер по реализации для обеспечения согласованных условий по всей Европе для доступности и эффективного использования радиочастотного спектра.

Спектральное обеспечение для нового поколения сотовых технологий всегда является сложной задачей. Однако, благодаря инновационному процессу "5G pioneer bands", предложенному EURO-5G, научное сообщество принять участие в дебатах о спектре и определить гармонизированные диапазоны, идеально соответствующие рыночным потребностям и стандартам пятого поколения технологий.

С самого начала Радиокomitee по спектру (RSPG) ставил перед отраслью задачу определить проблему, которую необходимо решить для 5G. EURO-5G ответил на этот строгий подход документами для рабочей группы по спектру 5G Инфраструктурной ассоциации (5G IA), которые показали, что одного диапазона 5G недостаточно для удовлетворения различных будущих потребностей рынка, как по емкости, так и по охвату.

RSPG и Европейская комиссия были открыты для подхода с использованием "пионерских" диапазонов, и во мнении RSPG Европейского союза появились три таких диапазона³¹:

- Низкий диапазон 700 МГц,
- Средний диапазон 3,4 - 3,8 ГГц (диапазон 3,6 ГГц).
- Высокий диапазон 24,25 - 27,5 ГГц (диапазон 26 ГГц)

Доступ к спектру является одним из самых важных ключей к успешному развитию 5G. Это подчеркивается как на европейском³², так и на международном³³ уровнях. Соответствующие глобально гармонизированные частотные диапазоны должны быть доступны в нужное время, а также должны учитываться аспекты управления и разрешения использования. Они должны соответствовать потребностям рынка, а также стандартам развивающихся технологий 5G. Одним из глубоких изменений, которые происходят, является введение в использование новых диапазонов в мм-волновой области радиочастотного спектра. Эти диапазоны имеют радикально отличающиеся технические и экономические характеристики из-за очень низкого дальнего действия, по сравнению с диапазонами, которые использовались для предоставления мобильных услуг национального уровня. Новые более высокие диапазоны предлагают возможности более широких радиоканалов и огромных прыжков в емкости и скорости передачи данных. Но это имеет свою цену. Стоимость охвата городов, городских поселений и целых стран этими мощными системами становится непосильной. Это создает новую ситуацию в эпоху 5G, когда один диапазон уже не может решить каждую проблему [см. приложения Б].

Общими словами, использование спектра частот является одним из наиболее важных факторов успеха 5G. На этот факт обращается внимание, как на европейском, так и на международном уровне. Глобально-гармонизированные частотные диапазоны должны быть доступны в нужное время, а также должны управляться соответствующими разрешениями. Они должны быть соответствовать потребностям рынка, а также новым стандартам технологии 5G. В связи с этим, одним из ключевых изменений, происходящих сейчас в 5G, является введение новых диапазонов частот в миллиметровом диапазоне

³¹Euro-5g – Supporting the European 5G Initiative [Б.м.], 2023. URL: https://5g-ppp.eu/wp-content/uploads/2017/10/Euro-5G-D5.4_Spectrum_for_5G_v1.0.pdf (дата обращения: 27.03.2023).

³²ЕС, 5G Action Plan [Б.м.], 2023. URL: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131 (дата обращения: 27.03.2023).

³³ITU-R, IMT Vision - Framework and overall objectives of the future, development of IMT for 2020 and beyond, Recommendation M.2083 [Б.м.], 2023. URL: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf (дата обращения: 27.03.2023).

радиочастот. Новые высокочастотные диапазоны предлагают возможности для более широких радиоканалов и значительных увеличений емкости и скорости передачи данных. Однако использование этих диапазонов ограничено, их покрытие ограничено, и стоимость покрытия такими системами в городах, городках и странах становится запретительной. В этой связи, EURO-5G внес значительный вклад в более глубокое понимание новых технических и экономических вызовов, с которыми столкнулась Европа при рассмотрении вопроса о спектральных диапазонах для 5G.

Данный документ также предоставляет обзор результатов деятельности 5G PPP, рабочей группы (WG) 5G Spectrum при 5G IA и проектов, которые внесли свой вклад в вопросы спектра. Рабочая группа занималась вопросами раннего доступа к частотным диапазонам и некоторыми аспектами управления ими. Проекты 5G PPP, внесшие свой вклад в спектр, указанные в таблице 1.

Таблица 1. Проекты 5G-PPP

Проекты	Содействие в вопросах спектра 5G
5G-Crosshaul	Предложили интегрированные беспроводные опции фронт-хола и бэк-хола в частотных диапазонах до 100 ГГц, особое внимание уделяется диапазону от 50 до 90 ГГц.
5G-XHaul	Фокусировались на использовании диапазона 60 ГГц для бэк-хола и фронт-хола.
COHERENT	Предложили схемы управления общим спектром
EURO-5G	Оказали поддержку и возглавили рабочую группу по спектру 5G.
METIS-II	Разработали требования к спектру и технические аспекты спектра.
mmMAGIC	Предложили спектр выше 6 ГГц, включая мм-волны, для мобильной связи 5G и само обратной связи.
SPEED-5G	Предложили динамический доступ к спектру для нескольких технологий радиодоступа.

Источник: Журнал T-Comm - Телекоммуникации и Транспорт³⁴

³⁴Данешманд Бехруз Мехди СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОНЦЕПЦИИ СОЗДАНИЯ И РАЗВИТИЯ СЕТЕЙ 5G/IMT-2020 В РОССИИ, КИТАЕ, США И ЕВРОПЕ // T-Comm. 2021. №6. URL: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-kontseptsii-sozdaniya-i-razvitiya-setey-5g-imt-2020-v-rossii-kitae-ssha-i-evrope> (дата обращения: 06.06.2023).

Таким образом, внедрение 5G технологий осуществляется под руководством многочисленных активистов, включая рабочие группы, национальные регуляторные органы, академические и научные учреждения, промышленность и малый и средний бизнес³⁵. Ключевыми аспектами этой работы являются управление и доступ к частотным диапазонам, а также поддержка исследований и разработок в области 5G. Для достижения этих целей национальные регуляторные органы Европейского Союза активно сотрудничают в рамках проектов и поддерживают исследовательские проекты и инновации, направленные на создание новых технологий и решений для сетей 5G. Этот общеевропейский процесс обладает уникальной спецификой в каждой из стран ЕС, отражая особенности и потребности конкретных национальных рынков.

1.5 Вклад национальных регуляторных органов в странах ЕС

Как и в предыдущих разделах было упомянуто все национальные регуляторные органы, они играют важную роль в контроле и обеспечении соблюдения требований универсального обслуживания в рамках 5G. Они регулярно проверяют выполнение обязательств операторами, поддерживают исследовательские проекты, инновации, а также принимает меры для исправления любых нарушений и улучшения качества услуг для граждан ЕС. Предотвратить анти-конкурентное поведение и обеспечить равные условия для всех компаний. Ниже рассмотрим более детально несколько примеров.

Германия активно участвует в разработке и развертывании сетей 5G. Федеральное сетевое агентство (BNetzA) отвечает за регулирование телекоммуникационного сектора в Германии, включая выделение радиочастот для сетей 5G³⁶. В 2019 году правительство Германии ввело новые требования безопасности для сетей 5G, включая исключение некоторых поставщиков из сетевой инфраструктуры, чтобы решить проблемы национальной безопасности³⁷. Правительство также запустило национальную стратегию развития сетей 5G³⁸, которая направлена на содействие развертыванию инфраструктуры

³⁵ Там же.

³⁶ Bundesnetzagentur // An official website of BNetzA. [Б.м.], 2023. URL:https://www.bundesnetzagentur.de/EN/Home/home_node.html (дата обращения: 05.04.2023).

³⁷ New security rules for the 5G roll-out to ensure network security // BMWK JOINT PRESS RELEASE. 2019. URL:<https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2019/20191015-new-security-rules-for-the-5G-roll-out-to-ensure-network-security.html> (дата обращения: 05.04.2023).

³⁸ Making 5G a success in Germany // Federal Ministry of Transport and Digital Infrastructure. [Б.м.], 2018. URL:<https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/5G%20Greece/Session%201%20Franziska%20SchillGERMANY%20-%20Making%205G%20Sa%20success%20in%20Germany.pdf> (дата обращения: 05.04.2023).

5G и поддержку разработки новых сценариев использования и инновационных приложений. Стратегия включает такие меры, как инвестиции в исследования и разработки, развертывание испытательных стендов и пилотных проектов, а также поддержка разработки новых бизнес-моделей, ориентированных на 5G. Германия также является родиной некоторых ведущих телекоммуникационных компаний Европы, таких как DeutscheTelekom и VodafoneGermany, которые активно участвуют в разработке и развертывании сетей 5G в стране.

Во Франции за регулирование телекоммуникационного сектора, включая сети 5G, отвечает Орган по регулированию электронных коммуникаций и почтовых услуг (ARCEP)³⁹. В 2020 году Франция ввела новые требования к развертыванию сетей 5G, включая обязательство операторов совместно использовать инфраструктуру, чтобы снизить воздействие развертывания 5G на окружающую среду. Правительство Франции также запустило национальную стратегию развития сетей 5G, которая включает такие меры, как финансирование исследований и разработок, развертывание испытательных стендов и пилотных проектов, а также поддержку разработки новых сценариев использования и инновационных приложений. Франция, как и другие страны ЕС, также решает проблемы национальной безопасности, связанные с сетями 5G, и принимает такие меры, как усиление проверки поставщиков оборудования и ограничения на использование определенных поставщиков в сетевой инфраструктуре. Правительство Франции также подчеркнуло необходимость регионального и международного сотрудничества в развитии сетей 5G для обеспечения совместимости и решения проблем безопасности и конфиденциальности⁴⁰.

В Польше Управление электронных коммуникаций (UKE) отвечает за регулирование телекоммуникационного сектора, включая сети 5G⁴¹. Польское правительство запустило национальную программу поддержки разработки и развертывания сетей 5G⁴², которая включает финансирование исследований и разработок, пилотных проектов и развертывания инфраструктуры. Программа также направлена на развитие сотрудничества между правительством, частным сектором и научными кругами

³⁹ ARCEP Homepage // An official english website of ARCEP. [Б.м.], 2023. URL:<https://en.arcep.fr/> (дата обращения: 05.04.2023).

⁴⁰ 5G REGULATION AND LAW IN FRANCE // CMS Expert Guides. [Б.м.], 2023. URL:<https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/france> (дата обращения: 09.04.2023).

⁴¹ Office of Electronic Communications // UKE. [Б.м.], 2023. URL:<https://uke.gov.pl/en/> (дата обращения: 09.04.2023).

⁴² Broadband in Poland // An official website of the European Union. [Б.м.], 2023. URL:<https://digital-strategy.ec.europa.eu/en/policies/broadband-poland> (дата обращения: 09.04.2023).

для использования всего потенциала технологии 5G в Польше. В дополнение к национальной программе Польша также работает над решением проблем национальной безопасности, связанных с сетями 5G, и приняла такие меры, как усиление проверки поставщиков оборудования и ограничения на использование определенных поставщиков в сетевой инфраструктуре. Польское правительство также подчеркнуло необходимость регионального и международного сотрудничества в развитии сетей 5G для обеспечения совместимости и решения проблем безопасности и конфиденциальности.

В Италии Министерство экономического развития и Управление по регулированию связи (AGCOM)⁴³ регулируют телекоммуникационный сектор, включая сети 5G. Правительство Италии запустило национальный план по поддержке развития сетей 5G⁴⁴, который включает финансирование развертывания инфраструктуры, исследований и разработок, а также разработку новых услуг и приложений. Национальный план также направлен на содействие внедрению технологии 5G в ключевых секторах экономики, таких как производство, транспорт и сельское хозяйство, для стимулирования инноваций и повышения производительности. В дополнение к национальному плану Италия также работает над решением проблем национальной безопасности, связанных с сетями 5G, и приняла такие меры, как более тщательная проверка поставщиков оборудования и ограничения на использование определенных поставщиков в сетевой инфраструктуре. Италия также уделяет большое внимание необходимости международного сотрудничества и взаимодействия в развитии сетей 5G и тесно сотрудничает с другими странами-членами ЕС и международными организациями для продвижения развертывания технологии 5G через границы.

1.6 Общая характеристика регулирования 5G в Европейском Союзе

ЕС признает наличие проблемы национальной безопасности для государств-членов, а также стратегическую ценность 5G для Союза в целом. Но у него нет ни средств, ни компетенций, чтобы вступать в такую конкуренцию с мировыми лидерами в области технологий 5G. Государствам-членам ЕС не хватает технологической базы и всех необходимых полномочий для самостоятельного управления 5G, поскольку некоторые из необходимых полномочий были переданы ЕС или могут повлиять на компетенции ЕС.

⁴³ Home - AGCOM // An official website of the AGCOM. [Б.м.], 2023. URL:<https://www.agcom.it/> (дата обращения: 09.04.2023).

⁴⁴ Broadband in Italy // An official website of the European Union. [Б.м.], 2023. URL:<https://digital-strategy.ec.europa.eu/en/policies/broadband-italy> (дата обращения: 09.04.2023).

Более того, ни одно отдельное государство не может иметь такие же возможности и потенциал для реагирования на эту проблему и на давление третьих государств, как скоординированные действия всех стран в рамках ЕС.

С момента принятия Плана действий по 5G в 2016 году и на основе полномочий, предоставленных ЕС в области электронных коммуникаций, сетевой и системной безопасности, кибербезопасности и сертификации, европейская политика 5G постепенно формировалась. Анализ этого процесса, его природы и особенностей, вовлеченных субъектов и мер, принимаемых для достижения его целей, позволяет сделать некоторые выводы в отношении трех основных вопросов, рассматриваемых в данном исследовании.

Задача достижения технологической автономии и цифрового суверенитета стала приоритетом в ЕС и постоянно подтверждается государствами-членами и институтами ЕС. Эта цель связана с ЕС, а не с его государствами-членами в отдельности, тот факт, что это общая, европейская, а не национальная или индивидуальная цель, имеет огромное значение. Это признание приверженности европейским действиям, несмотря на то, что это вопрос компетенции государства. В то время как государства по-прежнему апеллируют к своему суверенному статусу в физическом мире в традиционном понимании, идея цифрового суверенитета связана с деятельностью ЕС.

Определившись с предпочтением совместных европейских действий, необходимо определить модель организации европейской и национальной компетенций. Согласно статье 2 Договора о функционировании Европейского Союза, ЕС может осуществлять различные виды полномочий, начиная от исключительных или общих полномочий и заканчивая координирующими полномочиями или поддерживающими, продвигающими и дополняющими полномочиями. Среди этих вариантов координация национальной политики является методом, выбранным для 5G. Модель исключительных или общих полномочий не обязательно будет лучшим вариантом, учитывая, что для многих государств-членов это вопрос безопасности и национальных интересов. Кроме того, координация национальной политики оказалась эффективным и оперативным, а также реалистичным методом в других областях, имеющих особое значение, таких как экономическая, политики занятости.

Таким образом, ЕС обладает компетенцией координировать национальную политику государств-членов в отношении 5G. Другими словами, ЕС не может издавать законы или принимать юридически обязывающие акты в области 5G, поскольку это является обязанностью государств-членов. Однако государства-члены связаны моделью координации, установленной на европейском уровне для определения, реализации и оценки мер, принятых в этой области.

Европейскую модель 5G можно четко и прозрачно объяснить, разграничив регулирующие правовые обязанности государств и координирующие правовые обязанности ЕС. Правила и акты, имеющие юридические последствия для третьих сторон, являются ответственностью отдельных государств-членов. Цели, предметы, меры, процедуры и инструменты являются результатом европейской координации, в основном посредством норм «мягкого права», которые включают как этап программирования, так и оценку результатов.

Однако, несмотря на предложенную модель координации на европейском уровне, проблемы и вызовы остаются. Учитывая, что по Договору о функционировании ЕС, ЕС не обладает исключительными или общими полномочиями в области 5G, существует риск неконсистентности и неоднородности в подходах к внедрению 5G на территории ЕС, так как процесс внедрения 5G в Европейском Союзе представляет собой сложное переплетение технических и политических аспектов, которые предъявляют как вызовы, так и возможности.

Это подчеркивает необходимость дальнейшего анализа и обсуждения этой темы, с целью дать точную характеристику перспектив и проблем при переходе на 5G, который отвечает интересам всех государств-членов и их граждан.

Глава 2. Анализ проблем и вызовов при переходе на 5G в ЕС

2.1 Технологические аспекты перехода на 5G в ЕС

Прежде всего, стоит определить уникальность сети пятого поколения её характеристики и возможности. Технологии развиваются благодаря непрерывному прогрессу и опираются на инновационные решения, впервые примененные в предыдущих поколениях технологий. В этом контексте одним из последних и значимых достижений в области беспроводной коммуникации стало внедрение 5G. Пятое поколение беспроводных сетей развивалось как решение проблем, с которыми столкнулись предыдущие поколения, и одновременно как совершенствование существующих технологий. Например, первое поколение сетей (1G) использовалось и продолжает использоваться для аналоговых голосовых услуг, достигая скорости передачи данных до 2,4 кбит/с. Оно работает на аналоговых частотах, используя многоканальный доступ по частотному разделу Frequency Division Multiple Access (FDMA) и полосу радиосвязи. В свою очередь, второе поколение сетей (2G) начало использовать цифровые технологии, такие как многоканальный доступ по временному разделу Time Division Multiple Access (TDMA) и многоканальный доступ по кодовому разделу Code Division Multiple Access (CDMA). Глобальная система мобильной связи Global System for Mobile communications (GSM) объединила эти две цифровые технологии. Также была представлена улучшенная сеть 2G+, которая использует высокоскоростную коммутацию данных, общий пакетный радиосервис и усовершенствованные скорости передачи данных для глобальной эволюции. Третье поколение сетей (3G) объединяет несколько технологий 2G, таких как CDMA, GSM и TDMA, в единую систему, которая позволяет достигать большей скорости передачи данных, чем 1G и 2G, обеспечивая возможность для видео звонков и потокового видео. Четвертое поколение мобильных сетей (4G) использует стандарт долгосрочной эволюции Long Term Evolution (LTE). Он представляет высококачественную передачу видео и быстрый доступ к мобильному интернету⁴⁵.

