ЦИФРОВАЯ
ЭКОНОМИКА
D-ECONOMY.RU

Дайджест по телеком рынку:

системные проблемы и новые вызовы 1 полугодие 2025 года

АНО «Цифровая экономика» ——— 2025

Содержание

Содержание 2
Основные тренды развития регулирования телекоммуникационного сектора 4
Внедрение 5G Advanced / 6G 6
США 6
Великобритания 11
ЕС 11
Международные организаций в сфере связи и международное сотрудничество 12
Индия 12
Стимулирование разработки и внедрения новых технологий связи и телекоммуникации, в том числе интернета вещей и eSim 15
США 15
Южная Корея 16
Международные организаций и международное сотрудничество в сфере связи 17
Безопасность связи и коммуникаций, в том числе требования для операторов связи 18
Великобритания 19
ЕС 20
Япония 22
Южная Корея 23
Международные организаций в сфере связи и международное сотрудничество 24
Борьба с мошенничеством и антифрод 25
Южная Корея 25
Борьба со спам-звонками 26
США 26
Южная Корея 27
Индия 27
Импортозамещение оборудования связи и телекоммуникаций 31
США 31
ЕС 33
Китай 35
Южная Корея 36
Индия 36
Международные организаций в сфере связи и международное сотрудничество 37

Идентификация абонентов 39
США 39
Индия 40
Доступ правоохранительных органов к данным операторов связи 41
США 41
Источники 42

Основные тренды развития регулирования телекоммуникационного сектора

Регуляторные инициативы, внесенные на рассмотрение, принятые и / или вступившие в силу за рассмотренный период, направлены на повышение доступности интернета для населения, стимулирование развития сетей связи нового поколения и интернета вещей, повышение безопасности связи, борьбу с мошенничеством. Сохраняется тренд на поддержку развития собственного производства компонентной базы, который особенно ярко выражен в США в рамках торговой войны с Китаем.

В части **повышения доступности интернета** рассмотренные государства прилагают усилия по достижению 100% покрытия сетью Интернет территории своих стран. Это происходит в том числе за счет развития и использования спутниковой связи. В частности, в США рассматривается вопрос о расширении диапазона частот, предназначенных для спутниковой связи. Продолжается развитие инициатив, направленных на повышение качества и скорости доступа в интернет, в том числе за счет развития оптоволоконных линий связи.

Значимое число инициатив связано с **развитием сетей связи нового поколения и интернета вещей.** Особенно активны в данном направлении США, где предпринимаются шаги по переводу закрытых для использования диапазонов частот в коммерческое использование для стимулирования развития сетей 5G и других перспективных технологий связи. Также в США принят ряд инициатив, направленных на расширение использования беспилотных транспортных средств.

В области **обеспечения безопасности** отмечаются инициативы, направленные на модернизацию подходов к обеспечению кибербезопасности на фоне растущего числа киберугроз. Так, в Японии был принят закон об активной кибероборонe, о планах по принятию нового закона о кибербезопасности заявила Великобритания, план по управлению киберинцидентами был представлен в ЕС. Также в ответ на участившиеся случаи повреждения подводной инфраструктуры в ЕС был представлен план по усилению безопасности подводных кабелей. В США был предпринят ряд мер в связи с атаками на телекоммуникационный сектор, приписываемых группе хакеров “Соляной тайфун”.

Продолжается «донастройка» законодательства, регулирующего **борьбу со спамом и мошенничеством.** Так:

- В Южной Корее Комиссия по коммуникациям в сотрудничестве с Агентством интернета и безопасности и Samsung Electronics объявила о разработке функции на основе искусственного интеллекта (далее – ИИ), которая будет

автоматически блокировать на смартфонах сообщения с подозрением на вредоносный контент

- В США скорректированы правила блокировки вызовов, которые вступят в силу с 2026 года (блокировка должна производиться на основании любого обоснованного списка телефонных номеров, которые не используются для исходящих звонков (Do Not Originate list). Также рассматриваются предложения по изменению правил аутентификации абонентов в целях защиты пользователей от роботизированных звонков с подменой номера, которые совершаются с использованием сетей без IP.

- В Индии установлены подробные критерии для наложения штрафов на поставщиков услуг связи и информации за нарушение обязательств по предотвращению спама в зависимости от количества нарушений. Одновременно введены дополнительные финансовые санкции для операторов связи за искажение информации о спаме.

Кроме того, предпринимаются меры по идентификации входящих звонков, чтобы пользователи могли отличать телемаркетинговую коммуникацию (Индия - принято на уровне законодательства, США - на уровне рекомендаций Федеральной комиссии по связи).

Программа **импортозамещения оборудования** концентрируется в области государственной поддержки на строительство заводов по производству полупроводников, в т.ч.:

- 920 млн евро выделено из бюджета Германии на строительство компанией Infineon нового завода по производству полупроводников в Дрездене.

- Европейская комиссия провела церемонию, посвящённую запуску первых пяти пилотных линий в рамках инициативы «Чипы для Европы».

- Южная Корея объявила об увеличении пакета мер поддержки полупроводниковой промышленности до 33 трлн вон (23 млрд долл. США).

- США проводят «шоковую политику» в отношении торговых партнеров, пытаясь пересмотреть устоявшиеся двусторонние и многосторонние торговые соглашения. Президент США Дональд Трамп продолжает «войну чипов», ограничивая доступ иностранных потребителей к американским микросхемам. Постепенно в войну втягиваются все страны, имеющие отношение к производству полупроводников.

Внедрение 5G Advanced / 6G

США

Апелляционный суд шестого округа США в январе 2025 года отменил правило сетевой нейтральности[1], постановив, что правительство не имеет права причислять провайдеров широкополосного интернета к поставщикам телекоммуникационных услуг. Суд определил, что интернет-провайдеры в США относятся к поставщикам информационных услуг в соответствии с "Законом о телекоммуникациях 1996 года", на которые действие принципа сетевой нейтральности не распространяется.

Палата представителей повторно представила проект Закона о будущем использовании технологий для создания надёжных и усовершенствованных («FUTURE») сетей[2], предполагающий создание рабочей группы 6G[3], в которую войдут представители телекоммуникационной отрасли, общественных организаций и федерального правительства. Рабочая группа 6G будет отвечать за предоставление информации о беспроводной технологии 6G, в том числе о статусе разработки отраслевых стандартов, ограничениях 6G и о том, как организации на всех уровнях власти могут использовать 6G.

Палата представителей также повторно внесла на рассмотрение законопроект о продвижении лидерства США в органах, устанавливающих стандарты для сетей 5G, а также для будущих поколений телекоммуникационных сетей (Международный союз электросвязи, 3GPP, Институт инженеров электротехники и электроники и др.)[4].

Предприняты очередные шаги по созданию механизма перевода закрытых диапазонов радиочастотного спектра в открытое коммерческое использование. В январе 2025 года на рассмотрение внесен законопроект[5], который направлен на введение в коммерческое использование диапазон от 1,3 до 13,2 ГГц, который в настоящее время используется федеральными ведомствами, что является важным шагом для развития сетей 5G и других перспективных технологий связи. Закон требует выделения как минимум 2500 МГц спектра в диапазоне 1,3 - 13,2 ГГц для переквалификации его для коммерческого использования. Из них как минимум 1250 МГц должны быть доступны для полноценного лицензированного коммерческого использования. На выделение 1250 МГц отводится 2 года, на выделение остального диапазона - 5 лет.

Аукционы на распределение частот в выделенных 1250 МГц должны быть организованы Федеральной комиссией по электросвязи (далее - FCC). Для этого

закон продлевает полномочия FCC по проведению аукционов по передаче частот спектра в среднем диапазоне.

FCC предпринимает шаги по инициации торгов лицензиями на спектр AWS-3.1. FCC опубликовала Уведомление о предлагаемом нормотворчестве[6], в котором предлагается обновить правила, относящиеся к конкретным услугам для диапазонов спектра AWS-3 (диапазоны 1695-1710 МГц, 1755-1780 МГц и 2155-2180 МГц) путём согласования условий участия организаций в торгах.

«Закон о спектре, безопасных технологиях и инновациях» 2024 года обязывает FCC инициировать конкурсные торги на использование спектра AWS-3.1. Вырученные от аукциона средства планируется направить на поддержку программы FCC по возмещению поставщикам услуг связи расходов на замещение оборудования и услуг поставщиков Huawei Technologies Company и ZTE Corporation, признанных ненадежными в соответствии с «Законом о безопасных и надежных сетях связи» от 2019 года. Данное уведомление FCC является первым шагом на пути к организации торгов. В нем предлагается модернизировать существующие правила проведения торгов подобными лицензиями в соответствии с более современной практикой FCC в области аукционов на выделение частот.

FCC рассматривает целесообразность совместного использования диапазона 1675–1680 МГц[7]. Запрошены комментарии заинтересованных лиц.

В ноябре 2024 года Национальное управление телекоммуникаций и информации Министерства торговли США (далее - NTIA) пришло к выводу о том, что использование диапазона 1675–1680 МГц совместно с коммерческими беспроводными сервисами технически возможно при соблюдении определённых условий. В настоящее время он используется Национальным управлением океанических и атмосферных исследований для передачи срочных спутниковых данных.

NTIA и NASA рекомендовали выделить диапазон 18 ГГц (18,1–18,6 ГГц) для совместного использования коммерческим компаниями в космической деятельности и федеральными структурами[8]. Это соответствует результатам Всемирной конференции радиосвязи 2023 года (ВКР-23), на которой полоса частот 18 ГГц была выделена для связи «космос-космос» по всему миру[9].

FCC предпринимает регулирующие действия и инициативы в нижнем диапазоне 37–37,6 ГГц. 29 апреля 2025 года FCC опубликовала документ[10] который, среди прочего, устанавливает систему лицензирования для федерального и коммерческого использования частот, учитывая приоритетный доступ для военных систем.

Принятая система лицензирования для данного диапазона предполагает получение частными компаниями общенациональной неисключительной

лицензии, и только после этого подачу ими заявки на регистрацию на конкретном объекте.

FCC запрашивает комментарии касательно изменения ограничения по мощности и внеполосным излучениям для диапазона 4,9 ГГц, предназначенного для использования в целях общественной безопасности[11].

В частности, рассматривается вопрос о том, чтобы:

- максимальная эффективная изотропно излучаемая мощность (EIRP) для базовых станций в диапазоне 4,9 ГГц составляла 3280 Вт/МГц, а для мобильных и портативных станций в этом диапазоне — 2 Вт EIRP;
- ограничить максимальную выходную мощность базовых станций, излучающих за пределами разрешённой лицензиатом полосы частот, до -13 дБм/МГц;
- ограничить плотность потока мощности в любом месте на границе зоны обслуживания лицензиата до -76 дБм/м2 /МГц при измерении на высоте 1,5 метра над землёй.

Предполагается, что изменения могут способствовать более эффективному развёртыванию 5G в этом диапазоне.

FCC запросила комментарии касательно предложения о предоставлении спектра частот 12,7 ГГц и 42 ГГц для спутниковой связи в качестве альтернативы или дополнения к наземной беспроводной связи, в том числе о разрешении использования спутниковой связи «Земля-космос» и «космос-Земля».[12] Оба диапазона соседствуют со спектрами, уже используемыми для спутниковой связи.

В настоящее время нормативные ограничения препятствуют интенсивному использованию диапазона 12,7–13,25 ГГц для спутниковой связи, а диапазон 42,0–42,5 ГГц не используется.

FCC разрешила вывод на рынок мобильных устройств производителей Ericsson и Samsung, работающих как в диапазоне 3,5 ГГц, так и в диапазоне 3,7 ГГц на основании запросов производителей[13]. Комиссия посчитала, что разрешение на продажу таких устройств отвечает общественным интересам, поэтому для них были сделаны исключения в виде неприменения к данным устройствам положений разделов 96.41(e) и 2.947(f) правил FCC.

FCC изучает возможность использования верхнего С-диапазона (3,98-4,2 ГГц)[14] **для коммерческих беспроводных услуг.** FCC запросила комментарии о том, следует ли полностью или частично перепрофилировать верхний С-диапазон для использования в целях предоставления коммерческих беспроводных услуг, и, если да, то какой объем спектра должен быть предоставлен и каким образом.

Одновременно FCC запросила комментарии о том, как перепрофилирование диапазона повлияет на радиовысотомеры, которые работают в соседнем диапазоне 4,2–4,4 ГГц.

Сенат внёс на рассмотрение законопроекты об оценке[15] и аудите[16] спектра, используемого государственными структурами.

В случае их принятия NTIA будет обязана периодически оценивать стоимость и проводить аудит спектра, закреплённого за государственными организациями или выделенного им. Оценка будет основываться на максимальной потенциальной стоимости спектра в случае его перераспределения для коммерческого использования.

По итогам Конгрессу будет представляться отчёт о результатах аудита.

T-Mobile официально стал первым провайдером сетей в Соединённых Штатах, предлагающим общенациональное покрытие 5G Advanced[17].

16 апреля закончился приём заявок в рамках третьего раунда Wireless Innovation Fund[18]. Поступило 94 заявки на сумму почти 3 млрд долл. США государственного финансирования, предполагающие привлечение более 1,3 млрд долл. США частных инвестиций.

Программы в этом раунде финансирования направлены на инвестиции в программные решения:

- использующие данные из интерфейсов Open RAN и/или инновации, характерные для Open RAN, для повышения энергоэффективности, экономии средств, увеличения производительности или получения других преимуществ для отраслей (например, коммунального хозяйства, горнодобывающей промышленности, производства, беспилотной авиации);
- снижающие стоимость и сложность интеграции с несколькими поставщиками за счёт автоматизации.

В рамках первых двух раундов финансирования NTIA выделила более 550 млн долл. США на 35 проектов. Первый раунд был направлен на поддержку тестирования, исследований, разработок и создание испытательных центров, второй — на стимулирование инноваций и коммерциализацию открытых радиоустройств.

NTIA в начале года (при администрации президента США Джо Байдена) одобрило первоначальные предложения ряда штатов по программе BEAD (Broadband, Equity, Access, and Deployment), направленную на расширение высокоскоростного широкополосного интернет-доступа[19]. Бюджет программы составляет 42,45 млрд долл. США. Программа предполагает инвестиции на

федеральном уровне в высокоскоростной и доступный Интернет. Программа должна стимулировать провайдеров к строительству инфраструктуры широкополосной связи в районах, которые экономически непривлекательны для частных вложений без соответствующих государственных инвестиций, таких как сельские общины с небольшим количеством домов. Средства по программе в течение предыдущих трех лет выделялись, но не расходовались[20].