И наконец, технология 5G представляет собой революционный шаг в развитии мобильной связи, способную удовлетворить потребности, как отдельных пользователей, так и крупных предприятий⁴⁶. Это достигается за счет использования модульных сетевых

⁴⁵ 1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G [Б.м.], 2023. URL: <https://net-informations.com/q/diff/generations.html> (дата обращения: 12.04.2023).

⁴⁶ From 1G to 5G: A Brief History of the Evolution of Mobile Standards // Brainbridge Workforce Solutions [Б.м.], 2023. URL: <https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards> (дата обращения: 12.04.2023).

функций, которые обеспечивают гибкость и экономическую эффективность, при этом оставаясь масштабируемыми для поддержки широкого спектра сценариев использования. Данный подход позволяет 5G поддерживать различные варианты использования, от Интернета вещей и умных городов до тактильных вычислений и голографических взаимодействий. Это подтверждает фундаментальное изменение парадигмы беспроводной мобильной связи, которое происходит благодаря внедрению 5G. Эта технология не только усиливает возможности текущего поколения связи, предлагая более высокую пропускную способность и меньшую задержку, но и открывает двери для принципиально новых приложений, отвечая более строгим требованиям к задержке и пропускной способности. Это обеспечивается за счет использования нового спектра и увеличения спектральной эффективности, что позволяет преодолеть так называемую "проблему последней мили".

В Таблице 2 приведены особенности всех беспроводных стандартов.

Таблица 2. Особенности беспроводных стандартов⁴⁷

Особенности	1G	2G	3G	4G	5G
Технология	AMPS, NMT, TACS	GSM	WCDMA	LTE, WiMax	MIMO, миллиметровые волны
Частота	30 кГц	1.8 ГГц	1.6-2 ГГц	2-8 ГГц	3-30 ГГц
Пропускная способность	2 кбит/с	14.4 - 64 кбит/с	2 Мбит/с	2000 Мбит/с до 1 Гбит/с	1 Гбит/с и выше
Система доступа	FDMA	TDMA/CDMA	CDMA	CDMA	OFDM/BDMA
Ядро сети	PSTN	PSTN	Пакетная сеть	Интернет	Интернет

Пятое поколение беспроводной связи предлагает три преимущества по сравнению с предыдущим поколением 4G:

- Большую скорость
- Большую отзывчивость (низкую задержку)
- Больше пропускной способности для подключения к большому числу устройств

⁴⁷ 5G revolution: Challenges and opportunities developments // official web site of IEEE Xplore [Б.м.], URL: <https://ieeexplore.ieee.org/document/9668550> (дата обращения: 27.04.2023).

Эта технология имеет значительный экономический потенциал в различных областях, таких как производство, розничная торговля и здравоохранение. Ожидается, что к 2035 году во всем мире будет влиито 13,2 триллиона долларов капитала. Возможности, предусмотренные для этой технологии, бесчисленны, начиная от поддержки автономных автомобилей, удаленных операций в здравоохранении, умных городов, домов и действительно всемирной связи до устройств и Интернета вещей (IoT).

Кроме того, технология 5G более эффективно использует энергию по сравнению с предыдущими поколениями. Следовательно, развертывание 5G в городах, домах и на предприятиях снизит энергопотребление сети, способствуя обезуглероживанию и, в конечном счете, устойчивым практикам.

Таким образом, технология 5G играет важную роль в более широкой стратегии Европейского союза по цифровой трансформации его экономики и общества. Эта технология становится основой для развития ряда отраслей, включая промышленность 4.0, автоматизированное вождение, смарт-города, электронное здравоохранение и сельское хозяйство. Благодаря своей способности поддерживать массовое соединение устройств и обеспечивать высокую скорость передачи данных, 5G открывает новые возможности для инноваций и прогресса в этих областях. Улучшение доступа к сети во всех уголках Европы также является ключевой целью 5G. В районах, где до сих пор не было достаточного покрытия, 5G обещает предоставить высокоскоростной интернет, расширяя возможности и уровень жизни для людей, проживающих в этих местах. С этой точки зрения, 5G играет важную роль в обеспечении цифрового равенства на всей территории Европейского союза. Более того, 5G имеет большой потенциал для стимулирования экономического роста в ЕС. Он может улучшить производительность, увеличить гибкость предприятий и способствовать инновациям, создавая новые рабочие места и способствуя экономическому росту. Это, в свою очередь, ведет к улучшению качества жизни для граждан Европейского союза и увеличению общей экономической процветаемости региона. С точки зрения стратегической автономии, для Европейского союза важно иметь надежную и безопасную инфраструктуру 5G. Это важно не только для обеспечения безопасности данных граждан и компаний ЕС, но и для поддержания стратегической независимости в мире, где цифровые технологии становятся все более центральными. 5G также может играть ключевую роль в достижении целей устойчивого развития ЕС. Способность технологии поддерживать умные инфраструктуры, такие как умный транспорт и умная энергетика, может помочь снизить выбросы углерода и способствовать более устойчивому обществу.

В общем, 5G не просто новая технология для Европейского союза. Это ключевой инструмент для содействия цифровой трансформации, социально-экономического развития, стратегической автономии и устойчивости, делая его важной частью будущего ЕС. Однако, несмотря на все эти преимущества, важно помнить, что технология 5G также столкнется с серьезными препятствиями на пути своего развертывания, особенно в контексте Европейского Союза. К ним относятся не только технические проблемы, но и политические факторы.

Технология 5G представляет собой новый стандарт телекоммуникаций. Она может использоваться совместно с рядом других технологий, таких как гетерогенные сети Heterogeneous Networks (HetNets), коммуникация Device-to-Device (D2D), программно-определенные сотовые сети Software-Defined Networking (SDN), массивная система множественного ввода/вывода Multiple-Input Multiple-Output (MIMO), 3D MIMO, Проект партнерства третьего поколения (3GPP) и коммуникация Machine-to-Machine (M2M) ⁴⁸.

Несмотря на то, что эти технологии предлагают множество преимуществ, они также несут в себе множество потенциальных вызовов. В результате, ряд исследователей точно описали несколько вызовов, связанных с ними. Кроме того, как и в предыдущих поколениях, ряд проблемы возникает и при внедрении такие как проблемы со спектром и т.д.

2.2 Проблемы со спектром.

Проблемы со спектром в контексте 5G связаны с ограниченностью доступного радиочастотного спектра и необходимостью увеличения его объема для поддержки более высокой пропускной способности и скорости передачи данных в сетях 5G.

Предыдущие поколения мобильной связи использовали определенные диапазоны радиочастотного спектра, например, от 1340 до 1960 МГц. Однако для технологии 5G ожидается значительное увеличение пропускной способности и скорости передачи данных. Это требует большего объема доступного спектра и более широких полос пропускания для обеспечения эффективной работы сетей 5G.

Однако расширение спектра для 5G сталкивается с несколькими проблемами. Во-первых, доступ к новым частотным диапазонам требует согласования с регулирующими

⁴⁸ Woon Hau Chin, Zhong Fan, and Russell Haines. Emerging Technologies and Research Challenges for 5G Wireless Networks [Б.м.] (дата обращения: 12.04.2023). 2023.URL:https://www.researchgate.net/publication/260393079_Emerging_Technologies_and_Research_Challenges_for_5G_Wireless_Networks (дата обращения: 12.04.2023).

органами и координации между различными операторами связи. Во-вторых, выделение дополнительного спектра может быть ограничено из-за уже существующих использований спектра другими службами и системами. Также стоимость спектра является значительной проблемой, особенно для развивающихся стран.

Для успешного развертывания 5G потребовалось ЕС разработать стратегии гармонизации спектра, оптимизировать использование доступного спектра, провести исследования и разработки новых технологий и методов управления спектром, а также провести переговоры с национальными регуляторными органами и другими заинтересованными сторонами для согласования и выделения необходимого спектра для 5G.

Надо отдельно отметить на счет стоимости спектра, которая является серьезной проблемой при развертывании 5G сетей. Она может значительно варьироваться в зависимости от страны и ее экономического статуса. В развивающихся странах стоимость спектра для 5G может быть выше, чем в развитых странах.

Одна из причин высокой стоимости спектра для развивающихся стран заключается в том, что для них существует большая потребность в инвестициях в инфраструктуру и развитие связи. Они могут столкнуться с ограниченными ресурсами и финансовыми возможностями, что делает выделение средств на приобретение спектра более сложным.

Стоимость спектра также может быть зависима от конкуренции на рынке связи. Если на рынке есть ограниченное число операторов связи, спрос на спектр может быть высоким, что приводит к повышению цен на его приобретение.

Для развивающихся стран, столкнувшихся с высокой стоимостью спектра, возможны различные подходы для смягчения этой проблемы. Например, они могут привлекать частные инвестиции, предлагать гибкие платежные условия или применять субсидирование и содействие со стороны правительства. Также возможны договоренности о снижении стоимости спектра или его разделении между операторами.

Важно отметить, что Европейский союз и другие страны активно работают над решением проблем со спектром, разрабатывая стратегии и инициативы, чтобы обеспечить достаточный спектр для успешного развертывания и использования 5G сетей. Это включает в себя гармонизацию спектра, привлечение частных инвестиций, сотрудничество между операторами связи и государственными органами, а также применение новых технологий и методов для эффективного использования доступного спектра. Обеспечение доступности и доступного спектра для всех стран является важным аспектом глобального развертывания 5G. Международные организации и государства работают над разработкой стратегий и политик для облегчения доступа к спектру и

снижения его стоимости для более широкого использования 5G технологии по всему миру. Совместные усилия Европейского союза и других стран позволяют создать благоприятную среду для развертывания 5G сетей, обеспечивая не только необходимый спектр, но и сотрудничество между различными участниками, а также разработку инновационных решений для эффективного использования доступного спектра. Это способствует развитию цифровой экономики, улучшению связности и созданию новых возможностей для граждан и бизнеса в рамках единого европейского цифрового рынка.

2.3 Стоимость развертывания.

Помимо проблем со спектром, доступные и гибкие инфраструктуры для систем 5G, такие как столбы, башни, антенны и системы оптоволокон, также важны для обеспечения емкости и покрытия 5G. Другими словами, требуется высокая стоимость разработки и обслуживания для работы всей системы, особенно инфраструктуры оптоволокон.

Разработка и развертывание сетей 5G требует значительных инвестиций в инфраструктуру и технологии, потенциальных затрат на модернизацию существующей инфраструктуры и опасения по поводу концентрации рынка в телекоммуникационном секторе. Переход на 5G имеет и потенциальные экономические преимущества, такие как увеличение инноваций, создание рабочих мест и экономический рост. В ЕС встает необходимость скоординированного и комплексного подхода для обеспечения внедрения технологии 5G таким образом, чтобы максимизировать экономический рост и выгоды для всех.

В ЕС существует ряд возможностей финансирования для поддержки развития сетей 5G, включая программу Horizon 2020 Европейской комиссии, Horizon Europe и Инвестиционный план Европейского инвестиционного банка для Европы. Многие европейские страны инвестируют в собственные инфраструктурные проекты 5G, а правительства некоторых стран предлагают гранты и субсидии для поддержки перехода на технологию 5G. С 2014 года Европейская комиссия также напрямую софинансировала более 100 проектов 5G в рамках программы "Горизонт 2020"⁴⁹.

⁴⁹ Special Report 03/22: 5G roll-out in the EU // ECA Europe. [Б.м.], 03.2022. URL: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (дата обращения: 17.04.2023).

Программа Horizon 2020 действовала с 2014 по 2020 год и имела, по оценкам, финансирование в размере около 70 миллиардов евро⁵⁰. Это примерно на 13% меньше, чем предложила Европейская комиссия, и на 30% меньше, чем хотел парламент⁵¹. Детали Horizon 2020, включая его модель финансирования, горячо обсуждались после этого в серии "триалогов" — внутренних переговоров с участием национальных министров, членов Европейского парламента и Европейской комиссии. Европейская комиссия заблаговременно определила возможности 5G, установив государственно-частное партнерство в области 5G (5G-PPP⁵²) в 2013 году для ускорения исследований и инноваций в области технологии 5G, на которое было выделено 700 миллионов евро на исследования⁵³. В период с 2014 по 2020 год ERC, как европейская организация, финансирующая передовые исследования, профинансировала 6707 исследовательских проектов в рамках проекта Horizon 2020 на сумму 13,3 миллиарда евро⁵⁴. Horizon 2020 предоставлял гранты на исследовательские и инновационные проекты в рамках открытых и конкурсных конкурсов. Юридические лица из любой страны имели право подавать проектные предложения в рамках этих конкурсов. Участники из стран-членов Европейского Союза и стран, ассоциированных с Horizon 2020⁵⁵, автоматически получали финансирование, что в свою очередь говорит об уменьшении бюрократических работ для получения субсидирования.

За увеличение инвестиций в ЕС, включая область инфраструктуры 5G отвечала инициатива Европейского инвестиционного банка (ЕИБ), известная также как "План Юнкера" (по имени бывшего председателя Европейской комиссии Жан-Клода Юнкера) и Инвестиционный план для Европы, который был запущен в 2014 году с целью привлечения не менее 500 млрд евро инвестиций к 2020 году. План состоит из трех основных компонентов, включая Европейский фонд стратегических инвестиций (EFSl),

⁵⁰ Quirin Schiermeier Horizon 2020 deal reached in Brussels // Nature. [Б.м.], 26.06.2013. URL:<https://www.nature.com/articles/nature.2013.13279> (дата обращения: 17.04.2023).

⁵¹ Alison Abbott Europe scales back research plans // Nature. [Б.м.], 12.02.2013. URL:<https://www.nature.com/articles/494159a> (дата обращения: 17.04.2023).

⁵² About the 5G PPP // The 5G Infrastructure Public Private Partnership. [Б.м.], 2023. URL:<https://5g-ppp.eu/> (дата обращения: 17.04.2023).

⁵³ 5G RESEARCH IN HORIZON 2020 WEBCAST // The 5G Infrastructure Public Private Partnership. [Б.м.], 2023. URL:<https://5g-ppp.eu/european-5g-actions/> (дата обращения: 17.04.2023).

⁵⁴ ERC reveals mapping of its funded research // European Research Council. [Б.м.], 14.07.2022. URL:<https://erc.europa.eu/news-events/news/erc-reveals-mapping-its-funded-research> (дата обращения: 18.04.2023).

⁵⁵ Alison Abbott Farewell to Europe's Horizon 2020 // Nature. [Б.м.], 16.12.2020. URL:<https://www.nature.com/articles/d41586-020-03516-6> (дата обращения: 18.04.2023).

который предоставляет гарантии и другие формы поддержки для стимулирования частных инвестиций в ключевые сектора, такие как инфраструктура, исследования и инновации, а также малые и средние предприятия. EFSI был использован для поддержки различных проектов, связанных с 5G, таких как развертывание сетей 5G в Испании и разработка технологии 5G в Финляндии. Европейский консультативный центр по инвестициям и Европейский портал инвестиционных проектов, которые призваны помочь связать инвесторов с жизнеспособными инвестиционными проектами по всему ЕС⁵⁶. EFSI поддержал два проекта, направленных на достижение более плотного развертывания ячеек и поддержку стандартизации. Общая инвестиционная стоимость этих проектов составила €3,9 млрд., включая €1 млрд. финансирования из EFSI⁵⁷.

В период 2014-2020 годов ЕС поддержал развитие 5G более чем на 4 млрд. евро, как напрямую из бюджета ЕС, так и через финансирование Европейского инвестиционного банка. Бюджет ЕС финансировал проекты, связанные исключительно с исследованиями, в то время как ЕИБ поддерживал как исследования, так и развертывание⁵⁸. По состоянию на август 2021 года он предоставил кредиты на общую сумму 2,5 млрд. евро для девяти проектов 5G в пяти государствах-членах ЕС. Кроме того, около €1,9 млрд. было выделено из бюджета ЕС на период 2014-2020 годов.

В 2021 году общая стоимость развертывания 5G во всех государствах-членах ЕС до 2025 года оценивается в диапазоне от 281 до 391 миллиарда евро, поровну разделенных между строительством новой инфраструктуры 5G и обновлением фиксированной инфраструктуры до гигабитных скоростей⁵⁹. Основная часть этих инвестиций должна финансироваться операторами мобильной связи. Эта смета расходов распределяется поровну между строительством новой инфраструктуры 5G и модернизацией существующей инфраструктуры. Инвестиции окажут значительное влияние на экономическое и технологическое развитие ЕС в ближайшие годы.

⁵⁶ Eulalia Rubio, David Rinaldi, Thomas Pellerin-Carlin INVESTMENT IN EUROPE: MAKING THE BEST OF THE JUNKER PLAN // Notre Europe. [Б.м.], 06.2016. URL: https://europe-solidarity.eu/documents/ES_investmentjunkerplan-mar16.pdf (дата обращения: 19.04.2023).

⁵⁷ Special Report 03/22: 5G roll-out in the EU // ECA Europe. [Б.м.], 03.2022. URL: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (дата обращения: 19.04.2023).

⁵⁸ Special Report 03/22: 5G roll-out in the EU // ECA Europe. [Б.м.], 03.2022. URL: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (дата обращения: 19.04.2023).

⁵⁹ Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All // Commission estimate based on data by EIB, Analysis, GSMA and company announcements, and ETNO – European Telecommunications, [Б.м.], 03.2021. URL: <https://etno.eu/downloads/reports/connectivity%20and%20beyond.pdf> (дата обращения: 27.04.2023).

По данным European 5G observatory 81% населения ЕС охвачено как минимум одним оператором, предлагающим услуги 5G на момент 10 Мая 2023 Г.

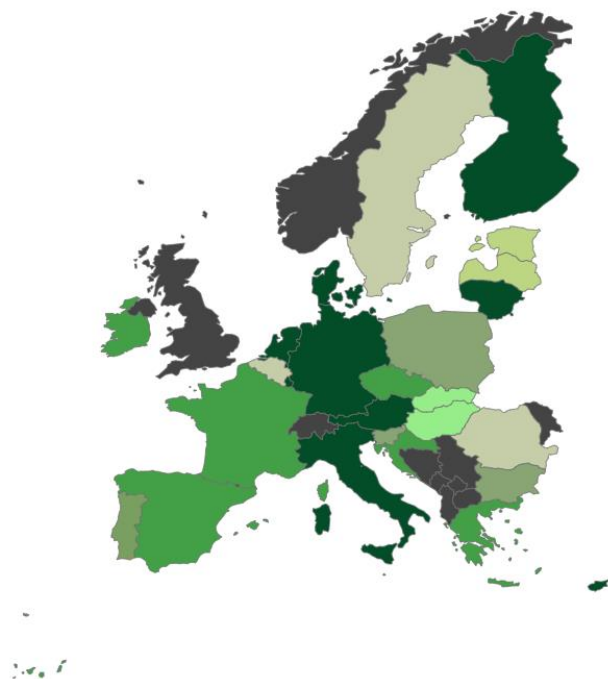


Рисунок 1 – Карта: покрытие 5G⁶⁰

Для более глубокого понимания технологических проблем, связанных с использованием спектра и его доступностью, были проведены анализы, определяющие, на каких частотах в настоящее время доступна технология 5G в странах Европейского союза. Были также изучены вопросы, связанные со стоимостью развертывания 5G и основными операторами и поставщиками этой технологии. [см. приложения В].

2.4 Проблемы безопасности.

Революционная технология 5G, это после долгосрочной эволюции (LTE). Она помогает увеличить скорость передачи беспроводных данных. Кроме того, она может создать обширное широкополосное подключение, более высокую и быструю мобильность. Она также поддерживает низкую задержку и высокое качество обслуживания по сравнению с другими предыдущими поколениями (например, 1G до 4G). Более того, она поддерживает не только мобильные устройства, но и различное новое оборудование, например, коммуникацию (M2M), Интернет вещей (IoT) и кибер-

⁶⁰ European 5G scoreboard Overview of 5G developments // official web site of European 5g observatory [Б.м.], URL: <https://5gobservatory.eu/observatory-overview/eu-scoreboard/> (дата обращения: 27.04.2023).

физические системы (CPSs). Однако она также сталкивается со многими новыми проблемами безопасности, и решения для старых поколений не подходят для него. На основе мета-анализа различных обзоров литературы, проблемы безопасности 5G приведены ниже.

Таблица 3. Проблемы безопасности

№	Проблемы безопасности	Описание
1	Мобильные виртуальные операции	Утечка данных, незащищенный Wi-Fi, подмена сети, фишинговые атаки, шпионское ПО, нарушенная криптография, неправильная обработка сессий
2	Телекоммуникационный мошенничество	Slamming, cramming, мошенничество с бесплатными номерами, социальная инженерия, обход проблем
3	Проблемы IoT	Атаки на Wi-Fi, радиочастоты, точки доступа и подобные
4	Сетевые атаки	Атаки на доступность, аутентификацию и конфиденциальность, атаки DoS/DDoS, уязвимости программно-определенных сетей (SDN), виртуализация сетевых функций (NFV)
5	Конфиденциальность пользователя	Отслеживание местоположения, идентификация и потеря личных данных через семантические информационные атаки, атаки на идентификатор международного мобильного абонента (IMSI)
6	Уязвимости безопасности сети, коммуникация	Подслушивание, атака "человек посередине", атака повторного воспроизведения, атака DoS, перекрестная атака, вирусные/вредоносные атаки

Источник: IEEE Xplore⁶¹

Ниже рассмотрим более подробно все существующие угрозы, которые увеличились вместе со скоростью передачи данных.

⁶¹ 5G revolution: Challenges and opportunities/developments // official web site of IEEE Xplore [Б.м.], URL: <https://ieeexplore.ieee.org/document/9668550> (дата обращения: 27.04.2023).

2.4.1 Мобильные виртуальные операции.

Утечка данных - Мобильные приложения часто являются причиной непреднамеренной утечки данных. Например, «опасные» приложения представляют реальную проблему для мобильных пользователей, которые предоставляют им широкие разрешения, но не всегда проверяют безопасность. Как правило, это бесплатные приложения из официальных магазинов приложений, которые работают так, как рекламируется, но также отправляют личные — и потенциально корпоративные — данные на удаленный сервер, где они добываются рекламодателями, а иногда и киберпреступниками. Утечка данных также может происходить через враждебные мобильные приложения, подписанные предприятием. Эти мобильные вредоносные программы используют код распространения, свойственный популярным мобильным операционным системам, таким как iOS и Android, для перемещения ценных данных по корпоративным сетям, не вызывая подозрений.

Незащищенный Wi-Fi -Никто не хочет сжигать свои сотовые данные, когда доступны беспроводные точки доступа, но бесплатные сети Wi-Fi обычно не защищены. Согласно V3, трое британских политиков, которые согласились принять участие в бесплатном эксперименте по обеспечению безопасности беспроводной сети, были легко взломаны экспертами по технологиям. Их социальные сети, PayPal и даже их разговоры по VoIP были скомпрометированы.

Подмена сети. Спуфинг сети — это когда хакеры устанавливают поддельные точки доступа — соединения, которые выглядят как сети Wi-Fi, но на самом деле являются ловушками — в общественных местах с интенсивным движением, таких как кафе, библиотеки и аэропорты. Киберпреступники дают точкам доступа общие названия, такие как «Бесплатный Wi-Fi в аэропорту» или «Кофейня», чтобы побудить пользователей подключиться. В некоторых случаях злоумышленники требуют от пользователей создать «учетную запись» для доступа к этим бесплатным службам с паролем. Поскольку многие пользователи используют одну и ту же комбинацию электронной почты и пароля для нескольких служб, хакеры могут скомпрометировать электронную почту пользователей, электронную торговлю и другую защищенную информацию.

Фишинговые атаки - Поскольку мобильные устройства всегда включены, они являются главными объектами фишинговых атак. По данным CSO, мобильные пользователи более уязвимы, потому что они часто отслеживают свою электронную почту в режиме реального времени, открывая и читая электронные письма по мере их получения. Пользователи мобильных устройств также более уязвимы, поскольку

почтовые приложения отображают меньше информации, чтобы приспособиться к меньшему размеру экрана.

Шпионское ПО - Хотя многие мобильные пользователи беспокоятся о том, что вредоносные программы отправляют потоки данных обратно киберпреступникам, есть ключевая угроза ближе к дому: шпионское ПО. Во многих случаях пользователям следует беспокоиться не о вредоносных программах от неизвестных злоумышленников, а о шпионских программах, установленных супругами, коллегами или работодателями для отслеживания их местонахождения и активности. Также известные как stalkerware, многие из этих приложений предназначены для загрузки на устройство цели без ее согласия или ведома. Комплексный антивирус и антивирусный пакет для обнаружения вредоносных программ должны использовать специальные методы сканирования для этого типа программ, которые требуют несколько иного обращения, чем другие вредоносные программы, из-за того, как они попадают на устройство и для чего они предназначены.

Сломанная криптография - По данным Института информационной безопасности учебные материалы, нарушение криптографии может произойти, когда разработчики приложений используют слабые алгоритмы шифрования или не могут должным образом реализовать надежное шифрование. В первом случае разработчики могут использовать знакомые алгоритмы шифрования, несмотря на их известные уязвимости, чтобы ускорить процесс разработки приложений. В результате любой мотивированный злоумышленник может использовать уязвимости для взлома паролей и получения доступа. Во втором примере разработчики используют высоконадежные алгоритмы, но оставляют открытыми другие «черные ходы», ограничивающие их эффективность. Например, хакеры могут быть не в состоянии взломать пароли, но если разработчики оставят в коде недостатки, позволяющие злоумышленникам изменять высокоуровневые функции приложения, такие как отправка или получение текстовых сообщений, им может не понадобиться пароль для возникновения проблем.

Неправильная обработка сеанса - Чтобы облегчить доступ к транзакциям с мобильных устройств, многие приложения используют «токены», которые позволяют пользователям выполнять несколько действий без необходимости повторной аутентификации своей личности. Как и пароли для пользователей, токены генерируются приложениями для идентификации и проверки устройств. Защищенные приложения генерируют новые токены при каждой попытке доступа или «сеансе» и должны оставаться конфиденциальными. Согласно манифесту, неправильная обработка сеанса происходит, когда приложения непреднамеренно обмениваются маркерами сеанса,

например, со злоумышленниками, что позволяет им выдавать себя за законных пользователей. Часто это результат сеанса, который остается открытым после того, как пользователь ушел из приложения или веб-сайта. Например, если сотрудник вошел на сайт внутренней сети компании со своего планшета и забыл выйти из системы после завершения задачи, оставаясь открытым, киберпреступник сможет свободно исследовать веб-сайт и другие подключенные части сети его работодателя.

Согласно Harvard Business Review (HBR), несмотря на то, что мобильная безопасность становится предпочтительной целью для хакеров, она не имеет приоритета по сравнению с сетевой и компьютерной безопасностью. HBR сообщает, что даже в рамках мобильной экосистемы расходы на безопасность хронически недофинансируются по сравнению с разработкой мобильных приложений. По мере того, как наша зависимость от мобильных устройств растет, растет ценность данных и, следовательно, мотивация киберпреступников. В дополнение к угрозам мобильной безопасности, которые мы только что обсудили, будьте готовы к новым угрозам, сосредоточенным на следующих трех ключевых областях воздействия:

SMiShing: как и при фишинге, киберпреступники пытаются обманным путем заставить людей загружать вредоносное ПО, переходить по вредоносным ссылкам или раскрывать конфиденциальную информацию. Атака *SMiShing* запускается через текстовые сообщения вместо электронной почты.

BYOD: поскольку бизнес-пользователям предоставляется высокоуровневый доступ с личных мобильных устройств, смартфоны и планшеты эффективно заменяют настольные компьютеры для решения многих бизнес-задач. Однако персональные мобильные устройства не обеспечивают того же уровня встроенной безопасности или контроля, что и настольные компьютеры, принадлежащие организации, которые они заменяют.

2.4.2 Телекоммуникационный мошенничество

Slamming — это незаконная практика, когда телефонный оператор изменяется без явного согласия клиента. Это часто происходит, когда третья сторона заявляет, что клиент согласился на переключение, но на самом деле этого не было.

Cramming — это другая форма мошенничества, при которой клиентам незаконно начисляются сборы за дополнительные услуги, на которые они не подписывались. Эти сборы могут быть замаскированы под вполне законные платежи, и клиенты могут не заметить их на своих счетах.

Мошенничество с бесплатными номерами — это когда мошенники используют бесплатные телефонные номера, чтобы казаться более доверительными. Они могут представляться представителями банка, страховой компании или любой другой организации, чтобы убедить людей дать им конфиденциальную информацию.

Социальная инженерия — это тактика мошенничества, при которой мошенники пытаются обмануть людей, чтобы они раскрыли свои личные данные, такие как пароли или номера банковских карт. Это часто достигается путем манипуляции, обмана или эксплуатации доверия.

Обход проблем — это термин, который часто используется в IT и кибербезопасности, чтобы описать процесс обхода технических препятствий или ограничений. Это может включать в себя обход систем защиты, защиты от копирования или других мер безопасности.

2.4.3 Проблемы IoT.

Беспроводные сети, включая Wi-Fi и радиочастотные коммуникации, представляют собой важные элементы современной телекоммуникации. Однако, несмотря на их удобство и широкое распространение, эти технологии подвержены ряду угроз безопасности. Далее представлены некоторые из этих атак, включая те, которые могут осуществляться на уровне радиочастот и точек доступа:

Атака "человек посередине" (MitM): Эта атака происходит, когда злоумышленник успешно встраивается в беспроводное соединение, перехватывая и возможно модифицируя данные, которые передаются между двумя сторонами. В сфере Wi-Fi это может происходить, когда атакующий находится в пределах действия беспроводного сигнала и способен перехватить и вмешаться в данные, передаваемые между устройством и точкой доступа.

Атака с использованием "злого близнеца": В этом сценарии злоумышленник создает фальшивую точку доступа Wi-Fi, которая маскируется под настоящую. Если устройство пользователя подключается к такой точке доступа, его данные могут быть перехвачены или даже подвергнуты атаке "человек посередине".

Wi-Fi Pineapple: Это аппаратное устройство, которое способно выполнять широкий спектр атак на Wi-Fi, включая создание "злого близнеца" и проведение атак "человек посередине". Wi-Fi Pineapple также способен проводить сложные атаки, такие как автоматическое подключение ничего не подозревающих устройств к его сети.

Сетевые атаки: Атаки типа отказа в обслуживании (DoS) и распределенного отказа в обслуживании (DDoS) могут быть направлены против точек доступа Wi-Fi. Эти атаки могут привести к существенному снижению производительности сети или даже к полной потере связи.

Атаки на шифрование: Данные, передаваемые по беспроводным сетям, обычно защищаются с помощью шифрования. Однако некоторые злоумышленники могут попытаться взломать эти шифры, особенно более старые и менее безопасные, такие как WEP.

2.4.4 Сетевые атаки

Сетевые атаки могут быть разнообразными и включать различные векторы атаки, в том числе, но, не ограничиваясь этим, атаки на доступность, аутентификацию, конфиденциальность, а также атаки типа отказа в обслуживании (DoS/DDoS).

Атаки на доступность: Эти атаки направлены на прекращение или существенное снижение доступности сети или услуг для законных пользователей. DoS и DDoS являются примерами таких атак, когда злоумышленники насыщают сеть или сервер нежелательным трафиком, чтобы вывести их из строя.

Атаки на аутентификацию: Эти атаки могут включать в себя всякого рода попытки обхода, подмены или взлома механизмов аутентификации, чтобы получить несанкционированный доступ к сети или данным.

Атаки на конфиденциальность: Это атаки, при которых злоумышленник пытается получить доступ к защищенной информации, такой как личные данные, пароли или финансовая информация.

Уязвимости в программно-определенных сетях (SDN): Поскольку SDN управляются программным обеспечением, они могут быть подвержены уязвимостям,

которые могут быть эксплуатированы злоумышленниками. Это может включать в себя уязвимости в самом программном обеспечении, но также может включать проблемы с конфигурацией или безопасностью в управлении и контроле сети.

Уязвимости в виртуализации сетевых функций (NFV): Виртуализация сетевых функций (NFV) позволяет сетевым операторам динамически и гибко разворачивать и управлять сетевыми службами. Однако, как и любая технология, NFV имеет свои недостатки. Это может включать проблемы с изоляцией между виртуализированными функциями, а также риски, связанные с масштабированием и управлением таких сетей.

2.4.5 Конфиденциальность пользователя в рамках 5G.

Он представляет собой серьезное и важное обсуждение, особенно в свете растущих угроз и злоупотреблений в цифровой среде. Ниже представлены некоторые из специфических угроз и вопросов безопасности, которые могут возникнуть в этом контексте:

Отслеживание местоположения: В рамках сети 5G, как и в любой сотовой сети, возможно отслеживание местоположения пользователя. Это может происходить через анализ данных о сотовых турбинах, к которым подключено устройство, а также через другие технологии, такие как GPS. Это может представлять угрозу для приватности пользователя, если эти данные становятся доступными третьим сторонам без согласия пользователя.

Идентификация и потеря личных данных через семантические информационные атаки: Семантические информационные атаки используют сложные методы анализа для извлечения информации из зашифрованных или анонимизированных данных. Например, злоумышленник может анализировать паттерны сетевого трафика или другие метаданные, чтобы определить, что пользователь делает онлайн, даже если сам контент трафика зашифрован.

Атаки на идентификатор международного мобильного абонента (IMSI): IMSI - это уникальный номер, который идентифицирует каждого абонента в сети GSM, 3G и 4G. Однако IMSI можно перехватить, и это может привести к серьезным последствиям, включая возможность отслеживания местоположения пользователя, перехвата звонков и текстовых сообщений и других форм злоупотребления. В 5G были внесены некоторые улучшения для защиты IMSI, но всё ещё остаются определенные риски.

Подслушивание: Подслушивание включает в себя перехват и, возможно, запись данных, передаваемых по сети. Это может происходить как на уровне радиочастот, так и на уровне сетевого протокола. Шифрование и аутентификация являются основными средствами борьбы с подслушиванием.

2.4.6 Уязвимости безопасности сети, коммуникация

Атака повторного воспроизведения: Эта атака происходит, когда злоумышленник перехватывает и затем повторно передает валидные данные, чтобы обмануть систему или устройство. В контексте 5G это может быть использовано для подделки сигналов или данных.

Атака DoS (Denial of Service): В атаке типа DoS злоумышленник пытается перегрузить сеть или устройство с целью прервать нормальное функционирование. В контексте 5G, где многие критически важные системы могут зависеть от непрерывной связи, такие атаки могут иметь серьезные последствия.

Перекрестная атака: Это тип атаки, при котором злоумышленник пытается использовать уязвимости или информацию, полученную в одной системе или контексте, для атаки на другую систему.

Вирусные/вредоносные атаки: Вредоносное программное обеспечение или вирусы могут быть использованы для атаки на устройства или сети 5G. Это может включать в себя все, от спама и фишинга до распространения вредоносного программного обеспечения или проведения других вредоносных действий.