Из бюджета BEAD в начале января 2025 года выделены средства на финансирование окончательных предложений штатам:

- Невада - более 416 млн долл. США[21] на подключение более 43,5 тыс. домохозяйств и предприятий к Интернету;
- Делавэр - более 107 млн долл. США[22] на подключение 5,7 тыс. домохозяйства и предприятий к Интернету;
- Луизиана - более 1,3 млрд долл. США[23] для подключения 140 тыс. домохозяйств и предприятий.

По состоянию на середину декабря 2024 года одобрены первоначальные предложения 56 штатов и территорий на сумму 42,45 млрд долл. США.

В 2023 году первоначальное одобрение получила заявка Луизианы[24] на 12,7 млн долл. США[25].

В соответствии с условиями программы через год после утверждения первоначального предложения штаты должны представить окончательное предложение, в котором, помимо прочего, подробно описывается результат процесса и отбора получателей субгрантов. Соблюдение данных требований необходимо для выделения средств.

При этом с момента запуска программы в 2021 году фактического выделения средств по ней не было[26].

Планируется пересмотр требований BEAD.

16 января 2025 года рекомендовано выделить более 162 млн долл. США[27] по 4 заявкам (Taos Pueblo, Pueblo de Cochiti, Kawerak, Inc, Old Harbor Native Corporation) на проведение волоконно-оптической линии связи на землях коренных народов из бюджета программы о предоставлении услуги по широкополосной передаче данных для коренных народов.

В начале января выделено 18 млн долл. США 7 организациям коренных народов для расширения доступа к высокоскоростному интернету[28].

Из Фонда инноваций в области беспроводной связи (с капиталом в 1,5 млрд долл. США) NTIA выделено:

- более 117 млн долл. США[29] на девять проектов; из них почти 10 млн долл. США получит Rampart Communications, Inc. на проект ASPEN (компания Rampart в сотрудничестве с Технологическим институтом Вирджинии создаст новую технологию физического уровня 6G для провайдеров мобильных беспроводных сетей);

- более 19 млн долл. США[30] (в рамках третьей и последней серии грантов по второму уведомлению о возможностях финансирования) на два проекта. Из них более 9 млн долл. США получит компания Recon RF, Inc. на проект по проведению исследований и разработок создания сверхэффективных интерфейсных модулей для открытых радиомодулей 5G/6G нового поколения.

17 января 2025 года NTIA рекомендовало выделить из конкурсной грантовой программы Digital Equity (общий объем финансирования программы - 1,25 млрд долл. США), более 369 млн долл. США 41 организации для поддержки проектов по развитию цифровых навыков и инклюзивности в сообществах по всей стране[31].

Великобритания

Управление по телекоммуникациям (далее – Ofcom) предложило не регулировать цены на высокоскоростной доступ к широкополосному интернету до 2031 года с одновременным обеспечением скорости до 80 Мбит/с для пользователей медно-волоконных линий[32].

Планируется, что к 2027 году 96% жилых домов будет обеспечено оптоволоконным покрытием. Предполагается ограничить цены на услуги доступа к интернету с низкой скоростью, сохраняя доступность для тех, кто пользуется более старыми медно-волоконными линиями. Ограничение будет распространяться на тарифы BT Openreach для подключений со скоростью до 80 Мбит/с, что больше текущего лимита в 40 Мбит/с.

Консультации регулятора по этим предложениям продлятся до 12 июня, а окончательное решение будет принято в марте 2026 года.

ЕС

Федеральное министерство цифровых технологий и транспорта Германии объявило о начале программы «Gigabit Funding 2025»[33]. На устранение цифрового неравенства будет выделено 1,2 млрд евро.

Финансирование покрывает около 50-70% затрат на развертывание гигабитных сетей, а также 100% затрат на внешние консультации и проектно-изыскательские работы. Бюджеты выделяются районам, где подключение объектов ниже 100 Мбит/с. При этом социальные объекты имеют право на финансирование вне

зависимости от текущей скорости. Заявки могут подавать муниципалитеты, сельские районы, ассоциации местных органов власти и компании с госучастием.

Международные организаций в сфере связи и международное сотрудничество

В феврале 2025 года в ходе заседания рабочей группы Международного союза электросвязи МСЭ-R WP5D обсуждено[34] большое количество материалов по разработке проекта документа «Минимальные требования к техническим характеристикам (TPRS) для радиоинтерфейса (ов) IMT-2030 (6G)».

По итогам обсуждения составлен предварительный список минимальных технических характеристик и обновлён рабочий документ.

В июне 2026 года планируется выпустить технический отчёт 38-й серии «Исследование сценариев и требований 6G».

Индия

В 2025 году закончился первый этап (поддержка исследований) и начался второй (разработка концепции и коммерциализации технологических решений) Дорожной карты по развитию и внедрению технологии 6G в Индии «Bharat 6G Vision Document»[35].

Началась реализация Национальной широкополосной миссии (NBM) 2.0[36], направленной на расширение покрытия волоконно-оптическими линиями и покрытия 5G на территории Индии.

В ее рамках к 2030 году планируется:

- увеличить количество подключённых по волоконно-оптическому кабелю деревень до 270 тыс. (сейчас подключено 50 тыс.);
- обеспечить широкополосным доступом не менее 90% основных учреждений, таких как школы, центры первичной медико-санитарной помощи;
- увеличить скорость широкополосного проводного интернета со среднего по стране показателя 63,55 Мбит/с в ноябре 2024 года до не менее 100 Мбит/с;
- не менее 30% всех вышек мобильной связи в стране должны работать на устойчивой энергии;
- доля подключенных домохозяйств в сельских районах должна вырасти с 45% до 60%.

Министерство информации и телерадиовещания Индии (далее - MIB) предложило комплексную нормативно-правовую базу для наземных вещательных компаний[37]. Эта инициатива направлена на использование достижений в области наземных коммуникационных технологий, что позволит вещательным компаниям предоставлять телевизионные каналы операторам распределительных платформ (DPO) с помощью кабельных, волоконно-оптических и сотовых сетей, Wi-Fi или облачных технологий. В настоящее время согласно представленному в 2022 году MIB «Руководству по восходящему и нисходящему вещанию спутниковых телеканалов в Индии в 2022 году» для телерадиовещания необходимо использовать спутниковые каналы.

Управление по регулированию телекоммуникаций Индии (далее - TRAI) предложило разрешить ряду компаний (Infosys, Tata Communications, Larsen&Toubro) стать провайдерами частных сетей 5G для предприятий по всей стране с помощью прямого доступа к спектру[38].

Предполагается, что использование собственных сетей 5G обойдется компаниям на 40% дешевле, чем использование инфраструктуры операторов или аренда у них частот.

TRAI опубликовало проект постановления о тарифах на телекоммуникационные услуги (71-я поправка) от 2025 года «О рационализации тарифов на широкополосную связь для точек коллективного доступа в Интернет (PDO) в рамках схемы PM-WANI»[39], предполагающий снижение тарифов на широкополосную связь для PDO в рамках схемы PM-WANI до размера, не превышающего в два раза тариф, применимый к розничным услугам широкополосной связи (FTTH) соответствующей пропускной способности, предлагаемого поставщиком услуг.