И наконец, подводя итог по технологическим аспектам можно сделать вывод о том что революция пятого поколения открывает новую эру для многих аспектов с крайне высокой скоростью, низкой задержкой, высокой производительностью и массовой связностью. Более того, технология 5G может поддерживать широкий спектр приложений, например, умные дома, умные города, автономные автомобили, беспилотники, Интернет вещей, мультимедиа и развлечения. Однако она также сталкивается с вызовами для пользователей, абонентов и поставщиков сети. Этот раздел представляет общий обзор технологии, возможностей и проблем развертывания. В частности, он указывает на преимущества 5G во многих областях, таких как энергетика, здравоохранение, транспорт, образование, автоматизация и Интернет вещей,

промышленность и интеллектуальные сети. Кроме того, описываются несколько проблем, связанных со многими услугами, интегрированными с 5G. Наконец, следует отметить, что в контексте 5G важно обсудить потенциальные проблемы безопасности. Еще одним важным моментом является то, что когда поставщики услуг предоставляют свои услуги или товары какому-либо государству, в данном случае ЕС, они должны соответствовать установленным стандартам и выполнить все требования. В противном случае это может привести к серьезным проблемам на международном уровне.

Как было показано в представленной таблице поставщиков, китайская компания играет значительную роль в переходе на 5G в ЕС. Учитывая текущие проблемы безопасности, страны ЕС, серьезно беспокоятся о защите данных. Это вызвало политические конфликты, анализ влияния которых мы проведем далее.

2.5 Политические аспекты и проблемы безопасности при переходе на 5G в ЕС

Переход к технологии 5G представляет собой как значительные экономические возможности, так и потенциальные риски безопасности для европейских стран. Политические проблемы, связанные с переходом на 5G в Европе, включают озабоченность по поводу роли китайского технологического гиганта Huawei в развитии сетей 5G, разногласия между странами-членами ЕС по поводу рисков, создаваемых китайскими компаниями, напряженность в отношениях между ЕС и США по этому вопросу, а также необходимость скоординированного и прозрачного подхода к переходу на 5G в Европе. Проблемы безопасности включают риски кибербезопасности, связанные с расширением возможностей подключения и передачи данных в сетях 5G, а также потенциальное влияние 5G на национальную безопасность. Решение этих проблем потребует тщательного рассмотрения и действий со стороны политиков в Европе и за ее пределами, включая разработку четких руководящих принципов и нормативных актов для обеспечения высочайшего уровня безопасности и конфиденциальности для граждан и предприятий, а также расширения сотрудничества и координации между странами.

На фоне глобального противостояния между Вашингтоном и Пекином Европейская комиссия пересматривает свою политику в отношении Китая во всем, от передачи технологий до недобросовестной конкуренции и зависимости от иностранных технологических компаний, таких как Huawei. Предполагаемые связи Huawei с китайским правительством и опасения по поводу шпионажа и возможности кибератак создали напряженность и разногласия в Европейском Союзе.

Перемена позиции к китайским поставщикам в ЕС была вызвана изменениями в китайских законах о разведке и безопасности в последние годы. В одном из примеров, статья 7 Закона о национальной разведке Китая гласит: “Все организации и граждане должны поддерживать, помогать и сотрудничать с национальной разведкой в соответствии с законом и защищать секреты работы национальной разведки, о которых им известно. Государство защищает отдельных лиц и организации, которые поддерживают, содействуют и сотрудничают с национальной разведкой”⁶². Еще один пример для наглядности обеспокоенности властей ЕС взят из статьи 22 Закона о контршпионаже от 2014 года: “Когда органы государственной безопасности проводят расследование, чтобы узнать о шпионском поведении или собрать соответствующие доказательства, соответствующие организации и отдельные лица должны правдиво предоставлять информацию и не должны отказываться”⁶³. Правила применения, опубликованные в ноябре 2017 года, разъяснили положения закона: “Когда органы государственной безопасности выполняют задачи по контршпионажу в соответствии с законом, а граждане и организации, которые обязаны предоставлять помещения или иную помощь в соответствии с законом, отказываются это делать, это представляет собой намерение воспрепятствовать органам государственной безопасности выполнять задачи по контршпионажу в соответствии с законом”⁶⁴. Это вызвало опасения, что китайское правительство может попросить китайские компании, такие как Huawei, внедрить “бэкдоры” в свое оборудование, которые позволили бы Пекину получить доступ в целях шпионажа или саботажа, заявили официальные лица ЕС⁶⁵.

В связи с этим в январе 2019 г. ЕС начал рассмотрение внесения поправок в закон о кибербезопасности 2016 года, который требует, чтобы предприятия, задействованные в

⁶² PRC National Intelligence Law (as amended in 2018) // China Law Translate. [Б.м.], 27.07.2017. URL:<https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> (дата обращения: 07.05.2023).

⁶³ Counter-espionage Law of the People's Republic of China // China Law Translate. [Б.м.], 03.11.2014. URL:<https://www.chinalawtranslate.com/en/anti-espionage/> (дата обращения: 07.05.2023).

⁶⁴ Samantha Hoffman and Elsa Kania Huawei and the ambiguity of China's intelligence and counter-espionage laws // The Strategist, ASPI. [Б.м.], 13.09.2018. URL:<https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/> (дата обращения: 07.05.2023).

⁶⁵ Robin Emmott, Foo Yun Chee, Joanna Plucinska Exclusive: EU considers proposals to exclude Chinese firms from 5G networks // Reuters. [Б.м.], 31.01.2019. URL:<https://www.reuters.com/article/us-usa-china-huawei-tech-europe-exclusiv/exclusive-eu-considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUSKCN1PO2MN> (дата обращения: 07.05.2023).

критически важной инфраструктуре, принимали соответствующие меры безопасности⁶⁶. Что в свою очередь может рассматриваться как запрет на оборудование Huawei Technologies Co. для мобильных сетей следующего поколения, и что процесс изменения закона окажет сдерживающий эффект на бизнес, который европейские страны ведут с китайскими производителями телекоммуникационного оборудования, по словам одного из источников международного агентства новостей Reuters⁶⁷.

Дипломаты Китая в Европейском союзе предупредили о возможных экономических последствиях для стран, которые исключили Huawei из списка возможных поставщиков и подрядчиков по причинам, не связанным с экономикой. С одной стороны, вмешательство правительства КНР может быть оправдано защитой интересов национальных компаний и противодействием американским инициативам по дискредитации и сдерживанию китайских компаний-лидеров в сфере высоких технологий. Однако, с другой стороны, такое вмешательство может стать дополнительным аргументом для противников Huawei, касательно тесных связей этой частной компании с государством. В ряде случаев официальных заявлений со стороны Китая даже не требовалось, поскольку многие политические лидеры стран ЕС «превентивно» учитывают вероятность и последствия ответных мер КНР в случае принятия соответствующих решений.⁶⁸

Вдобавок ко всему, в начале 2019 г. Польша намерена была исключить Huawei из своей будущей сети 5G в пользу европейских игроков (Orange, T-Mobile, Nokia и Ericsson) после ареста сотрудника китайской телекоммуникационной компании по подозрению в шпионаже⁶⁹. В ответ на это Энди Парди, директор по безопасности Huawei Technologies USA, заявил, что Huawei готова работать с польским правительством над

⁶⁶ Directive (EU) 2016/1148 — cybersecurity of network and information systems // EUR-Lex. [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex%3A32016L1148> (дата обращения: 10.05.2023).

⁶⁷ Robin Emmott, Foo Yun Chee, Joanna Plucinska Exclusive: EU considers proposals to exclude Chinese firms from 5G networks // Reuters. [Б.м.], 31.01.2019. URL: <https://www.reuters.com/article/us-usa-china-huawei-tech-europe-exclusiv/exclusive-eu-considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUSKCN1PO2MN> (дата обращения: 10.05.2023).

⁶⁸ Гемуева Карина Алиевна Huawei в странах ЕС: проблема участия в развитии сетей 5G // Научно-аналитический вестник Института Европы РАН. 2020. №3. URL: <https://cyberleninka.ru/article/n/huawei-v-stranah-es-problema-uchastiya-v-razvitiy-setey-5g> (дата обращения: 10.05.2023).

⁶⁹ Joanna Plucinska, Anna Koper Poland set to exclude China's Huawei from 5G plans // Reuters. [Б.м.], 24.01.2019. URL: <https://www.reuters.com/article/us-poland-security/poland-set-to-exclude-chinas-huawei-from-5g-plans-idUSKCN1PI2B7> (дата обращения: 10.05.2023).

дополнительными шагами по укреплению доверия⁷⁰. А также добавил, что Huawei готова принять любые дополнительные меры безопасности, необходимые для продолжения гонки за развитие сетей 5G следующего поколения в Центральной и Восточной Европе⁷¹. В дальнейшем, Польша усилила давление на Huawei, что привело к тому, что китайская компания заявила о том, что действия польского правительства носят политический характер и могут быть направлены на то, чтобы исключить Huawei из развития сети 5G в стране⁷². Можно связать это с тем, что Варшава в 2019 г. пыталась убедить США увеличить свое военное присутствие в Польше, встревоженная возросшей напористостью России, тем самым показав свою лояльность к США⁷³. Администрация бывшего президента США Дональда Трампа похвалила Польшу за аресты, а бывший вице-президент Майк Пенс заявил в 2019 году, что они продемонстрировали приверженность Варшавы обеспечению того, чтобы телекоммуникационный сектор "не был скомпрометирован таким образом, который угрожает нашей национальной безопасности"⁷⁴. По примеру Польши последовала и Румыния⁷⁵.

В марте 2019 г. Европейская Комиссия предложила делиться большим количеством данных для решения проблем кибербезопасности, связанных с сетями 5G, проигнорировав призывы США запретить технологии Huawei. Крупные операторы связи выступают против запрета Huawei, заявляя, что такой шаг может отложить развертывание 5G в блоке на годы⁷⁶. Из-за этого в Брюсселе начались разговоры об ужесточении правил сетевой безопасности вместо запрета китайским компаниям выхода на европейский рынок⁷⁷.

⁷⁰ China's Huawei says ready to work with Poland to build trust // Reuters. [Б.м.], 13.02.2019. URL:<https://www.reuters.com/article/us-huawei-europe-poland/chinas-huawei-says-ready-to-work-with-poland-to-build-trust-idUSKCN1Q20ZT> (дата обращения: 15.05.2023).

⁷¹ Janis Laizans, Anna Koper Huawei ready to tackle extra security to stay in 5G kit race // Reuters. [Б.м.], 13.02.2019. URL:<https://www.reuters.com/article/us-huawei-europe-poland/huawei-ready-to-tackle-extra-security-to-stay-in-5g-kit-race-idUSKCN1Q21N3> (дата обращения: 15.05.2023).

⁷² Huawei fears it may be excluded from Poland's 5G network // Reuters. [Б.м.], 09.09.2020. URL:<https://www.reuters.com/article/us-poland-5g-huawei/huawei-fears-it-may-be-excluded-from-polands-5g-network-idUSKBN2602BY> (дата обращения: 15.05.2023).

⁷³ Россия укрепит западную границу, поскольку США планируют разместить больше войск в Польше // Sputnik. [Б.м.], 17.06.2019 URL:<https://sputnikglobe.com/20190617/russia-to-reinforce-western-border-as-us-plans-to-deploy-more-troops-in-poland-1075907109.html> (дата обращения: 15.05.2023).

⁷⁴ Alicja Ptak, Justyna Pawlak Polish trial begins in Huawei-linked China espionage case // Reuters. [Б.м.], 01.06.2021. URL:<https://www.reuters.com/world/china/polish-trial-begins-huawei-linked-china-espionage-case-2021-05-31/> (дата обращения: 15.05.2023).

⁷⁵ Laurens Cerulus Huawei challenges legality of 5G bans in Poland, Romania // Politico. [Б.м.], 02.11.2020

⁷⁶ Robin Emmott, Foo Yun Chee Exclusive: EU to drop threat of Huawei ban but wants 5G risks monitored - sources // Reuters. [Б.м.], 23.03.2019. URL:<https://www.reuters.com/article/us-eu-huawei-tech-exclusive/exclusive-eu-to-drop-threat-of-huawei-ban-but-wants-5g-risks-monitored-sources-idUSKCN1R32K3>

К тому же запрет на покупку телекоммуникационного оборудования у китайских фирм увеличит стоимость сетей 5G в Европе, замена всего китайского оборудования обойдется примерно на 55 миллиардов евро и задержит внедрение технологии примерно на 18 месяцев. Оценка является частью отчета лоббистской группы телекоммуникационных компаний GSMA, которая представляет интересы 750 операторов мобильной связи⁷⁸. “Половина этих дополнительных затрат будет связана с тем, что на европейских операторах сказались более высокие затраты на ввод после значительной потери конкуренции на рынке мобильного оборудования”, - говорится в отчете, - “кроме того, операторам потребуется заменить существующую инфраструктуру, прежде чем внедрять обновления 5G”. Но с этим утверждением не согласен финский производитель телекоммуникационного оборудования Nokia. “Мы предлагаем техническое решение, при котором мы можем наложить наше оборудование 5G поверх оборудования 4G другого поставщика. Это решение может снизить стоимость и сложность смены поставщика”, - сказал представитель Eric Mangan⁷⁹. Однако другую оценку, отличающуюся от GSMA, дает европейская консалтинговая компания Strand Consult, специализирующаяся на телекоммуникационной отрасли: 3,5 млрд долларов⁸⁰. Вдобавок, Deutsche Telekom заявила, что если Huawei запретят в Европе, это приведет к задержке развертывания сетей 5G на срок до двух лет. Чтобы избежать подобных сбоев, Deutsche Telekom предложила новый процесс сертификации безопасности сетевого оборудования мобильной связи, который позволил бы операторам связи в Германии продолжать использовать продукты китайских производителей в своих планах развертывания 5G⁸¹.

Швеция тоже стала одной из сторонников принятия мер против китайского производителя телекоммуникационных услуг в 2020 году и планировала изъять

(дата обращения: 19.05.2023).

⁷⁷ Giles Turner Huawei Has Skirted Outright Bans in Europe. But Not 5G Regulations // Bloomberg. [Б.м.], 15.04.2019. URL:<https://www.bloomberg.com/news/articles/2019-04-15/huawei-s-avoiding-outright-bans-but-not-5g-regulations-in-europe?srnd=technology-vp> (дата обращения: 19.05.2023).

⁷⁸ Gwénaëlle Barzic Europe's 5G to cost \$62 billion more if Chinese vendors banned: telcos // Reuters. [Б.м.], 07.06.2019. URL:<https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3> (дата обращения: 19.05.2023).

⁷⁹ Europe 5G to cost many billions more if Chinese vendors banned // Al Jazeera. [Б.м.], 07.06.2019. URL:<https://www.aljazeera.com/economy/2019/6/7/europe-5g-to-cost-many-billions-more-if-chinese-vendors-banned> (дата обращения: 19.05.2023).

⁸⁰ The real cost to rip and replace of Chinese equipment in telecom networks. // Strand Consult. 09.2019. URL:https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/10/Strand-Consult_The-real-cost-to-rip-and-replace-of-Chinese-equipment-in-telecom-networks-003-1.pdf (дата обращения: 19.05.2023).

⁸¹ Lucian Armasu Huawei Facing Potential Ban in Europe Too // Tom's Hardware. [Б.м.], 31.01.2019. URL:<https://www.tomshardware.com/news/huawei-ban-europe-eu-5g-china.38538.html> (дата обращения: 19.05.2023).

существующее оборудование Huawei к 1 января 2025 года⁸². Huawei раскритиковала июньское решение, заявив: “Суд принял без дальнейшего анализа предположения и широкие спекуляции сил безопасности и обороны, а также отсутствие конкретных доказательств и детального анализа со стороны властей. Эти власти получили слишком большое влияние в вопросах, в которых они не компетентны”⁸³. В ходе дальнейших судебных слушаний апелляционный суд в Швеции оставил в силе ранее вынесенное постановление, поскольку шведские власти обеспокоены связями Huawei с правительством Китая⁸⁴.

Было зафиксировано, что развертывание услуг 5G по всей Европе замедлилось из-за санкций США против Huawei и из-за того, что европейские правительства рассматривают последствия использования китайского оборудования⁸⁵.

Правительство Германии по состоянию на январь 2019 года рассматривало возможность запрета Huawei на поставку оборудования 5G в стране, заявив, что проблемы безопасности имеют “высокую актуальность”⁸⁶. Это решение ознаменовало бы отход от Германии, которая была менее красноречива, чем ее западные союзники, включая США и Великобританию, в отношении проблем безопасности Huawei. К тому же министр иностранных дел Германии Хайко Маас выразил сомнение в том, что Huawei Technologies может участвовать в разработке и строительстве сети 5G в стране⁸⁷. Комментарии министра иностранных дел являются самым сильным признаком того, что Берлин готов придерживаться более жесткого подхода к Huawei и может исключить китайского поставщика оборудования, по крайней мере, из некоторых частей сети 5G.

⁸² Yash Mishra A Swedish court bans Huawei 5G equipment, Huawei say ‘decision made on assumptions’// HC Newsroom. [Б.м.], 23.06.2021. URL:<https://www.huaweicentral.com/a-swedish-court-bans-huawei-5g-equipment-huawei-say-decision-made-on-assumptions/> (дата обращения: 20.05.2023).

⁸³ Laurens Cerulus Huawei seeks EU court involvement in Swedish ban // Politico. [Б.м.], 06.10.2021. URL:<https://www.politico.eu/article/huawei-sweden-china-5g-court-case-european-union/> (дата обращения: 20.05.2023).

⁸⁴ Sweden maintains ban on Huawei 5G equipment // TeleGeography. [Б.м.], 23.22.2022. URL:<https://www.commsupdate.com/articles/2022/06/23/sweden-maintains-ban-on-huawei-5g-equipment/> (дата обращения: 20.05.2023).

⁸⁵ Esha Vaish Europe's 5G delayed by trade war and security reviews, says Tele2 CEO // Reuters. [Б.м.], 01.07.2019. URL:<https://www.reuters.com/article/us-tele2-huawei-tech/europes-5g-delayed-by-trade-war-and-security-reviews-says-tele2-ceo-idUSKCN1TW2WC> (дата обращения: 20.05.2023).