Необходимость внесения поправок обусловлена существенным отставанием от запланированных показателей программы PM-WANI, направленной на расширение общедоступного доступа к WiFi по всей Индии (к 2030 году - 50 млн точек коллективного WiFi-доступа). Основным негативным фактором является высокая стоимость подключения к интернету и аренды сетей, которую устанавливают поставщики телекоммуникационных услуг и интернет-провайдеры. В результате многие потенциальные операторы PDO неохотно инвестируют в инфраструктуру, необходимую для предоставления общедоступных услуг WiFi.

Департамент телекоммуникаций Индии ввёл новые требования на выдачу лицензий для провайдеров спутниковой связи[40]. Новые нормы касаются как уже работающих так и новых операторов, включая Starlink и Kuiper (принадлежит Amazon).

В частности, правила требуют создания специальных мониторинговых зон внутри Индии вдоль сухопутных и морских границ (на расстоянии до 50 км и до 200

морских миль соответственно от рубежей). Это требуется для того, чтобы органы безопасности могли отслеживать трафик на этих территориях.

Среди прочих требований значатся:

- получатели лицензии должны закрывать доступ к сайтам, заблокированным в Индии;
- операторы должны незамедлительно прекращать работу терминала, если власти считают, что он используется для мошеннических действий;
- сами терминалы должны быть зарегистрированы в Индии и обспечивать регулярную верификацию оборудования.

Стимулирование разработки и внедрения новых технологий связи и телекоммуникации, в том числе интернета вещей и eSim

США

FCC предоставила операторам беспилотных авиационных систем (БАС) доступ к диапазону 5030–5091 МГц.[41] Одна или несколько систем динамического управления частотами (DFMS) будут управлять и координировать доступ к спектру и обеспечивать его безопасное и эффективное использование, предоставляя операторам-заявителям временные частоты для поддержки связи по каналу управления БАС с уровнем надёжности, подходящим для операций в контролируемом воздушном пространстве и в других условиях, критически важных для безопасности.

Ранее эти операции проводились в центральной части диапазона, на значительном расстоянии от частот, смежных с 5030–5091 МГц, в целях минимизации рисков для смежных пользователей.

FCC запросила комментарии о предлагаемых изменениях правил обслуживания диапазонов[42] **для беспилотных летательных аппаратов и систем усовершенствованной (повышенной) воздушной мобильности (новая аэромобильность)**[43]**, в частности об:**

- определении терминов: беспилотные авиационные системы (UAS CNPC); беспилотные летательные аппараты (UAS); воздушное судно, эксплуатируемое без возможности прямого вмешательства человека изнутри воздушного судна или на нем (UA);
- открытии диапазона 450 МГц для авиационных командно-диспетчерских операций; предоставлении единой общенациональной лицензии в этом диапазоне; а также принятии гибких правил лицензирования, эксплуатации и технических правил, которые будут способствовать эффективному использованию диапазона на разных высотах, сводя к минимуму помехи для соседних операций;
- расширении операций радиолокации в диапазоне 24,45–24,65 ГГц, разрешив в нем вторичные операции радиолокации, что позволит обнаруживать, например, беспилотные летательные аппараты на общественных мероприятиях и объектах, которые по своей природе являются объектами незаконного наблюдения или контрабандных поставок (стадионы, тюрьмы, граница США и объекты критически важной инфраструктуры). Полученная информация не будет использована в

навигационных целях. Таким образом, повысится эффективность применения недостаточно используемого сегмента спектра;

- изменении ограничений мощности, установленных для коммерческих авиационных систем «воздух-земля» в диапазонах 849-851 МГц и 894-896 МГц, которые используются для подключения во время полёта. В настоящее время рабочая мощность определяется по пиковой мощности. Вместо этого предлагается измерять и регулировать эффективную мощность излучения в соответствии со средней мощностью;

- предлагаемых изменениях в правила предоставления услуг в шаге сетки частот 650 килогерц на частоте 450 МГц. В настоящее время воздушно-наземная связь в этой полосе частот ограничена голосовой связью с воздушными судами, летящими на больших высотах, фактически запрещена связь на больших расстояниях и на малых высотах. Изменения позволят обеспечить расширение операций БПЛА на различных высотах, включая меньшие высоты, разрешив использование диапазона для управления беспилотными авиационными системами и связью без полезной нагрузки (UAS CNPC) и поддержания операций систем усовершенствованной (повышенной) воздушной мобильности. Для внедрения этих изменений предлагается:

  - внедрить лицензию по географической структуре с общенациональным охватом (в настоящее время на этот диапазон выдано 53 лицензии одному лицензиату), установив в т.ч. новые требования к лицензиату;
  - разрешить передачу определённых данных беспилотных летательных аппаратов в полосе 450 МГц[44];
  - создать новую наземно-воздушную службу для охвата всех существующих операций наземно-воздушных и беспилотных авиационных систем в диапазоне 450 МГц, что может способствовать развитию систем усовершенствованной (повышенной) воздушной мобильности.

Южная Корея

Корейская комиссия по коммуникациям (KCC) объявила[45], что для устранения неудобств, с которыми сталкиваются пользователи при обмене файлами большого размера, она приняла меры по внедрению Apple RCS на iPhone в качестве замены существующих сервисов обмена сообщениями.

RCS — это усовершенствованная версия службы коротких сообщений (SMS) и службы мультимедийных сообщений (MMS), которая предлагает такие функции, как передача больших файлов (до 300 МБ) и уведомления о прочтении.

Пользователи iPhone и Galaxy смогут обмениваться файлами большого размера. В настоящее время ограничение – 1 Мб.

Международные организаций и международное сотрудничество в сфере связи

Rakuten Mobile (японский оператор мобильной связи) будет поддерживать американских разработчиков радиомодулей (RU), поддерживающих открытую архитектуру (open radio units (RUs))[46] (Battelle Memorial Institute, Microelectronics Technology, Eridan Communications и Airspan Networks[47]), в рамках проекта NTIA по развитию Open RAN при финансовой поддержке Фонда инноваций в сфере беспроводной связи[48].

Безопасность связи и коммуникаций, в том числе требования для операторов связи

США

В рамках борьбы с кибератаками на телекоммуникационный сектор, обострившейся в связи с деятельностью группы хакеров, известной как «Соляной тайфун», FCC учредила подразделение национальной безопасности для повышения устойчивости телекоммуникационного сектора США[49], снижения зависимости от иностранных цепочек поставок, борьбы с киберугрозами и шпионажем, а также стратегической конкуренцией в сфере критически важных технологий.

В его состав войдут представители восьми различных бюро и отделов агентства.

Цели совета:

- снизить зависимость от иностранных компаний в цепочках поставок телекоммуникационных услуг и технологий в США;
- устранить уязвимости, связанные с киберугрозами, шпионажем и слежкой;
- поддержать лидерство США в гонке технологий, включая 5G, спутники, квантовые вычисления, Интернет вещей и робототехнику.

На фоне продолжающейся борьбы с кибератаками на сектор телекоммуникаций, приписываемых группе "Соляной тайфун", FCC 15 января 2025 года опубликовала Декларативное постановление и уведомление о предлагаемом нормотворчестве (NPRM)[50].