⁸⁶ Elizabeth Schulze, Chloe Taylor Huawei could be banned from 5G in Germany // CNBC. [Б.м.], 18.01.2019. URL:<https://www.cnn.com/2019/01/18/huawei-5g-ban-in-germany.html> (дата обращения: 20.05.2023).

⁸⁷ German minister casts doubt on Huawei participation in 5G build-out // Reuters. [Б.м.], 05.11.2019. URL:<https://www.reuters.com/article/us-germany-telecoms-5g/german-minister-casts-doubt-on-huawei-participation-in-5g-build-out-idUSKBN1XE2EB> (дата обращения: 21.05.2023).

Канцелярия Меркель и Министерство экономики, которые опасаются жестких ограничений в отношении китайских компаний, чтобы не навредить торговым отношениям с Пекином, подвергаются давлению со стороны партии ХДС, требующей ввести прямой запрет на использование Huawei в национальной сети 5G. По настоянию разведывательной службы Германии и администрации США правительство Германии согласилось ужесточить ограничения на Huawei, которые заблокируют доступ ее компонентов к основной сети, но позволят использовать их в менее чувствительных областях⁸⁸. В ответ на это последовала угроза от китайского посла в Берлине. Посол Ву заявил, что Huawei не имеет юридических обязательств предоставлять данные китайскому правительству, затем напомнил, что на долю немецких производителей приходится четверть из 28 миллионов автомобилей, проданных в Китае в 2018 г.⁸⁹. Напоминание, что Китай является крупнейшим рынком для Volkswagen AG, BMW AG и производителя Mercedes-Benz Daimler AG, причем каждая компания инвестировала миллиарды долларов в создание производства и дистрибуции в КНР.

В итоге, Германия ужесточила надзор за поставщиками телекоммуникационных сетей⁹⁰, что, хотя и не привело к запрету Huawei, но затруднило китайской компании закрепиться на крупнейшем рынке Европы. Однако, все три немецких оператора мобильной связи - Deutsche Telekom, Vodafone и Telefonica Deutschland - являются клиентами Huawei.

Министр инноваций и технологий Венгрии Ласло Палкович в июне 2019 г. сообщил, что Будапешт изучает пример Германии, своего крупнейшего иностранного инвестора, где, по его словам, была разработана система оценки для точного выявления возможных угроз безопасности. Однако, Венгрия, как важный политический партнер Китая в ЕС заявила, что у нее нет доказательств того, что оборудование Huawei может представлять угрозу безопасности, а министр иностранных дел Петер Сийярто объявил на

⁸⁸ Arne Delfs Huawei Could Face Outright 5G Network Ban by Merkel's Own Party // Bloomberg. [Б.м.], 15.11.2019. URL:<https://www.bloomberg.com/news/articles/2019-11-15/huawei-could-face-outright-5g-network-ban-by-merkel-s-own-party?srd=technology-vp> (дата обращения: 21.05.2023).

⁸⁹ Tony Czuczka, Steven Arons China Threatens Retaliation Should Germany Ban Huawei 5G // Bloomberg. [Б.м.], 15.12.2019. URL:<https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned> (дата обращения: 21.05.2023).

⁹⁰ Douglas Busvine, Andreas Rinke Germany moves to toughen Huawei oversight: sources // Reuters. [Б.м.], 30.09.2020. URL:<https://www.reuters.com/article/us-germany-huawei/germany-moves-to-toughen-huawei-oversight-sources-idUSKBN26L16Q> (дата обращения: 22.05.2023).

мероприятии в Китае во вторник, что Венгрия привлечет Huawei к развертыванию сети 5G⁹¹.

Стоит также разобрать кейс другой крупной страны ЕС - Франции. После предупреждения США о Huawei в 2019 г. в разгар Торговой войны в Сенат Франции Правительство внесло законопроект, направленный на ужесточение проверок телекоммуникационного оборудования, который был сразу же отклонен, т.к. по заверениям некоторых сенаторов "правительство не предоставило им достаточно времени для надлежащего обсуждения вопроса, который они признали важным и стратегическим"⁹². Но это не помешало Франции негласно сокращать влияние Huawei на французских операторов связи. Французский конгломерат Bouygues рассматривал все варианты, включая судебные иски, чтобы обеспечить себе право сотрудничать с китайской Huawei в развертывании сетей мобильной связи 5G во Франции⁹³. Но попытки не увенчались успехом. Затем власти Франции сообщили операторам связи, планирующим приобрести оборудование Huawei 5G, что они не смогут продлевать лицензии на это оборудование по истечении срока их действия, фактически выводя китайскую компанию из сетей мобильной связи к 2028 году⁹⁴. И никто не высказался насчет этого заявления: ни Huawei, ни Bouygues, ни Altice и другие.

Телефонные компании, включая подразделение SFR Altice Europe NV и Bouygues Telecom, начали вывозить беспроводное оборудование Huawei из крупных французских городов после того, как правительство предприняло меры по удалению китайского поставщика из всех, кроме изолированных частей страны. Связано это с тем, что Конституционный совет Франции подписал постановление, которое обязывает операторов связи отключать оборудование Huawei в густонаселенных районах, где сети модернизируются до беспроводной технологии пятого поколения, по словам людей,

⁹¹ Hungarian minister opens door to Huawei for 5G network rollout // Reuters. [Б.м.], 05.11.2019. URL:<https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U> (дата обращения: 22.05.2023).

⁹² French Senate rejects tougher telecoms controls despite U.S. Huawei warning // Reuters. [Б.м.], 07.02.2019. URL:<https://www.reuters.com/article/us-huawei-europe-france/french-senate-rejects-tougher-telecoms-controls-despite-u-s-huawei-warning-idUSKCN1PV2B8> (дата обращения: 22.05.2023).

⁹³ Bouygues wants to ensure it can work with Huawei on 5G: CEO // Reuters. [Б.м.], 20.02.2020. URL:<https://www.reuters.com/article/us-bouygues-results-5g/bouygues-wants-to-ensure-it-can-work-with-huawei-on-5g-ceo-idUSKBN20E1BL> (дата обращения: 22.05.2023).

⁹⁴ Mathieu Rosemain, Gwénaëlle Barzic Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028 // Reuters. [Б.м.], 22.07.2020. URL:<https://www.reuters.com/article/us-france-huawei-5g-security-exclusive/exclusive-french-limits-on-huawei-5g-equipment-amount-to-de-facto-ban-by-2028-idUSKCN24N26R> (дата обращения: 23.05.2023).

знакомых с ситуацией.⁹⁵ Франция, опираясь на идеи Макрона о европейском суверенитете, стремится найти золотую середину, которая позволила бы Huawei оставаться поставщиком, не допуская ее к более неотъемлемым частям своей беспроводной инфраструктуры.

В дальнейшем эти противоречия и разногласия затрудняют выработку единого подхода к рискам безопасности, создаваемым китайскими компаниями при разработке сетей 5G. Некоторые страны-члены ЕС запретили Huawei участвовать в своих сетях 5G, в то время как другие разрешили компаниям играть определенную роль в развитии такой инфраструктуры. Это привело к разногласиям и критике со стороны США, которые оказывают давление на своих союзников, чтобы те полностью запретили Huawei доступ к своим сетям. Кроме того, необходимо решить проблемы безопасности, которые возникают в связи с расширением возможностей подключения и передачи данных в результате применения технологии 5G. Это включает в себя возможность кибератак и шпионажа со стороны частных и государственных структур, а также необходимость защиты критически важной инфраструктуры и военных сетей.

Для решения этих проблем ЕС разработал ряд рекомендаций по развертыванию сетей 5G для обеспечения высокого уровня безопасности. Эти руководящие принципы включают такие меры, как оценка рисков, разнообразие поставщиков и требования к сертификации поставщиков. Страны-члены ЕС также призвали к более тесному сотрудничеству для выработки единого подхода к решению проблем безопасности 5G.

В конечном итоге, переход на технологию 5G представляет собой как вызовы, так и возможности для европейских стран, особенно в контексте геополитической напряженности и экономической конкуренции. Он потребует тщательного рассмотрения рисков и преимуществ технологии, а также разработки эффективной политики и нормативно-правовых актов для обеспечения высочайшего уровня безопасности и конфиденциальности для граждан и предприятий.

Наблюдается длительная дискуссия по поводу участия китайской компании Huawei в развертывании сетей 5G на территории Европейского союза. В этой дискуссии становятся очевидными глубокие противоречия между различными участниками, такими как операторы мобильных сетей, национальные агентства по кибербезопасности, спецслужбы и компания Huawei. Также становится очевидной конфликт интересов между странами, в котором Европейский союз оказался втянутым. Более того, на Европейский

⁹⁵ Helene Fouquet, Tara Patel France's Huawei Ban Begins to Kick In With Purge in Urban Areas // Bloomberg. [Б.м.], 01.03.2021. URL: <https://www.bloomberg.com/news/articles/2021-03-01/france-s-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas?srnd=technology-vp> (дата обращения: 24.05.2023).

союз оказывается давлением со стороны Китая и США в связи с экономическими различиями. Ситуация усложняется тем, что в настоящее время мир столкнулся с пандемией коронавируса, про которую также необходимо учитывать при принятии решений относительно развертывания сетей 5G.

Политические лидеры стран Европейского союза сталкиваются с трудной задачей сохранения баланса интересов всех участников и корректирования взаимодействия между Европейским союзом и Китаем, принимая во внимание свои долгосрочные стратегические интересы и учитывая возможные негативные последствия экономического, социального и политического характера. Тем не менее, возможно, что крупные страны Европейского союза пойдут по пути компромисса и максимально снизят потенциальные риски безопасности, не исключив Huawei из числа возможных поставщиков. В любом случае, многое будет зависеть от того, как будет осуществляться диалог с заинтересованными сторонами, который усложнен на данный момент кризисом эффективной коммуникации на международном уровне, вызванным информационными войнами.

И собрав все воедино хочется согласиться с Гемуевой К.А.: “В таких условиях члены ЕС фактически оказываются один на один с акторами, несопоставимыми с ними по экономическому и политическому весу, что открывает главным участникам торгового конфликта возможность для массированного продвижения собственных интересов. Более того, при отсутствии единой независимой стратегии, направленной на защиту интересов объединения, позиции ЕС как глобального игрока на рынке ИКТ могут быть ослаблены и утрачен инновационный потенциал, необходимый для удержания конкурентных преимуществ при переходе к новому технологическому укладу⁹⁶”.

⁹⁶ Гемуева Карина Алиевна Huawei в странах ЕС: проблема участия в развитии сетей 5G // Научно-аналитический вестник Института Европы РАН. 2020. №3. URL: <https://cyberleninka.ru/article/n/huawei-v-stranah-es-problema-uchastiya-v-razvitiy-setey-5g> (дата обращения: 24.05.2023).

ЗАКЛЮЧЕНИЕ

Данная диссертация посвящена исследованию проблем перехода на технологию 5G в Европейском союзе с учетом технологических и политических аспектов. Одной из задач данного исследования было изучение регулирования 5G в ЕС, чтобы получить полное представление о механизмах внедрения этой технологии и органах, ответственных за ее осуществление.

В ходе выполнения данной поставленной задачи, были определены основные законодательные акты касающейся 5G, а так же их недостатки. Несмотря на эти недостатки, Регулирование для обеспечения полного покрытия 5G в ЕС играет важную роль в формировании рамок и стандартов, необходимых для успешного внедрения и развертывания 5G сетей. Оно направлено на обеспечение эффективного спектрального управления, создание условий для конкуренции и инноваций, а также обеспечение безопасности и защиты потребителей.

Регулирование 5G в ЕС осуществляется на нескольких уровнях. На уровне Европейского союза разрабатываются общие политические и правовые рамки, определяются стратегические цели и направления развития. В рамках ЕС отсутствуют общие или неограниченные полномочия, и Евросоюз может осуществлять только те функции, которые ему предоставлены в соответствии с договорами. А для обеспечения полного покрытия 5G в Европейском союзе регулирование осуществляется при участии национальных регуляторных органов стран-членов [см. приложения А]. Они осуществляют регулирование национальных рынков и контролируют соблюдение правил и стандартов ЕС.

Одной из главных задач регулирования является обеспечение доступности и равного распределения спектра для 5G сетей. Регуляторы разрабатывают и применяют политику спектрального управления, определяя выделение спектра для 5G, и ставят условия его использования. Это позволяет создать равные возможности для операторов связи и обеспечить полное покрытие 5G сетями в разных регионах ЕС.

Второй задачей данного исследования было анализировать проблемы, которые обсуждаются в Европейском союзе в контексте перехода на технологию 5G. Проблемы, которые обсуждаются в Европейском союзе в связи с переходом на 5G, представляют собой сложную смесь технологических и политических и социальных вопросов.

Технологические проблемы включают в себя вопросы, связанные со спектром и его доступностью [см. приложения В] а так же проблемы безопасности которое представляет собой сложное пересечение технологических и политических вопросов. Определение и

выделение подходящего спектра для 5G сетей требует согласования и координации между различными заинтересованными сторонами, включая операторов связи, правительственные органы и регуляторы. Ограниченные ресурсы спектра и конкуренция за его использование могут стать препятствием для полного покрытия 5G в ЕС.

Другой технологической проблемой является стоимость развертывания и обновления инфраструктуры для 5G. Внедрение новых технологий требует значительных инвестиций в обновление существующих сетей, приобретение нового оборудования и обучение персонала. Финансовые аспекты являются важным фактором при принятии решений о развертывании 5G сетей. Именно Европейский союз обладает экономической мощностью, которая позволяет решать финансовые вопросы в связи с внедрением 5G. Через различные программы, такие как Horizon Europe, ЕС выделяет миллиарды евро для активного развертывания 5G на всей территории Европы с целью стать одним из мировых лидеров в области 5G.

Однако санкции США против китайской компании Huawei, одного из основных поставщиков технологии 5G в ЕС, затруднили процесс ее внедрения. Как уже упоминалось ранее, сложное пересечение технологических и политических вопросов вызывало ожесточенные дискуссии в Европейском союзе. С одной стороны, внедрение 5G требует значительных финансовых затрат, а с другой стороны возникает вопрос информационной безопасности. Страны ЕС столкнулись с дилеммой, в которой необходимо было учесть технологические преимущества компании Huawei и одновременно обеспечить безопасность своих коммуникационных сетей. Принятие решения стало сложным процессом, поскольку требовалось сбалансировать экономические выгоды и потенциальные угрозы для национальной безопасности и конфиденциальности данных.

В ответ на эти санкции, Европейский союз и некоторые его члены начали проводить обзоры и оценки потенциальных угроз, связанных с использованием оборудования Huawei. Были разработаны стратегии и политики, направленные на обеспечение безопасности и защиты критической инфраструктуры при внедрении 5G.

В результате, некоторые страны ЕС приняли меры для ограничения участия Huawei в развертывании своей инфраструктуры 5G, ограничивая или исключая ее участие в критически важных сетях и инфраструктурных проектах. Другие страны, в то же время, продолжают сотрудничать с Huawei, стремясь использовать ее технологии 5G для достижения высокой производительности и эффективности своих сетей.

В рамках политического диалога и сотрудничества, страны ЕС проводят консультации и обмен информацией о мерах безопасности и регуляторных рамках, чтобы

минимизировать возможные риски при развертывании 5G сетей. Также исследуются, и практикуется альтернативные поставщики оборудования, такие как Nokia и Ericson и решения проблем, чтобы обеспечить разнообразие и конкуренцию на рынке.

Аналитически резюмируя, обсуждаемые проблемы значительно влияют на процесс обеспечения полного покрытия 5G в ЕС. Технологические проблемы, такие как спектр, стоимость внедрения 5G и проблемы безопасности, а также политические проблемы, связанные с ограничениями китайской компании Huawei, имеют соответствующие последствия.

Во-первых, все эти проблемы создают сложную цепочку, которая затрудняет процесс внедрения 5G. На данный момент в некоторых странах ЕС внедрение 5G уже завершено, в то время как в других оно составляет всего лишь около 20%. Ограничения доступного радиочастотного спектра также создают препятствия, поскольку не все операторы связи могут перейти на 5G.

Во-вторых, процесс внедрения 5G оказывает влияние на законодательство ЕС. Ранее принятые законы об информационной безопасности не были адаптированы для обработки больших объемов передачи данных. Проблемы со спектром усложняют выделение необходимого спектра, а стоимость внедрения 5G затрудняет участие операторов связи в этом процессе. Проблемы безопасности заставляют ЕС пересматривать законодательные акты, включая Европейский кодекс электронных связей и законы о кибербезопасности.

В-третьих, политические разногласия, включая санкции против Huawei, добавляют еще один аспект проблемам внедрения 5G. Такие разногласия ухудшают отношения с основным поставщиком 5G в ЕС, что дополнительно усложняет ситуацию.