Предлагается требовать от операторов связи защищать свои сети от незаконного доступа или перехвата сообщений, и уполномочить FCC принимать правила, реализующие это требование. Одновременно предлагается требовать от поставщиков услуг связи разработать и внедрить комплексные планы по обеспечению кибербезопасности и управлению рисками в цепочке поставок, направленные на повышение безопасности их сетей и упрощение контроля FCC за сетевой инфраструктурой и методами управления этих поставщиков, а также обязать поставщиков связи проходить ежегодную сертификацию, подтверждающую, что они разработали, обновили и внедрили планы управления рисками в соответствии с Системой кибербезопасности Национального института стандартов и технологий (NIST).

Новый председатель FCC Брендан Карр выступил с заявлением, в котором не согласился с действиями FCC и оспорил ее юридические полномочия в этой сфере.

Принято и вступило в силу правило[51], в соответствии с которым провайдеры кабельной связи, беспроводной и проводной передачи голоса по интернет-протоколу (VoIP) в зонах стихийных бедствий, где активирована Система отчетности о стихийных бедствиях (DIRS)[52], должны предоставлять:

- на ежедневной основе в DIRS: информацию о состоянии своей инфраструктуры до тех пор, пока DIRS не будет деактивирована, даже если их инфраструктура не изменилась по сравнению с предыдущим днем;
- в течение 24 часов после отключения DIRS: итоговый отчёт, в котором подробно описывается состояние их инфраструктуры на момент отключения DIRS, и указывается предполагаемая дата устранения оставшихся сбоев.

В период работы DIRS с поставщиков услуг снимаются обязательства по подаче отчётов о сбоях в Систему отчётности о сбоях в работе сети (NORS) при условии своевременной подачи информации в DIRS.

В Сенате и Палате представителей рассматривается проект Закона о прозрачности коммуникаций с иностранными лицами[53], который обяжет FCC публиковать список находящихся в иностранной собственности организаций, имеющих разрешения, лицензии или другие полномочия, выданные FCC, а также для других целей.

Великобритания

Правительство Великобритании обнародовало планы по принятию нового закона о кибербезопасности и устойчивости к угрозам, направленного на повышение способности страны защищаться от растущих рисков, связанных с киберугрозами[54]. Законопроект планируется принять в конце 2025 года. Он является ключевой частью более широкой стратегии Правительства по защите критически важной национальной инфраструктуры (CNI), поддержке экономического роста и обеспечению устойчивости цифровой среды Великобритании.

Предполагается:

- Расширение сферы применения Положений о сетевых и информационных системах, в целях охвата более широкого круга организаций и поставщиков. Это позволит распространить регулирование на центры обработки данных, поставщиков управляемых услуг (MSP) и других критически важных поставщиков, обеспечив соблюдение высоких стандартов кибербезопасности и отказоустойчивости более широким кругом организаций.

- Расширение полномочий регулирующих органов. Регулирующие органы получат дополнительные инструменты для повышения киберустойчивости в отраслях, за которыми они наблюдают. Это включает в себя новые обязательства для организаций сообщать о более широком спектре значительных киберинцидентов, что позволит быстрее и более эффективно реагировать на возникающие угрозы.

- Большая гибкость в адаптации. Правительство получит больше возможностей для обновления системы в соответствии с меняющейся ситуацией с угрозами. Это означает, что правила могут быть быстро расширены, чтобы охватить новые и развивающиеся отрасли, обеспечивая Великобритании гибкость перед лицом динамичных киберугроз.

- Новые полномочия исполнительной власти в сфере национальной безопасности для принятия решительных мер в ответ на серьёзные киберугрозы.

ЕС

Опубликовано Совместное сообщение Верховного представителя ЕС по иностранным делам и безопасности (HRVP) и Европейской Комиссии относительно усиления безопасности и отказоустойчивости подводных кабелей[55].

Предполагается, в т.ч.:

- разработка и внедрение мер по повышению устойчивости и безопасности подводных кабелей и увеличению инвестиций в прокладку новых, а также повышение их жизнеспособности, в т.ч. путём приоритетного финансирования внедрения новых «умных» кабелей, обеспечивающих повышенную отказоустойчивость;

- финансирование тестирования готовности / стресс-тестирования коммуникационных кабелей в рамках Закона о киберсолидарности;

- повышение эффективности антикризисной системы на уровне ЕС для оперативного реагирования на инциденты, связанные с подводными кабелями, и увеличение ремонтных мощностей для обеспечения быстрого восстановления повреждённых кабелей;

- ужесточение требований к безопасности и оценка рисков, связанных с подводными кабелями. Планируется разработка «Инструментария по обеспечению безопасности кабелей», содержащего меры по смягчению последствий, в т.ч. путём снижения выявленных рисков, уязвимостей и зависимостей. В настоящее время проводится работа по оценке рисков и

разработке сценариев. Данная работа поможет выявить зависимости в цепочках поставок, чтобы гарантировать достаточное количество запасных частей для прокладки кабелей в необходимые оперативные сроки.

Работа в рамках совместного заявления основана на нескольких уже реализуемых в ЕС мероприятиях.

Ожидается, что к концу 2025 года будут представлены карта существующих и планируемых подводных кабельных инфраструктур; Скоординированная оценка рисков, связанных с подводными кабелями; набор мер по снижению безопасности кабелей и приоритетный список кабельных проектов, представляющих интерес для Европы.

Европейская комиссия представила предложения по обеспечению эффективного реагирования на крупномасштабные киберинциденты[56]**.** Предлагаемый план кибербезопасности в целях улучшения координации действий ЕС в связи с киберкризисами обновляет комплексную систему ЕС по управлению кризисными ситуациями в сфере кибербезопасности и определяет соответствующих участников ЕС, описывая их роли на протяжении всего жизненного цикла кризиса.

Документ призван представить в ясной, простой и доступной форме структуру ЕС по управлению кризисными ситуациями в сфере кибербезопасности.

Документ не будет иметь обязывающей силы. Его цель - дать рекомендации по конкретным действиям при возникновении киберинцидента. Рекомендации документа помогают распознать киберинцидент, описывают возможности для их обнаружения, в том числе инструменты реагирования и восстановления, необходимые для смягчения последствий, сдерживания и локализации киберинцидентов.

Документ призван содействовать укреплению сотрудничества между гражданскими и военными структурами, включая НАТО, учитывая, что масштабные киберинциденты, затрагивающие гражданскую инфраструктуру Евросоюза, могут привести в действие механизмы реагирования НАТО.

Документ также дополняет совместное заявление Еврокомиссии и Верховного представителя ЕС по иностранным делам и безопасности об укреплении безопасности и устойчивости подводных кабелей от 21 февраля 2025 года.

Комиссия выделит 1,3 млрд евро на внедрение критически важных технологий, имеющих стратегическое значение для будущего Европы и технологического суверенитета континента, в рамках программы «Цифровая Европа» (Digital Europe Programme) на 2025–2027 годы[57].

Ключевые приоритеты в рамках программы работы в области цифровых технологий включают:

- повышение доступности приложений генеративного искусственного интеллекта (далее – ГенИИ), в том числе в сфере здравоохранения и социального обеспечения;
- поддержка европейских центров цифровых инноваций, которые предоставляют компаниям и государственному сектору доступ к техническим экспертам и тестированию технологий, а также консультации, обучение и навыки для внедрения новейших технологий;
- развитие инициативы Destination Earth, в рамках которой создаётся цифровая модель Земли для поддержки адаптации к изменению климата и управления рисками стихийных бедствий. Финансирование позволит создать более мощную модель, к которой смогут получить доступ больше исследователей;
- повышение киберустойчивости. Решения в области кибербезопасности, такие как Резерв кибербезопасности ЕС, повысят устойчивость и безопасность критически важных объектов инфраструктуры, включая больницы и подводные кабели;
- развитие возможностей образовательных и учебных заведений ЕС в области цифровых навыков, чтобы они могли растить и привлекать таланты, а также повышать уровень профессиональных навыков в Европе;
- облегчение внедрения новой архитектуры кошелька цифровой идентификации ЕС и Европейской инфраструктуры доверия, а также содействие её внедрению в государствах-членах;
- стимулирование преобразований в государственном секторе путём разработки эффективных, высококачественных, совместимых цифровых государственных услуг.

Инновации также будут ускоряться благодаря новой платформе «Стратегические технологии для Европы» (STEP), которая присваивает многообещающим проектам знак качества STEP Seal, чтобы расширить их возможности по получению государственного и частного финансирования.

Япония

Япония приняла закон об активной кибероборонe[58].

Его положения позволят военным и правоохранительным органам предпринимать упреждающие и активные кибероперации, обяжут владельцев критически важной

инфраструктуры сообщать об инцидентах и разрешит ограниченный сбор данных для отслеживания потенциальных угроз.

Закон предусматривает двусторонний подход, уделяя внимание как пассивной, так и активной киберзащите, позволяющей правительству собирать телекоммуникационные метаданные для обнаружения и предотвращения кибератак в рамках более масштабных реформ в сфере национальной безопасности для укрепления кибербезопасности страны. В частности, он позволяет правительству собирать техническую информацию, такую как IP-адреса и временные метки, у поставщиков телекоммуникационных услуг в случаях выявления потенциальной кибератаки, чтобы отслеживать связь между Японией и внешними субъектами.

Предполагается создание совета по кибербезопасности и надзорного комитета для улучшения анализа угроз и сбора информации. Закон также вводит новые требования к поставщикам критически важной инфраструктуры, согласно которым они должны оперативно сообщать о происшествиях, связанных с кибербезопасностью.

Предусмотрено создание сил кибербезопасности в составе представителей полиции и армии. На них возлагаются обязанности по активному пресечению попыток хакерской деятельности и установлению скрытого контроля за деятельностью государственных структур, частных корпораций, объектов инфраструктуры.

В законе содержится положение о неукоснительном соблюдении конституционного положения о тайне частной переписки.

Южная Корея

Корейская комиссия по связи (далее - KCC) провела экстренное совещание с тремя крупнейшими операторами мобильной связи — KT, LGU+ и SK Broadband по вопросу жалоб пользователей на услуги широкополосного интернета в зонах возникновения стихийных пожаров[59].

KCC обратилась к операторам мобильной связи с просьбой:

- проинформировать домохозяйства, находящиеся в зоне возникновения стихийных пожаров, о том, что они могут отменить подписку на интернет-услугу без комиссии за отмену, и упростить процесс подачи заявки на отмену;
- создать специальную горячую линию для консультаций, учитывая большое количество пожилых людей в пострадавших районах;

- увеличить период временной приостановки предоставления услуг максимум до одного года для пострадавших домохозяйств в зонах бедствия. Кроме того, политика отказа от взимания платы, которую внедряли операторы мобильной связи, теперь будет отражена в их правилах и условиях и полностью реализована по запросу КСС, если интернет-сервис недоступен из-за потери, полного или частичного разрушения жилых объектов в зонах бедствия.

Одновременно жителей девяти регионов, признанных зонами бедствия из-за случайных взрывов и масштабных лесных пожаров, освободили от уплаты лицензионного сбора за прием телевизионного сигнала[60].

Международные организаций в сфере связи и международное сотрудничество

Агентства ООН по телекоммуникациям, авиации и морскому судоходству выразили обеспокоенность относительно участившихся случаев помех в системах спутниковой навигации и спуфинга, что угрожает безопасности судов и самолётов по всему миру.[61]

Международный союз электросвязи (МСЭ), Международная организация гражданской авиации (ИКАО) и Международная морская организация (ИМО) призвали к срочной защите радионавигационной спутниковой системы (РНС), которая обеспечивает точную глобальную навигацию и хронометраж.

В связи с участившимися инцидентами агентства разработали для стран комплексный подход, состоящий из пяти ключевых шагов, к обеспечению надёжной работы спутниковой радионавигационной службы.

Борьба с мошенничеством и антифрод

Южная Корея

В смартфонах Samsung Electronics будет реализована функция блокировки вредоносных сообщений[62].

Корейская комиссия по коммуникациям объявила о разработке «функции блокировки вредоносных сообщений на основе ИИ» в сотрудничестве с Корейским агентством интернета и безопасности (KISA) и Samsung Electronics.

Эта функция основана на технологии ИИ, которая автоматически блокирует на смартфонах сообщения, предположительно содержащие вредоносный контент. Спам-сообщения, содержащие подозрительные телефонные номера и вредоносные URL-адреса, автоматически помещаются в папку со спамом.

Эта разработка является частью правительственных «Комплексных мер по предотвращению рассылки спама», о которых было объявлено в ноябре прошлого года. Эти меры направлены на предотвращение различных видов ущерба, причиняемого вредоносными сообщениями, связанными с незаконными кредитами, контентом для взрослых и азартными играми.

Компания Samsung Electronics сначала внедрит эту функцию в свои новейшие смартфоны Galaxy (серия S25), а затем постепенно - в другие существующие устройства с помощью обновления до Android 15 (One UI 7).

Пользователи могут выборочно разблокировать или проверить автоматически заблокированные сообщения в разделах «Заблокированные вредоносные сообщения», «Сообщения, заблокированные ИИ» и «Сообщения, заблокированные пользователем».

Борьба со спам-звонками

США

Суд принял трактовку понятия «телефонное домогательство»[63].

За некоторыми исключениями Закон о защите прав потребителей при использовании телефонной связи запрещает «телефонные звонки с предложениями» на номера, внесённые в Национальный реестр «Не беспокоить». В Решении Апелляционного суда седьмого округа по делу *«Халс против Зипонго»* указано, что «телефонным домогательством» в соответствии с Законом о защите прав потребителей является звонок или сообщение с целью убедить или побудить кого-либо оплатить имущество, товары или услуги.

Суть дела: Истец якобы получил около 20 звонков и текстовых сообщений от Foodsmart, которая заключила контракт с программой медицинского страхования для предоставления бесплатных консультаций участникам программы. В сообщениях описывались услуги Foodsmart, которые были доступны Халсу бесплатно в рамках его программы медицинского страхования, финансируемой государством и программой Medicaid. Когда Халс пользовался услугами Foodsmart, его лечащий врач, а не Халс, платил Foodsmart.

Компания Foodsmart подала ходатайство о вынесении решения в упрощённом порядке и заявила, что, поскольку её звонки и текстовые сообщения были направлены на то, чтобы предоставить Халсу информацию о бесплатной услуге, и не побуждали к покупке товара, услуги или имущества и, следовательно, не могут считаться «домогательством» в соответствии с Законом о добросовестной практике в сфере телекоммуникаций. Халс возразил, что его медицинская страховая компания оплатила бы услуги, если бы он их принял, и поэтому эти звонки и сообщения были направлены на то, чтобы побудить Халса воспользоваться услугами Foodsmart.