В целом, обсуждаемые проблемы имеют значительное влияние на процесс обеспечения полного покрытия 5G в ЕС, создавая сложности в технологическом, финансовом, безопасностном и политическом аспектах. Для успешного внедрения 5G необходимо учитывать эти проблемы и разрабатывать соответствующие стратегии и меры, чтобы преодолеть вызовы, с которыми сталкивается Европейский союз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. 5G Action Plan // An official website of the European Commission. [Б.м.], 2023. URL:<https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan> (дата обращения: 13.03.2023).
2. Call for future Clean Aviation partnership // official web site of European commission. [Б.м.], 2023. URL: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/call-future-clean-aviation-partnership-2020-08-26_en (дата обращения: 13.03.2023).
3. Quliyev N. 5G TECHNOLOGIES ARE CREATING A NEW WORLD ORDER // Norwegian Journal of Development of the International Science. [Б.м.], 2023. URL: <https://cyberleninka.ru/article/n/5g-technologies-are-creating-a-new-world-order> (дата обращения: 13.03.2023).
4. SURVEY ON ARTIFICIAL INTELLIGENCE TECHNIQUES IN 5G NETWORKS A. Abdellah1, A. Koucheryavy. [Б.м.], 2023. URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2020_1/1-10.pdf (дата обращения: 13.03.2023).
5. Batalla, Jordi Mongay, et al. "Security risk assessment for 5G networks: National perspective." IEEE Wireless communications 27.4 (2020): 16-22. [Б.м.], 2023.
6. Allam, Zaheer, and David S. Jones. "Future (post-COVID) digital, smart and sustainable cities in the wake of 6G: Digital twins, immersive realities and new urban economies." Land use policy 101 (2021): 105201.
7. The European 5G Annual Journal 2021. [Б.м.], 2023. URL: <https://bscw.5g-ppp.eu/pub/bscw.cgi/d424095/5G%20European%20Annual%20Journal%202021.pdf> (дата обращения: 13.03.2023).
8. Garben, Sacha, and Inge Govaere, eds. The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future. Bloomsbury Publishing, 2017. [Б.м.], 2023. URL: https://books.google.ru/books?hl=en&lr=&id=XwMzDwAAQBAJ&oi=fnd&pg=PR5&ots=ENflu98uY7&sig=tEtDE13oNelW8Hpyc_WUBkEmpEo&redir_esc=y#v=onepage&q&f=false (дата обращения: 13.03.2023)
9. European Electronic Communications Code // An official website of Body of European Regulators for Electronic Communications. [Б.м.], 2023. URL:<https://www.berec.europa.eu/en/berec/european-electronic-communications-code> (дата обращения: 16.03.2023).

10. Official Journal of the European Union. [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:321:FULL&from=IT> (дата обращения: 16.03.2023).
11. Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks. [Б.м.], 2023. URL: https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf (дата обращения: 16.03.2023).
12. Tsilikas, Haris. "Huawei v. ZTE in context—EU competition policy and collaborative standardization in wireless telecommunications." IIC-International Review of Intellectual Property and Competition Law 48.2 (2017): 151-178. [Б.м.], 2023. URL: <https://link.springer.com/article/10.1007/s40319-017-0560-7> (дата обращения: 16.03.2023).
13. Commission opens infringement procedures against 24 Member States for not transposing new EU telecom rules // official web site of European commission [Б.м.], 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_206 (дата обращения: 16.03.2023).
14. OJEU, L 194, 19.07.2016, [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL> (дата обращения: 16.03.2023).
15. OJEU, L 151, 7.06.2019 [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2019%3A151%3ATOC> (дата обращения: 20.03.2023).
16. Radio equipment // European Commission. [Б.м.], 2023. URL: https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards/radio-equipment_en (дата обращения: 20.03.2023).
17. DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL // Official Journal of the European Union. L 153/62. 22.5.2014. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=EN> (дата обращения: 20.03.2023).
18. О GDPR на русском // GDPR документы и материалы, на русском языке. [Б.м.], 2023. URL: <https://ogdpr.eu/ru> (дата обращения: 20.03.2023).
19. Data protection in the EU // European Commission. [Б.м.], 2023. URL: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (дата обращения: 20.03.2023).
20. What does the General Data Protection Regulation (GDPR) govern? // European Commission. [Б.м.], 2023. URL: https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en (дата обращения: 20.03.2023).

21. Telecommunications national regulatory authorities // An official website of the European Commission. [Б.м.], 2023. URL: <https://digital-strategy.ec.europa.eu/en/policies/telecommunications-national-regulatory-authorities> (дата обращения: 24.03.2023).
22. Geoffrey Myers Spectrum Auctions // LSE Press. [Б.м.], 2023. URL: <https://press.lse.ac.uk/site/books/m/10.31389/lsepress.spa/> (дата обращения: 24.03.2023).
23. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules [Б.м.], 2023. URL: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules (дата обращения: 24.03.2023).
24. About the Connecting Europe Facility // An official website of the European Union. [Б.м.], 2023. URL: https://inea.ec.europa.eu/programmes/connecting-europe-facility/about-connecting-europe-facility_en (дата обращения: 27.03.2023).
25. Connecting Europe Facility // European Commission. [Б.м.], 2023. URL: <https://wayback.archive-it.org/12090/20221222151902/https://ec.europa.eu/inea/en/connecting-europe-facility> (дата обращения: 27.03.2023).
26. CEF Telecom // INNOVATION AND NETWORKS EXECUTIVE AGENCY. [Б.м.], 2023. URL: <https://wayback.archive-it.org/12090/20221222152013/https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom> (дата обращения: 27.03.2023).
27. Directive (eu) 2018/1972 of the European parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217> (дата обращения: 27.03.2023).
28. Directive (eu) 2018/1972 of the European parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217> (дата обращения: 27.03.2023).
29. Directive (eu) 2018/1972 of the European parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code [Б.м.], 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217> (дата обращения: 27.03.2023).

30. Euro-5g – Supporting the European 5G Initiative [Б.м.], 2023. URL: https://5g-ppp.eu/wp-content/uploads/2017/10/Euro-5G-D5.4_Spectrum_for_5G_v1.0.pdf (дата обращения: 27.03.2023).
31. EC, 5G Action Plan [Б.м.], 2023. URL: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131 (дата обращения: 27.03.2023).
32. ITU-R, IMT Vision - Framework and overall objectives of the future, development of IMT for 2020 and beyond, Recommendation M.2083 [Б.м.], 2023. URL: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf (дата обращения: 27.03.2023).
33. Bundesnetzagentur // An official website of BNetzA. [Б.м.], 2023. URL: https://www.bundesnetzagentur.de/EN/Home/home_node.html (дата обращения: 05.04.2023).
34. New security rules for the 5G roll-out to ensure network security // BMWK JOINT PRESS RELEASE. 2019. URL: <https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2019/20191015-new-security-rules-for-the-5G-roll-out-to-ensure-network-security.html> (дата обращения: 05.04.2023).
35. Making 5G a success in Germany // Federal Ministry of Transport and Digital Infrastructure. [Б.м.], 2018. URL: <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/5G%20Greece/Session%201%20Franziska%20Schill%20GERMANY%20-%20Making%205G%20Sa%20success%20in%20Germany.pdf> (дата обращения: 05.04.2023).
36. ARCEP Homepage // An official english website of ARCEP. [Б.м.], 2023. URL: <https://en.arcep.fr/> (дата обращения: 05.04.2023).
37. 5G REGULATION AND LAW IN FRANCE // CMS Expert Guides. [Б.м.], 2023. URL: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/france> (дата обращения: 09.04.2023).
38. Office of Electronic Communications // UKE. [Б.м.], 2023. URL: <https://uke.gov.pl/en/> (дата обращения: 09.04.2023).
39. Broadband in Poland // An official website of the European Union. [Б.м.], 2023. URL: <https://digital-strategy.ec.europa.eu/en/policies/broadband-poland> (дата обращения: 09.04.2023).
40. Home - AGCOM // An official website of the AGCOM. [Б.м.], 2023. URL: <https://www.agcom.it/> (дата обращения: 09.04.2023).

41. Broadband in Italy // An official website of the European Union. [Б.м.], 2023. URL:<https://digital-strategy.ec.europa.eu/en/policies/broadband-italy> (дата обращения: 09.04.2023).
42. 1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G [Б.м.], 2023. URL: <https://net-informations.com/q/diff/generations.html> (дата обращения: 12.04.2023).
43. From 1G to 5G: A Brief History of the Evolution of Mobile Standards // Brainbridge Workforce Solutions [Б.м.], 2023. URL: <https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards> (дата обращения: 12.04.2023).
44. Woon Hau Chin, Zhong Fan, and Russell Haines. Emerging Technologies and Research Challenges for 5G Wireless Networks [Б.м.] (дата обращения: 12.04.2023). 2023. URL:https://www.researchgate.net/publication/260393079_Emerging_Technologies_and_Research_Challenges_for_5G_Wireless_Networks (дата обращения: 12.04.2023).
45. Special Report 03/22: 5G roll-out in the EU // ECA Europe. [Б.м.], 03.2022. URL:https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (дата обращения: 17.04.2023).
46. Quirin Schiermeier Horizon 2020 deal reached in Brussels // Nature. [Б.м.], 26.06.2013. URL:<https://www.nature.com/articles/nature.2013.13279> (дата обращения: 17.04.2023).
47. Alison Abbott Europe scales back research plans // Nature. [Б.м.], 12.02.2013. URL:<https://www.nature.com/articles/494159a> (дата обращения: 17.04.2023).
48. About the 5G PPP // The 5G Infrastructure Public Private Partnership. [Б.м.], 2023. URL:<https://5g-ppp.eu/> (дата обращения: 17.04.2023).
49. 5G RESEARCH IN HORIZON 2020 WEBCAST // The 5G Infrastructure Public Private Partnership. [Б.м.], 2023. URL:<https://5g-ppp.eu/european-5g-actions/> (дата обращения: 17.04.2023).
50. ERC reveals mapping of its funded research // European Research Council. [Б.м.], 14.07.2022. URL:<https://erc.europa.eu/news-events/news/erc-reveals-mapping-its-funded-research> (дата обращения: 18.04.2023).
51. Alison Abbott Farewell to Europe's Horizon 2020 // Nature. [Б.м.], 16.12.2020. URL:<https://www.nature.com/articles/d41586-020-03516-6> (дата обращения: 18.04.2023).
52. Eulalia Rubio, David Rinaldi, Thomas Pellerin-Carlin INVESTMENT IN EUROPE: MAKING THE BEST OF THE JUNKER PLAN // Notre Europe. [Б.м.], 06.2016. URL:https://europe-solidarity.eu/documents/ES_investmentjunkerplan-mar16.pdf (дата обращения: 19.04.2023).

53. Special Report 03/22: 5G roll-out in the EU // ECA Europe. [Б.м.], 03.2022. URL:https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (дата обращения: 19.04.2023).
54. Special Report 03/22: 5G roll-out in the EU // ECA Europe. [Б.м.], 03.2022. URL:https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf (дата обращения: 19.04.2023).
55. Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All // Commission estimate based on data by EIB, Analysis, GSMA and company announcements, and ETNO – European Telecommunications, [Б.м.], 03.2021. URL:<https://etno.eu/downloads/reports/connectivity%20and%20beyond.pdf> (дата обращения: 27.04.2023).
56. European 5G scoreboard Overview of 5G developments // official web site of European 5g observatory [Б.м.], URL: <https://5gobservatory.eu/observatory-overview/eu-scoreboard/> (дата обращения: 27.04.2023).
57. PRC National Intelligence Law (as amended in 2018) // China Law Translate. [Б.м.], 27.07.2017. URL:<https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> (дата обращения: 07.05.2023).
58. Counter-espionage Law of the People's Republic of China // China Law Translate. [Б.м.], 03.11.2014. URL:<https://www.chinalawtranslate.com/en/anti-espionage/> (дата обращения: 07.05.2023).
59. Samantha Hoffman and Elsa Kania Huawei and the ambiguity of China's intelligence and counter-espionage laws // The Strategist, ASPI. [Б.м.], 13.09.2018. URL:<https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/> (дата обращения: 07.05.2023).
60. Robin Emmott, Foo Yun Chee, Joanna Plucinska Exclusive: EU considers proposals to exclude Chinese firms from 5G networks // Reuters. [Б.м.], 31.01.2019. URL:<https://www.reuters.com/article/us-usa-china-huawei-tech-europe-exclusiv/exclusive-eu-considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUSKCN1PO2MN> (дата обращения: 07.05.2023).
61. Directive (EU) 2016/1148 — cybersecurity of network and information systems // EUR-Lex. [Б.м.], 2023. URL:<https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex%3A32016L1148> (дата обращения: 10.05.2023).
62. Robin Emmott, Foo Yun Chee, Joanna Plucinska Exclusive: EU considers proposals to exclude Chinese firms from 5G networks // Reuters. [Б.м.], 31.01.2019. URL:<https://www.reuters.com/article/us-usa-china-huawei-tech-europe-exclusiv/exclusive-eu-considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUSKCN1PO2MN>

considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUSKCN1PO2MN (дата обращения: 10.05.2023).

63. Гемуева Карина Алиевна Huawei в странах ЕС: проблема участия в развитии сетей 5G // Научно-аналитический вестник Института Европы РАН. 2020. №3. URL: <https://cyberleninka.ru/article/n/huawei-v-stranah-es-problema-uchastiya-v-razvitii-setey-5g> (дата обращения: 10.05.2023).

64. Joanna Plucinska, Anna Koper Poland set to exclude China's Huawei from 5G plans // Reuters. [Б.м.], 24.01.2019. URL:<https://www.reuters.com/article/us-poland-security/poland-set-to-exclude-chinas-huawei-from-5g-plans-idUSKCN1PI2B7> (дата обращения: 10.05.2023).

65. China's Huawei says ready to work with Poland to build trust // Reuters. [Б.м.], 13.02.2019. URL:<https://www.reuters.com/article/us-huawei-europe-poland/chinas-huawei-says-ready-to-work-with-poland-to-build-trust-idUSKCN1Q20ZT> (дата обращения: 15.05.2023).

66. Janis Laizans, Anna Koper Huawei ready to tackle extra security to stay in 5G kit race // Reuters. [Б.м.], 13.02.2019. URL:<https://www.reuters.com/article/us-huawei-europe-poland/huawei-ready-to-tackle-extra-security-to-stay-in-5g-kit-race-idUSKCN1Q21N3> (дата обращения: 15.05.2023).

67. Huawei fears it may be excluded from Poland's 5G network // Reuters. [Б.м.], 09.09.2020. URL:<https://www.reuters.com/article/us-poland-5g-huawei/huawei-fears-it-may-be-excluded-from-polands-5g-network-idUSKBN2602BY> (дата обращения: 15.05.2023).

68. Россия укрепит западную границу, поскольку США планируют разместить больше войск в Польше // Sputnik. [Б.м.], 17.06.2019 URL:<https://sputnikglobe.com/20190617/russia-to-reinforce-western-border-as-us-plans-to-deploy-more-troops-in-poland-1075907109.html> (дата обращения: 15.05.2023).

69. Alicja Ptak, Justyna Pawlak Polish trial begins in Huawei-linked China espionage case // Reuters. [Б.м.], 01.06.2021. URL:<https://www.reuters.com/world/china/polish-trial-begins-huawei-linked-china-espionage-case-2021-05-31/> (дата обращения: 15.05.2023).

70. Laurens Cerulus Huawei challenges legality of 5G bans in Poland, Romania // Politico. [Б.м.], 02.11.2020

71. Robin Emmott, Foo Yun Chee Exclusive: EU to drop threat of Huawei ban but wants 5G risks monitored - sources // Reuters. [Б.м.], 23.03.2019. URL:<https://www.reuters.com/article/us-eu-huawei-tech-exclusive/exclusive-eu-to-drop-threat-of-huawei-ban-but-wants-5g-risks-monitored-sources-idUSKCN1R32K3> (дата обращения: 19.05.2023).

72. Giles Turner Huawei Has Skirted Outright Bans in Europe. But Not 5G Regulations // Bloomberg. [Б.м.], 15.04.2019. URL:<https://www.bloomberg.com/news/articles/2019-04-15/huawei-s-avoiding-outright-bans-but-not-5g-regulations-in-europe?srnd=technology-vp> (дата обращения: 19.05.2023).
73. Gwénaëlle Barzic Europe's 5G to cost \$62 billion more if Chinese vendors banned: telcos // Reuters. [Б.м.], 07.06.2019. URL:<https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3> (дата обращения: 19.05.2023).
74. Europe 5G to cost many billions more if Chinese vendors banned // Al Jazeera. [Б.м.], 07.06.2019. URL:<https://www.aljazeera.com/economy/2019/6/7/europe-5g-to-cost-many-billions-more-if-chinese-vendors-banned> (дата обращения: 19.05.2023).
75. The real cost to rip and replace of Chinese equipment in telecom networks. // Strand Consult. 09.2019. URL:https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/10/Strand-Consult_The-real-cost-to-rip-and-replace-of-Chinese-equipment-in-telecom-networks-003-1.pdf (дата обращения: 19.05.2023).
76. Lucian Armasu Huawei Facing Potential Ban in Europe Too // Tom's Hardware. [Б.м.], 31.01.2019. URL:<https://www.tomshardware.com/news/huawei-ban-europe-eu-5g-china,38538.html> (дата обращения: 19.05.2023).
77. Yash Mishra A Swedish court bans Huawei 5G equipment, Huawei say 'decision made on assumptions'// HC Newsroom. [Б.м.], 23.06.2021. URL:<https://www.huaweicentral.com/a-swedish-court-bans-huawei-5g-equipment-huawei-say-decision-made-on-assumptions/> (дата обращения: 20.05.2023).
78. Laurens Cerulus Huawei seeks EU court involvement in Swedish ban // Politico. [Б.м.], 06.10.2021. URL:<https://www.politico.eu/article/huawei-sweden-china-5g-court-case-european-union/> (дата обращения: 20.05.2023).
79. Sweden maintains ban on Huawei 5G equipment // TeleGeography. [Б.м.], 23.22.2022. URL:<https://www.commsupdate.com/articles/2022/06/23/sweden-maintains-ban-on-huawei-5g-equipment/> (дата обращения: 20.05.2023).
80. Esha Vaish Europe's 5G delayed by trade war and security reviews, says Tele2 CEO // Reuters. [Б.м.], 01.07.2019. URL:<https://www.reuters.com/article/us-tele2-huawei-tech/europes-5g-delayed-by-trade-war-and-security-reviews-says-tele2-ceo-idUSKCN1TW2WC> (дата обращения: 20.05.2023).
81. Elizabeth Schulze, Chloe Taylor Huawei could be banned from 5G in Germany // CNBC. [Б.м.], 18.01.2019. URL:<https://www.cnn.com/2019/01/18/huawei-5g-ban-in-germany.html> (дата обращения: 20.05.2023).

82. German minister casts doubt on Huawei participation in 5G build-out // Reuters. [Б.м.], 05.11.2019. URL:<https://www.reuters.com/article/us-germany-telecoms-5g/german-minister-casts-doubt-on-huawei-participation-in-5g-build-out-idUSKBN1XE2EB> (дата обращения: 21.05.2023).