Решение вынесено в пользу компании Foodsmart.

На апелляционном уровне большинство судей постановило, что, поскольку сообщения Foodsmart побуждали истца пользоваться бесплатными для него услугами, они не могут считаться «телефонным домогательством» в соответствии с разделом 47 Кодекса США § 227 (a)(4).

С 25 марта 2026 года вступят в силу принятые FCC правила, изменяющее правила блокировки вызовов[64]. В частности:

- все поставщики услуг голосовой связи в США, участвующие в процессе звонка, должны блокировать вызовы на основании любого обоснованного списка телефонных номеров, которые не используются для исходящих

звонков (Do Not Originate, DNO) (у каждой компании может быть свой перечень);

- поставщики услуг голосовой связи должны немедленно уведомлять абонентов о блокировке их вызовов (на основании обоснованной аналитики – не DNO), проходящих через мультиплексирование с временным разделением каналов и IP-сети, с использованием кода протокола инициирования сеанса (SIP) 603+.

FCC пока не требует отображения имени вызывающего абонента, но настоятельно рекомендует провайдерам продолжать разрабатывать инструменты нового поколения, такие как предоставление расширенных данных о вызовах (RCD) и решения для брендированных звонков, чтобы потребители получали эту информацию.

Южная Корея

KCC утвердила изменения в Постановление о применении Закона о сетях[65].

Провайдеры сети доставки контента (CDN) с объёмом продаж более 1 млрд вон (684 тыс. долл. США) в секторе информационно-коммуникационных услуг должны принять меры по предотвращению распространения незаконной информации, в т.ч. назначить сотрудников, ответственных за:

- технологические и управленческие меры,
- уведомление Корейской комиссии по стандартам связи о случаях незаконного распространения информации;
- включение в договоры или условия положений, запрещающих незаконное распространение информации.

Установлены критерии для наложения штрафов в зависимости от количества нарушений. Максимальный штраф, налагаемый на поставщиков услуг связи и информации, нарушающих обязательства по предотвращению спама, увеличился с 10 (6,8 тыс. долл. США) до 30 млн вон (20,5 тыс. долл. США) (первое нарушение - 7,5 млн вон, второе нарушение - 15 млн вон, третье нарушение - 30 млн вон).

Индия

TRAI ужесточила правила для борьбы со спам-звонками и сообщениями, внеся поправки в «Положение о предпочтениях клиентов в сфере коммерческих телекоммуникационных услуг, 2018»[66], в том числе:

- любой звонок или сообщение, отправленные с целью обмана или попытки обмана клиентов, классифицируются как нежелательные коммерческие коммуникации, что позволяет оперативно принимать меры в отношении телекоммуникационных ресурсов отправителя такого сообщения, включая отключение и внесение в чёрный список. Эта поправка позволит оперативно отключать такие телекоммуникационные ресурсы за счет использования технологии на основе блокчейна;

- запрещено использовать обычные 10-значные номера для телемаркетинга;

- должна обеспечиваться идентификация звонящего на основе определения линии вызывающего абонента: коммерческие сообщения должны поступать с установленных номеров или номеров специальных серий: серия 1400 предназначена для рекламных звонков, серия 1600 - для транзакционных и сервисных звонков;

- в заголовках сообщений должны использоваться стандартизированные идентификаторы по виду отправителя: абонент (-P), сервис (-S), правительство (-g) и транзакции (-t). Это поможет пользователям правильно различать сообщения;

- операторы связи должны предоставлять в рекламных сообщениях обязательную опцию, с помощью которой клиент может отказаться от получения таких сообщений. Запрос на согласие пользователя на получение маркетинговых коммуникаций возможен не ранее чем через 90 дней после того, как абонент отказался от них; при этом сам клиент может подключить подписку в любое время;

- согласие на получение информации, данное клиентом для завершения текущей транзакции, будет действительным только в течение 7 дней, чтобы компании не могли звонить или отправлять сообщения клиенту позднее под предлогом ранее данного согласия;

- согласие клиента на осуществление транзакционных и коммерческих служебных сообщений должно быть действительным только в течение срока действия договора между клиентом и отправителем, и, следовательно, после этого отправитель не может совершать сервисные звонки клиенту, если только клиент не даст на это явное согласие;

- предусмотрено раскрытие информации об использовании автодозвона / робозвонков и их регулирование для предотвращения излишнего беспокойства клиентов;

- поставщики услуг связи должны приостанавливать работу всех телекоммуникационных ресурсов отправителя, признанного виновным в неоднократных нарушениях. При первом нарушении пороговых значений,

установленных регулирующим органом, все телекоммуникационные ресурсы отправителя должны быть отключены на 15 дней. При последующих нарушениях - будут отключены у всех поставщиков услуг связи на один год (период сокращен с двух лет), а отправитель будет внесён в чёрный список;

- увеличены сроки подачи жалобы на нежелательные звонки и сообщения с 3 до 7 дней;
- сокращен период, в течение которого операторы связи должны реагировать на жалобы о спаме с 30 до 5 дней;
- изменены критерии для наказания спамера - достаточно 5 жалоб в течение 10 дней, а не 10 жалоб в течение 7 дней, как раньше;
- для подачи жалобы абонентам не нужно заранее заявлять о нежелании получать сообщения от незарегистрированных отправителей;
- поставщики услуг связи должны размещать на своих веб-сайтах и в мобильных приложениях опцию для регистрации жалоб на спам на видном и легкодоступном месте;
- мобильные приложения должны автоматически сохранять журналы вызовов, сведения о SMS (с разрешения пользователя) и иметь возможность регистрировать жалобы с помощью скриншотов, предоставленных заявителем;
- введены дополнительные финансовые санкции для операторов связи за искажение информации о спаме в размере от 200 тыс. (2,3 тыс. долл. США) до 1 млн рупий (11,5 тыс. долл. США): 200 тыс. рупий за первое нарушение, 500 тыс. рупий - за второе нарушение и 1 млн рупий за каждое последующее нарушение;
- операторы связи должны анализировать характер звонков и SMS-сообщений на основе таких параметров, как большое количество звонков, их непродолжительность и низкий процент входящих звонков по отношению к исходящим в целях выявления спамеров в режиме реального времени;
- операторы связи обязаны использовать «приманки» — специальные номера, которые привлекают и регистрируют спам-звонки и сообщения, чтобы анализировать тенденции распространения спама и заблаговременно блокировать спамеров;
- ограничивается количество посредников между поставщиками услуг связи (Principal Entity) и телемаркетологами, чтобы обеспечить полную прослеживаемость коммерческих сообщений;

- отправители и телемаркетологи должны проходить физическую верификацию, биометрическую аутентификацию и привязывать уникальный номер мобильного телефона во время регистрации. Кроме того, операторы должны вести полный учёт жалоб и данных об отправителях, чтобы быстро выявлять и наказывать нарушителей;

- поставщики услуг связи должны заключать юридически обязывающие соглашения с зарегистрированными отправителями и телемаркетологами, в которых указываются их обязанности и штрафы за несоблюдение требований;

- поставщики услуг связи могут взимать с отправителей/телемаркетологов залог в качестве обеспечения соблюдения правил.

Правила не распространяются на спам-сообщения в OTT-приложениях, таких как WhatsApp.