83. Arne Delfs Huawei Could Face Outright 5G Network Ban by Merkel's Own Party // Bloomberg. [Б.м.], 15.11.2019. URL:<https://www.bloomberg.com/news/articles/2019-11-15/huawei-could-face-outright-5g-network-ban-by-merkel-s-own-party?srnd=technology-vp> (дата обращения: 21.05.2023).

84. Tony Czuczka, Steven Arons China Threatens Retaliation Should Germany Ban Huawei 5G // Bloomberg. [Б.м.], 15.12.2019. URL:<https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned> (дата обращения: 21.05.2023).

85. Douglas Busvine, Andreas Rinke Germany moves to toughen Huawei oversight: sources // Reuters. [Б.м.], 30.09.2020. URL:<https://www.reuters.com/article/us-germany-huawei/germany-moves-to-toughen-huawei-oversight-sources-idUSKBN26L16Q> (дата обращения: 22.05.2023).

86. Hungarian minister opens door to Huawei for 5G network rollout // Reuters. [Б.м.], 05.11.2019. URL:<https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U> (дата обращения: 22.05.2023).

87. French Senate rejects tougher telecoms controls despite U.S. Huawei warning // Reuters. [Б.м.], 07.02.2019. URL:<https://www.reuters.com/article/us-huawei-europe-france/french-senate-rejects-tougher-telecoms-controls-despite-u-s-huawei-warning-idUSKCN1PV2B8> (дата обращения: 22.05.2023).

88. Bouygues wants to ensure it can work with Huawei on 5G: CEO // Reuters. [Б.м.], 20.02.2020. URL:<https://www.reuters.com/article/us-bouygues-results-5g/bouygues-wants-to-ensure-it-can-work-with-huawei-on-5g-ceo-idUSKBN20E1BL> (дата обращения: 22.05.2023).

89. Mathieu Rosemain, Gwénaëlle Barzic Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028 // Reuters. [Б.м.], 22.07.2020. URL:<https://www.reuters.com/article/us-france-huawei-5g-security-exclusive/exclusive-french-limits-on-huawei-5g-equipment-amount-to-de-facto-ban-by-2028-idUSKCN24N26R> (дата обращения: 23.05.2023).

90. Helene Fouquet, Tara Patel France's Huawei Ban Begins to Kick In With Purge in Urban Areas // Bloomberg. [Б.м.], 01.03.2021.

URL:<https://www.bloomberg.com/news/articles/2021-03-01/france-s-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas?srnd=technology-vp> (дата обращения: 24.05.2023).

91. Гемуева Карина Алиевна Huawei в странах ЕС: проблема участия в развитии сетей 5G // Научно-аналитический вестник Института Европы РАН. 2020. №3. URL: <https://cyberleninka.ru/article/n/huawei-v-stranah-es-problema-uchastiya-v-razvitii-setey-5g> (дата обращения: 24.05.2023).

ПРИЛОЖЕНИЕ А Национальные регуляторные органы стран ЕС

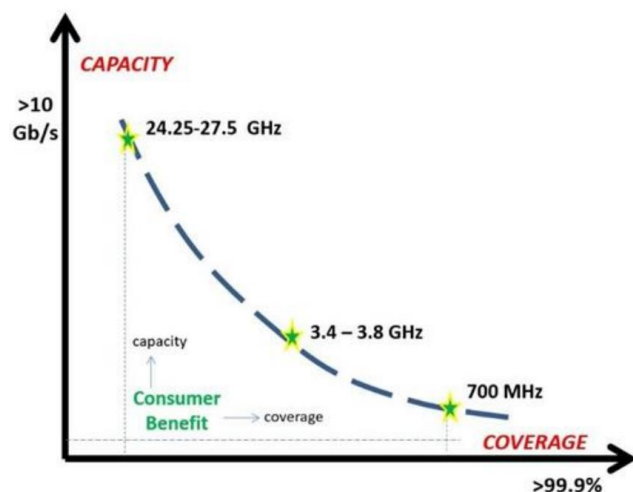
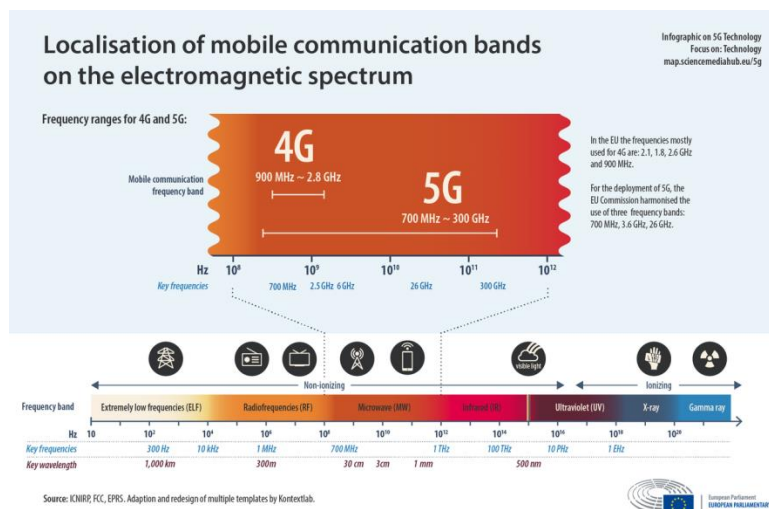
1.	Регуляторный орган по телекоммуникациям и почтовым услугам (Rundfunk und Telekom Regulierungs-GmbH, RTR). RTR осуществляет надзор и регулирование в отрасли связи в Австрии.
2.	Бельгийская комиссия по телекоммуникациям и почтовым услугам (Belgian Institute for Postal Services and Telecommunications, BIPT). BIPT осуществляет надзор и регулирование в отрасли связи и почтовых услуг в Бельгии.
3.	Комиссия по регулированию связи (Communications Regulation Commission, CRC). CRC осуществляет надзор и регулирование в области связи, включая телекоммуникации, в Болгарии.
4.	Хорватское агентство по почтовым услугам и электронным коммуникациям (Croatian Regulatory Authority for Network Industries, НАКОМ). НАКОМ осуществляет надзор и регулирование в отрасли связи, включая телекоммуникации и почтовые услуги, в Хорватии.
5.	Офис комиссара по электронным коммуникациям и почтовым услугам (Office of the Commissioner of Electronic Communications and Postal Regulation, OCECPR). OCECPR осуществляет надзор и регулирование в области электронных коммуникаций и почтовых услуг на Кипре.
6.	Чешское телекоммуникационное управление (Czech Telecommunication Office, STU). STU осуществляет надзор и регулирование в отрасли связи, включая телекоммуникации, в Чешской Республике.
7.	Датская служба по деловой активности (Erhvervsstyrelsen), также известная как Danish Business Authority, является национальным регуляторным органом в Дании, отвечающим за регулирование деловой деятельности, включая телекоммуникации и коммуникационные услуги.
8.	Эстонская служба технического надзора (Estonian Technical Surveillance Authority) отвечает за технический надзор и наблюдение в различных отраслях, включая телекоммуникации и коммуникационные услуги. Она обеспечивает соблюдение технических стандартов, регуляций и лицензионных требований для создания безопасной и эффективной коммуникационной среды. Отдел коммуникаций муниципалитета Эстонии (Estonian Municipal Department of Communications) отвечает за управление коммуникационными услугами и инфраструктурой на муниципальном уровне. Он работает над обеспечением

	надежных и доступных коммуникационных услуг для жителей и предприятий в соответствующем муниципалитете.
9.	Финская коммуникационная регуляторная служба (Finnish Communications Regulatory Authority) отвечает за регулирование коммуникаций в Финляндии, включая телекоммуникации и почтовые услуги. Министерство транспорта и связи Финляндии определяет стратегическое руководство и развитие сектора транспорта и связи, включая коммуникационную инфраструктуру.
10.	ARCEP (Autorité de Régulation des Communications Électroniques et des Postes) - это французский регуляторный орган, отвечающий за регулирование электронных коммуникаций и почтовых услуг.
11.	Регулирование в Германии осуществляется Федеральным институтом связи (Bundesnetzagentur). Он отвечает за лицензирование, контроль использования спектра и установку правил и требований для развертывания и эксплуатации 5G-сетей в стране.
12.	ЕЕТТ (Hellenic Telecommunications and Post Commission) - регуляторный орган в Греции, отвечающий за телекоммуникации и почтовые услуги. ЕЕТТ осуществляет надзор и регулирование в отрасли связи, включая лицензирование, контроль за использованием спектра и установку правил и требований для обеспечения эффективного функционирования коммуникационного сектора в Греции.
13.	НМНН (Nemzeti Média- és Hírközlési Hatóság) - это регуляторный орган в Венгрии, отвечающий за медиа и коммуникационные услуги. НМНН осуществляет надзор и регулирование в области телекоммуникаций, радиовещания, интернет-сервисов и других медиа-отраслей. Он отвечает за лицензирование, контроль качества услуг и защиту прав потребителей в сфере медиа и коммуникаций в Венгрии.
14.	Комиссия по регулированию связи (Commission for Communications Regulation, ComReg) - это регуляторный орган в Ирландии, ответственный за регулирование связи и телекоммуникаций. ComReg осуществляет надзор и регулирование в отрасли связи, включая телекоммуникации, радиовещание, интернет-сервисы и почтовые услуги.
15.	Регулирование в Италии осуществляется Агентством по коммуникациям (Agcom) и Национальным институтом связи (Institute for the Regulation of Electronic Communications). Они контролируют использование спектра,

	устанавливают правила и требования для развертывания и эксплуатации 5G-сетей в стране.
16.	Electronic Communications and Postal Regulatory Authority of Latvia (ECPRAL) - это орган регулирования электронных коммуникаций и почтовых услуг в Латвии. SPRK (Sabiedrisko pakalpojumu regulēšanas komisija) - это сокращение названия Electronic Communications and Postal Regulatory Authority of Latvia на латышском языке. SPRK отвечает за регулирование электронных коммуникаций и почтовых услуг в Латвии.
17.	Литовский регуляторный орган в сфере связи Rysiu Reguliavimo Tarnyba (RRT). Осуществляет надзор и регулирование в отрасли связи, включая телекоммуникации, интернет-сервисы и почтовые услуги. Он отвечает за лицензирование, контроль качества услуг, установление правил и требований для обеспечения эффективного функционирования коммуникационного сектора в Литве.
18.	ILR (Institut Luxembourgeois de Régulation) - регуляторный орган в Люксембурге, отвечающий за регулирование связи и медиа. Он осуществляет надзор и устанавливает правила для обеспечения эффективного функционирования коммуникационного сектора в Люксембурге.
19.	Malta Communications Authority (MCA) - регуляторный орган в Мальте, отвечающий за регулирование коммуникаций, включая связь, телекоммуникации, радиовещание и интернет-сервисы. MCA осуществляет надзор, лицензирование и установление правил для обеспечения эффективного функционирования коммуникационного сектора в Мальте.
20.	АСМ (Autoriteit Consument en Markt) - регуляторный орган в Нидерландах, отвечающий за защиту прав потребителей и регулирование рынков. АСМ осуществляет надзор и регулирование в различных секторах, включая телекоммуникации, энергетику, транспорт, почтовые услуги и другие. Он занимается контролем конкуренции, лицензированием, контролем качества услуг и защитой интересов потребителей в Нидерландах.
21.	UKE (Urząd Komunikacji Elektroniczej) - регуляторный орган в Польше, отвечающий за связь и электронные коммуникации. Он осуществляет надзор и регулирование в отрасли связи, включая телекоммуникации, интернет-сервисы, радиовещание и почтовые услуги.
22.	ANACOM (Autoridade Nacional de Comunicações) - португальский

	регуляторный орган в области почтовых и электронных коммуникаций. ANACOM осуществляет надзор и регулирование в сфере связи, включая телекоммуникации, интернет-сервисы, радиовещание и почтовые услуги. Он ответственен за лицензирование, контроль качества услуг, установление правил и требований для обеспечения эффективного функционирования коммуникационного сектора в Португалии.
23.	ANCOM (Autoritatea Națională pentru Administrare și Reglementare în Comunicații) - регуляторный орган в Румынии, отвечающий за управление и регулирование коммуникаций. ANCOM осуществляет надзор и контроль в отрасли связи, включая телекоммуникации, интернет-сервисы, радиовещание и почтовые услуги.
24.	Regulacny Urad (Regulatory Office for Electronic Communications and Postal Services) - регуляторный орган в Словакии, отвечающий за электронные коммуникации и почтовые услуги. Regulacny Urad осуществляет надзор и регулирование в отрасли связи, включая телекоммуникации, интернет-сервисы и почтовые услуги. Он занимается лицензированием, контролем использования спектра и установлением правил и требований для обеспечения эффективного функционирования коммуникационного сектора в Словакии.
25.	AKOS (Agencija za komunikacijska omrežja in storitve Republike Slovenije) - словенский регуляторный орган, отвечающий за коммуникационные сети и услуги. Он осуществляет надзор и регулирование в области связи, включая телекоммуникации, интернет-сервисы и почтовые услуги в Словении.
26.	Comisión Nacional de los Mercados y la Competencia (CNMC) - это испанский регуляторный орган, ответственный за регулирование рынков и конкуренции. CNMC осуществляет надзор и регулирование в различных отраслях, включая телекоммуникации, энергетику, почтовые услуги и другие.
27.	Шведское агентство связи (PTS) отвечает за регулирование связи, включая управление спектром, назначение лицензий, контроль качества услуг и защиту интересов потребителей. Оно играет важную роль в развитии и регулировании 5G в Швеции.

ПРИЛОЖЕНИЕ Б Иллюстрация покрытия и емкости по сравнению с частотой



Качественная иллюстрация покрытия и емкости по сравнению с частотой⁹⁷.

⁹⁷5G Infrastructure Association, Response to RSPG Public consultation on the Draft RSPG Opinion on spectrum related aspects for next-generation wireless systems (5G), Initiative on pioneer 5G bands [Б.м.], 2023. URL: https://circabc.europa.eu/d/a/workspace/SpacesStore/4ed94c29-182f-418a-b202-6861f69a4f3a/Responses_5G.pdf

ПРИЛОЖЕНИЕ В Обзор 5G в странах ЕС: частоты, стоимость, операторы, поставщики, уровень внедрения

ЕС27	Доступные диапазоны 5G	Стоимость радиоспектра €	Операторы 5G	Основные поставщики	Уровень внедрения
Австрия	700 MHz 3.6 GHz	644 млн.	Drei A1 Telekom Magenta Telekom	ZTE Nokia Huawei	91.7%
Бельгия	700 MHz 3.6 GHz	1,2 миллиарда	Orange Belgium Proximus Telenet Citymesh	Nokia Ericsson	29.6%
Болгария	3.6 GHz 26 GHz	6.9 млн.	A1 Vivacom Telenor	Ericsson Nokia	67.2%
Венгрия	700 MHz 3.6 GHz	368 млн.	Magyar Telecom Vodafone Hungary Yettel	Huawei Ericsson	57,9%
Германия	700 MHz 3.6 GHz 26 GHz	6,55 млрд	Deutsche Telekom Telefonica Vodafone Germany	Ericsson Nokia Huawei	93,2%
Греция	700 MHz 3.6 GHz 26 GHz	372,3 млн.	Wind Hellas Cosmote	Ericsson Huawei	85,7%
Дания	700 MHz 3.6 GHz 26 GHz	575,2 млн.	Telenor Telia TDC	Ericsson Nokia	97,8%

Ирландия	700 MHz 3.6 GHz	78,5 млн.	Three Ireland Vodafone Eir	Ericsson Huawei	83,9%
Испания	700 MHz 3.6 GHz 26 GHz	438 млн.	Masmovil Orange Vodafone Telefonica	Ericsson Nokia Huawei	82,3%
Италия	700 MHz 3.6 GHz 26 GHz	6,55 млрд.	Telecom Italia Windtre Vodafone Iliad	Ericsson Nokia Huawei	99,7%
Кипр	700 MHz 3.6 GHz	41,6 млн.	Tele2 Cyta Epic	Huawei	100%
Латвия	700 MHz 3.6 GHz	2,5 млн.	LMT Tele2	Nokia	42
Литва	700 MHz 3.6 GHz	-----	Tele2 Telia	Nokia	90,1
Люксембург	700 MHz 3.6 GHz	41,3 млн.	Post Orange Tango	Ericsson Nokia	93,2
Мальта	3.6 GHz	<i>Годовая аренда</i>	Epic	Ericsson	100
Нидерланды	700 MHz	1,3 млрд.	KPN T-Mobile Vodafone Ziggo	Ericsson Huawei	100
Польша	700 MHz 3.6 GHz	103,4 млн.	Play Polkomtel (Plus) Orange	Ericsson Nokia	63,4
Португалия	700 MHz 3.6 GHz	-----	Digi NOS	Ericsson Nokia	70,1

				huawei	
Румыния	700 MHz 3.6 GHz	-----	Vodafone Orange Digi	Ericsson Nokia huawei	26,8
Словакия	700 MHz 3.6 GHz	-----	Slovak Telecom Orange	Ericsson Nokia	55,3
Словения	700 MHz 3.6 GHz 26 GHz	164,2 млн.	A1 Telekom Slovenije	Ericsson	63,9
Финляндия	700 MHz 3.6 GHz 26 GHz	77,6 млн.	Elisa SYV Telia	Ericsson Nokia	94,7
Франция	700 MHz 3.6 GHz	2,1 млрд.	Orange Bouygues Telecom Free SFR	Huawei Ericsson Nokia	88,8
Хорватия	700 MHz 3.6 GHz 26 GHz	770 млн.	A1 Hrvatski Telekom Tele2	Ericsson Huawei	82,5
Чехия	700 MHz 3.6 GHz	251 млн.	Telefonica T-Mobile Vodafone	Ericsson Huawei	82,6
Швеция	700 MHz 3.6 GHz 26 GHz	-----	Tre Telenor Telia Tele2	Ericsson Nokia Huawei	20,5
Эстония.	700 MHz 3.6 GHz	-----	Telia Elisa Tele2	Ericsson Nokia	43,3

Отчет о проверке на заимствования №1



Автор: Собиров Сарварбек Соибжон угли
Проверяющий: Воробьева Вероника Сергеевна
Организация: Томский Государственный Университет

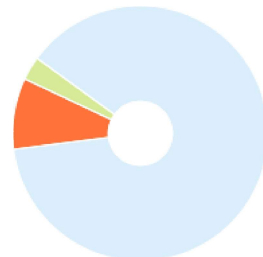
Отчет предоставлен сервисом «Антиплагиат» - <http://tsu.antiplagiat.ru>

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 180
Начало загрузки: 15.06.2023 10:16:07
Длительность загрузки: 00:00:25
Имя исходного файла:
PROBLEMY_PEREKHODA_NA_5G_V_ES_SOBIRO
V_S_S_032129 2212121.docx
Название документа:
PROBLEMY_PEREKHODA_NA_5G_V_ES_SOBIRO
V_S_S_032129 2212121
Размер текста: 156 кБ
Тип документа: Магистерская диссертация
Символов в тексте: 159441
Слов в тексте: 19880
Число предложений: 1214

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Начало проверки: 15.06.2023 10:16:32
Длительность проверки: 00:02:09
Комментарии: не указано
Поиск с учетом редактирования: да
Проверенные разделы: основная часть с. 2-3,5-62, содержание с. 4, приложение с. 72-80
Модули поиска: ИПС Адилет, Библиография, Сводная коллекция ЭБС, Интернет Плюс*, Сводная коллекция РГБ, Цитирование, Переводные заимствования (RuEn), Переводные заимствования по eLIBRARY.RU (EnRu), Переводные заимствования по коллекции Гарант: аналитика, Переводные заимствования по коллекции Интернет в английском сегменте, Переводные заимствования по Интернету (EnRu), Переводные заимствования по коллекции Интернет в русском сегменте, Переводные заимствования издательства Wiley, eLIBRARY.RU, СПС ГАРАНТ: аналитика, СПС ГАРАНТ: нормативно-правовая документация, Медицина, Диссертации НББ, Коллекция НБУ, Перефразирования по eLIBRARY.RU, Перефразирования по СПС ГАРАНТ: аналитика, Перефразирования по Интернету, Перефразирования по Интернету (EN), Перефразированные заимствования по коллекции Интернет в английском сегменте, Перефразированные заимствования по коллекции Интернет в русском сегменте, Перефразирования по коллекции издательства Wiley, Патенты СССР, РФ, СНГ, СМИ России и СНГ, Шаблонные фразы, Модуль поиска "tsu", Кольцо вузов, Издательство Wiley, Переводные заимствования



СОВПАДЕНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
9,41%	0%	3,07%	87,52%

Совпадения — фрагменты проверяемого текста, полностью или частично сходные с найденными источниками, за исключением фрагментов, которые система отнесла к цитированию или самоцитированию. Показатель «Совпадения» — это доля фрагментов проверяемого текста, отнесенных к совпадениям, в общем объеме текста.

Самоцитирования — фрагменты проверяемого текста, совпадающие или почти совпадающие с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа. Показатель «Самоцитирования» — это доля фрагментов текста, отнесенных к самоцитированию, в общем объеме текста.

Цитирования — фрагменты проверяемого текста, которые не являются авторскими, но которые система отнесла к корректно оформленным. К цитированиям относятся также шаблонные фразы; библиография; фрагменты текста, найденные модулем поиска «СПС Гарант: нормативно-правовая документация». Показатель «Цитирования» — это доля фрагментов проверяемого текста, отнесенных к цитированию, в общем объеме текста.

Текстовое пересечение — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.

Источник — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.

Оригинальный текст — фрагменты проверяемого текста, не обнаруженные ни в одном источнике и не отмеченные ни одним из модулей поиска. Показатель «Оригинальность» — это доля фрагментов проверяемого текста, отнесенных к оригинальному тексту, в общем объеме текста.

«Совпадения», «Цитирования», «Самоцитирования», «Оригинальность» являются отдельными показателями, отображаются в процентах и в сумме дают 100%, что соответствует полному тексту проверяемого документа.

Обращаем Ваше внимание, что система находит текстовые совпадения проверяемого документа с проиндексированными в системе источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности совпадений или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

№	Доля в тексте	Доля в отчете	Источник	Актуален на	Модуль поиска	Комментарии
[01]	3,47%	3,46%	Диплом ПЗ Князькин Антиплагиат.pdf	15 Фев 2023	Кольцо вузов	
[02]	1,92%	1,21%	Huawei in EU Countries: Participation in the Development of 5G Networks http://vestnikieran.instituteofeurope.ru	04 Ноя 2021	Перефразированные заимствования по коллекции Интернет в русском сегменте	
[03]	1,58%	0,58%	HUAWEI В СТРАНАХ ЕС: ПРОБЛЕМА УЧАСТИЯ В РАЗВИТИИ СЕТЕЙ 5G. http://elibrary.ru	09 Июл 2020	eLIBRARY.RU	
[04]	1,26%	1,26%	не указано	29 Сен 2022	Библиография	
[05]	1,15%	0%	Huawei in EU Countries: Participation in the Development of 5G Networks http://vestnikieran.instituteofeurope.ru	04 Ноя 2021	Интернет Плюс*	

[06]	1,13%	1,13%	https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf https://eca.europa.eu	30 Ноя 2022	Переводные заимствования по коллекции Интернет в английском сегменте	
[07]	1,13%	0,97%	Кашкин С.Ю., Четвериков А.О., Комментарий к основополагающим актам Европейского Союза в редакции Лиссабонского договора - 2008 г. http://ivo.garant.ru	09 Авг 2008	Переводные заимствования по коллекции Гарант: аналитика	
[08]	1,05%	1,05%	не указано	13 Янв 2022	Цитирование	
[09]	0,81%	0,41%	Huawei в странах ЕС: проблема участия в развитии сетей 5G – тема научной статьи по экономике и бизнесу читайте бесплатно текст научно-исследовательской работы в электронной библиотеке КиберЛенинка https://cyberleninka.ru	03 Июн 2023	Интернет Плюс*	
[10]	0,78%	0,49%	https://iorj.hse.ru/data/2021/12/14/1475910272/%D0%92%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA_2021_03-10_12_21.pdf https://iorj.hse.ru	24 Янв 2023	Переводные заимствования по коллекции Интернет в русском сегменте	
[11]	0,75%	0,75%	не указано	29 Сен 2022	Шаблонные фразы	
[12]	0,57%	0%	Международно-правовые и национально-правовые аспекты регулирования радиочастотного спектра (Ж. Дюмортье, И.Ю. Богдановская, Н. Вандезанде, журнал "Право. Журнал Высшей школы экономики", N 5, спецвыпуск 2021 г.) http://ivo.garant.ru	05 Фев 2022	Переводные заимствования по коллекции Гарант: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[13]	0,56%	0,56%	ВОПРОСЫ ИНВЕСТИЦИОННОЙ МИГРАЦИИ: АНАЛИЗ ПРОГРАММ СТРАН ЕВРОПЕЙСКОГО СОЮЗА. http://elibrary.ru	11 Фев 2019	Перефразирования по eLIBRARY.RU	
[14]	0,48%	0,12%	https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR_Vol_2_R.pdf https://itu.int	06 Фев 2023	Переводные заимствования по коллекции Интернет в русском сегменте	
[15]	0,29%	0,29%	https://iorj.hse.ru/data/2021/12/14/1475910272/%D0%92%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA_2021_03-10_12_21.pdf https://iorj.hse.ru	24 Янв 2023	Перефразированные заимствования по коллекции Интернет в русском сегменте	
[16]	0,27%	0%	Скачать Часть 1 https://naukaip.ru	09 Ноя 2022	Переводные заимствования по коллекции Интернет в русском сегменте	Источник исключен. Причина: Маленький процент пересечения.
[17]	0,24%	0%	Ценности Европейского Союза: понятие, правовая природа и влияние на конституционное право суверенных государств (Я.И. Лебедева, журнал "Журнал зарубежного законодательства и сравнительного правоведения", N 2, март-апрель 2022 г.) http://ivo.garant.ru	21 Мая 2022	Переводные заимствования по коллекции Гарант: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[18]	0,24%	0%	Акимов Л.Ю., Андриченко Л.В., Артемьева Е.А. и др. Разрешительная система в Российской Федерации: науч.-практич. пособие (отв. ред. А.Ф. Ноздрачев). - "Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФР... http://ivo.garant.ru	10 Дек 2016	Переводные заимствования по коллекции Гарант: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[19]	0,23%	0%	https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf https://eca.europa.eu	30 Ноя 2022	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[20]	0,2%	0%	https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2020-10%20Fudan%20Report_on_the_Cybersecurity.pdf?ver=1S1OWc8iFJFGOCkVPi467g%3D%3D https://airuniversity.af.edu	27 Окт 2022	Переводные заимствования по коллекции Интернет в английском сегменте	
[21]	0,19%	0,19%	Компетенция европейского союза в сфере здравоохранения (В.О. Тюменцев, журнал "Вестник Университета имени О.Е. Кутафина (МГЮА)", N 7, июль 2021 г.) http://ivo.garant.ru	30 Окт 2021	Переводные заимствования по коллекции Гарант: аналитика	
[22]	0,18%	0%	Опасные функции смартфона могут угрожать безопасности личным данным гражданам в РФ http://kursk.com	27 Апр 2021	СМИ России и СНГ	
[23]	0,18%	0%	Правовые триггеры цифровизации обращения с РАО и ОЯТ на территории Европейского союза (Л.М. Энтин, Ю.В. Лебедева, сетевое издание "Цифровое право (Digital Law Journal)", N 1 (том 3), январь-март 2022 г.) http://ivo.garant.ru	07 Мая 2022	Переводные заимствования по коллекции Гарант: аналитика	

[24]	0,16%	0%	Правовое регулирование цифрового банкинга в России и зарубежных странах (Европейский союз, США, КНР) (Е.П. Ермакова, Е.Е. Фролова, журнал "Вестник Пермского университета. Юридические науки", выпуск 4, октябрь-декабрь 2019 г.) http://ivo.garant.ru	18 Янв 2020	Переводные заимствования по коллекции Гарант: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[25]	0,16%	0%	Contents Administration.....9 I. Message from the President..... http://eett.gr	06 Янв 2018	Переводные заимствования (RuEn)	Источник исключен. Причина: Маленький процент пересечения.
[26]	0,16%	0%	https://conf.iict.kz/wp-content/uploads/2021/06/collection-apibk2021.pdf https://conf.iict.kz	30 Ноя 2022	Переводные заимствования по коллекции Интернет в русском сегменте	Источник исключен. Причина: Маленький процент пересечения.
[27]	0,15%	0%	Директива Европейского Парламента и Совета Европейского Союза 2018/1972 от 11 декабря 2018 г. об установлении Европейского Кодекса электронных коммуникаций (новая редакция) http://ivo.garant.ru	11 Ноя 2019	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[28]	0,15%	0%	Директива Европейского Парламента и Совета Европейского Союза 2018/1972 от 11 декабря 2018 г. об установлении Европейского Кодекса электронных коммуникаций (новая редакция) http://ivo.garant.ru	11 Ноя 2019	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[29]	0,15%	0%	Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации (А.Ю. Чурилов, журнал "Вестник Омской юридической академии", N 1, январь-март 2019 г.) http://ivo.garant.ru	20 Апр 2019	Переводные заимствования по коллекции Гарант: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[30]	0,14%	0%	СИСТЕМА И СПОСОБ УЛУЧШЕНИЯ РАБОТЫ МЕДИАСЕРВЕРА. http://elibrary.ru	29 Авг 2014	eLIBRARY.RU	Источник исключен. Причина: Маленький процент пересечения.
[31]	0,13%	0%	https://fips.ru/patent-analytics-new/5g-web.pdf https://fips.ru	13 Мар 2023	Переводные заимствования по коллекции Интернет в русском сегменте	Источник исключен. Причина: Маленький процент пересечения.
[32]	0,13%	0%	ОТЧЕТ МСЭ-R SM.2093. Руководство по регламентарной структуре для управления использованием спектра на национальном уровне Pandia.ru http://pandia.ru	09 Янв 2017	ПЕРЕФРАЗИРОВАНИЯ ПО ИНТЕРНЕТУ	Источник исключен. Причина: Маленький процент пересечения.
[33]	0,12%	0%	Современные средства связи http://bsac.by	26 Окт 2022	Переводные заимствования по коллекции Интернет в русском сегменте	Источник исключен. Причина: Маленький процент пересечения.
[34]	0,11%	0%	запись потока мультимедийных данных в трек указаний о приеме контейнерного медиафайла - патент РФ 2434277 - ХАННУКСЕЛА Миска (FI) (2/2) http://freepatent.ru	01 Янв 2017	ПЕРЕФРАЗИРОВАНИЯ ПО ИНТЕРНЕТУ	Источник исключен. Причина: Маленький процент пересечения.
[35]	0,11%	0%	ershova_e_a_evolyuciya-evropeyskogo-podhoda-k-obespecheniyu-tehnologicheskogo-suvereniteta-v-usloviyah-formirova.pdf	30 Мая 2023	Кольцо вузов	Источник исключен. Причина: Маленький процент пересечения.
[36]	0,11%	0%	EPRA News https://epra.org	14 Апр 2020	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[37]	0,1%	0%	Украина присоединилась к Европейскому механизму взаимодействия СЕФ - Омелян http://bin.ua	17 Авг 2019	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[38]	0,09%	0%	https://www.imemo.ru/files/File/ru/publ/2020/2020-016.pdf https://imemo.ru	03 Мая 2022	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[39]	0,09%	0%	Помпео: США добились прогресса в убеждении ЕС в рисках использования технологий Huawei http://news.am	17 Авг 2019	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[40]	0,09%	0%	https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1341&context=njtip https://scholarlycommons.law.northwestern.edu	03 Июн 2023	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[41]	0,09%	0%	Подвижная радиосвязь https://e.lanbook.com	21 Янв 2020	Сводная коллекция ЭБС	Источник исключен. Причина: Маленький процент пересечения.
[42]	0,09%	0%	Подвижная радиосвязь http://studentlibrary.ru	20 Дек 2016	Медицина	Источник исключен. Причина: Маленький процент пересечения.
[43]	0,09%	0%	http://www.sov-europe.ru/2019/2-2019/7.pdf http://sov-europe.ru	22 Янв 2020	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.

[44]	0,08%	0%	Цифровая трансформация и государственное управление: научно-практическое пособие (Емельянов А.С., Ефремов А.А., Калмыкова А.В. и другие; ред. кол.: д.ю.н., доц., Л.К. Терещенко, д.ю.н., доц. А.С. Емельянов, д.ю.н., проф. Н.А. Поветкина). - "Инфотропик ... http://ivo.garant.ru	30 Июл 2022	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[45]	0,07%	0%	Защити свой компьютер на 100 % от вирусов и хакеров http://ibooks.ru	09 Дек 2016	Сводная коллекция ЭБС	Источник исключен. Причина: Маленький процент пересечения.
[46]	0,07%	0%	Регламент Европейского Парламента и Совета Европейского Союза 2021/523 от 24 марта 2021 г. о принятии программы InvestEU, а также об изменении Регламента ЕС 2015/1017 http://ivo.garant.ru	11 Авг 2022	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[47]	0,06%	0%	EPRA News https://epra.org	14 Апр 2020	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[48]	0,05%	0%	https://research-api.cbs.dk/ws/portalfiles/portal/62183252/818897_MSc_Thesis_Waldemarsson_Sarasto_Lowenberg.pdf https://research-api.cbs.dk	03 Июн 2023	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[49]	0,05%	0%	https://www.rulit.me/data/programs/resources/pdf/Ven_Seti-6G-Put-ot-5G-k-6G-glazami-razrabotchikov_RuLit_Me_678557.pdf https://rulit.me	24 Фев 2022	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[50]	0,05%	0%	https://www.rulit.me/data/programs/resources/pdf/Ven_Seti-6G-Put-ot-5G-k-6G-glazami-razrabotchikov_RuLit_Me_678557.pdf https://rulit.me	31 Мая 2022	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[51]	0,05%	0%	Право цифровой среды (монография) (коллектив авторов; под ред. к.ю.н., доц. Т.П. Подшивалова, к.ю.н., доц. Е.В. Титовой, к.ю.н., доц. Е.А. Громовай). - "Проспект", 2022 г. http://ivo.garant.ru	20 Авг 2022	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[52]	0,04%	0%	https://unecon.ru/sites/default/files/1sbornik_sov.molodyh_uchenyh.pdf https://unecon.ru	06 Сен 2022	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[53]	0,02%	0%	https://russiancouncil.ru/papers/Sactions2020-Report51-Rus.pdf https://russiancouncil.ru	27 Апр 2020	Интернет Плюс*	Источник исключен. Причина: Маленький процент пересечения.
[54]	0,01%	0%	Дорофеева Дипломная работа.pdf	14 Июн 2021	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.
[55]	0,01%	0%	Диссертация	25 Мая 2021	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.
[56]	0,01%	0%	РАЗРАБОТКА РАБОЧЕЙ ПРОГРАММЫ КУРСА ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «ЦИФРОВАЯ КАРТОГРАФИЯ»	26 Мая 2023	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.
[57]	0,01%	0%	ВКР Крахмелец Л.А. 022110	05 Июн 2023	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.
[58]	0,01%	0%	ВКР_ШаколкинаСА.docx	15 Июн 2022	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.
[59]	0,01%	0%	Диплом Янковская pdf.pdf	19 Июн 2020	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.
[60]	0,01%	0%	Борисова	08 Июн 2020	Модуль поиска "tsu"	Источник исключен. Причина: Маленький процент пересечения.