При подготовке поправок рассматривался вопрос о лицензировании деятельности телемаркетологов и компаний, работающих через OTT-приложения, и формировании нормативной правовой базы для обеспечения подотчётности их как участников экосистемы. Пока данное предложение не нашло отражение в поправках к Положению[67].

TRAI дало определение международного SMS-сообщения[68]: «любое входящее SMS-сообщение, адресованное физическому лицу, должно рассматриваться как международное SMS-сообщение, если оно не может быть сгенерировано, передано или получено без использования или вмешательства какого-либо электронного устройства, компьютерной системы или компьютерного приложения, расположенных за пределами Индии».

Импортозамещение оборудования связи и телекоммуникаций

США

FCC начала расследование[69] текущих операций в США компаний, связанных с Коммунистической партией Китая, оборудование или услуги которых были включены в Закрытый перечень FCC (в т.ч. Huawei, ZTE, China Telecom) на основании выводов о том, что их оборудование или услуги создают неприемлемые риски для национальной безопасности Америки.

Сообщается, что FCC направила письма-запросы таким организациям и, по крайней мере, одну повестку в суд, а также собирает информацию и определит, какие дополнительные действия могут потребоваться.

США и КНР заключили торговую сделку[70], которая открывает возможности для дальнейших обсуждений в более комфортных для сторон условиях.

Договоренности предполагают закрепление нового уровня пошлин и, по всей видимости, снятие ограничений на экспорт редкоземельных металлов в США и этана в КНР.

Из высказываний президента США Дональда Трампа следует, что пошлины США на китайские товары теперь будут составлять 55%, а КНР на американские — 10%.

В ходе апрельской «гонки тарифов» взаимные пошлины стран были повышены до запретительных уровней: в США они составляли 145%, в Китае — 125%. В мае тарифы были временно снижены до 30% и 10% соответственно[71].

11 апреля Администрацией Трампа принято решение освободить от повышенных пошлин (145%) электронные устройства, такие как смартфоны, iPhone и ноутбуки[72]. Однако, впоследствии эти товары будут облагаться отдельными пошлинами.

Заявлено, что в ближайшие пару месяцев будут введены тарифы, нацеленные на конкретные отрасли бизнеса, в отношении определённых товаров, имеющих ключевое значение для национальной безопасности, которые «не подлежат обсуждению». Ожидается, что электроника будет отнесена к полупроводниковым товарам.

Объявлено об отмене правила президента США Джо Байдена о контроле за экспортом чипов с ИИ[73], которое должно было вступить в силу с 15 мая. Рассматривалась возможность его замены новым правилом[74], предусматривающим введение глобального режима лицензирования с межправительственными соглашениями.

Отмененное правило подразумевало ужесточение правил экспорта мощных высокотехнологичных чипов для систем ИИ в большинство стран мира.

1 апреля Министерство торговли США начало расследование о влиянии импорта полупроводников на национальную безопасность. В рамках расследования 16 апреля Министерство торговли опубликовало запрос[75] о предоставлении информации, в котором, помимо прочего, запрашивались комментарии общественности о роли иностранных компаний и правительств в полупроводниковой промышленности. Запрос появился после того, как семь сенаторов-республиканцев призвали министра торговли отменить правило предыдущей администрации о распространении ИИ. В письме от 11 апреля сенаторы утверждали, что правило «накладывает обременительные ограничения на американские компании, которые будет трудно соблюдать, а федеральному правительству будет ещё труднее обеспечить их соблюдение» и может задушить инновации и торговлю.

США начали расследование в отношении политики и практики КНР по развитию рынка полупроводников, направленные на достижение доминирования в полупроводниковой отрасли[76]. Расследование проводится в отношении рыночных практик КНР при производстве базовых полупроводников, в том числе их использование в качестве компонентов в более сложных продуктах для критически важных отраслей, таких как оборонная промышленность, автомобилестроение, медицинское оборудование, аэрокосмическая промышленность, телекоммуникации, производство электроэнергии и электрические сети. В ходе расследования будет оцениваться, способствуют ли действия, политика и практика Китая в отношении производства пластин из карбида кремния (или других пластин, используемых в качестве сырья для производства полупроводников) необоснованной дискриминации, обременению или ограничению торговли в США.

Расследование ведется по Разделу 301 Закона о торговле 1974 года, который предоставляет возможность вводить тарифы или другие экономические барьеры в ответ на действия иностранных государств, которые считаются несправедливыми или незаконными.

11 марта 2025 года в рамках расследования состоялись публичные слушания[77].

15 апреля 2025 года компания Nvidia заявила[78], что Правительство США заблокировало свободную продажу некоторых её чипов (Nvidia H20) для ИИ в Китай (без получения лицензии), и что в будущем для таких продаж потребуется лицензия.

13 мая Министерство торговли США выпустило руководство, в котором говорится, что использование чипов Ascend AI от Huawei в любой точке мира нарушает правила экспортного контроля США[79].

Ограничения касаются чипов Huawei Ascend 910B, Huawei Ascend 910C и Huawei Ascent 910D. Бюро промышленности и безопасности Министерства торговли США предупреждает, что использование данных чипов может повлечь за собой санкции в соответствии с правилом GP10, которое запрещает совершать сделки если известно, что произошло или может произойти нарушение правил экспортного контроля (EAR).

29 мая США ограничили экспорт в КНР программного обеспечения для проектирования микросхем, химических веществ и другой продукции[80].

Решение, в частности, затронуло поставки в Китай бутана и этана, используемых полупроводниковой отраслью, различного оборудования.

Минторг США разослал поставщикам специализированного программного обеспечения (далее - ПО) уведомления о том, что теперь для продажи их продуктов в Китай требуется получать лицензию.

Рассматривается законопроект, позволяющий встраивать в чипы GPS-приёмник для отслеживания их местоположения[81].

Отслеживать предлагается «любые процессорные модули и устройства верхнего ценового сегмента, подпадающие под ограничения США».

В результате Минторг США получит полномочия и, главное, техническую возможность проверять местонахождение чипов.

Компании также должны будут следить за тем, где оказались их микросхемы.

Механизм реализации не приводится.

ЕС

Европейская комиссия одобрила выделение 920 млн евро из бюджета Германии на строительство Infineon нового завода по производству полупроводников в Дрездене[82].

Помощь будет оказана в виде прямого гранта в размере до 920 млн евро компании Infineon для поддержки её инвестиций в размере 3,5 млрд евро.

Финансирование поддержит проект компании MEGAFAB-DD, целью которого является производство широкого спектра микросхем. Ожидается, что новый завод выйдет на полную мощность к 2031 году.

Новый завод станет первым в Европе предприятием, способным быстро переключаться с одного технологического процесса на другой, сохраняя при этом высокую производительность. Это будет предприятие полного цикла, занимающееся обработкой, тестированием и разделением пластин.

Производимые полупроводники будут использоваться в промышленности, автомобилестроении и потребительских товарах.

В рамках получения поддержки Infineon согласилась предоставить доступ к своему новому предприятию малым и средним предприятиям и исследовательским организациям для тестирования и создания прототипов.

Европейская комиссия провела церемонию, посвящённую запуску первых пяти пилотных линий в рамках инициативы «Чипы для Европы»[83]**.**

Предусмотрено финансирование на сумму 3,7 млрд евро, включая взносы ЕС в рамках программ «Горизонт Европы» и «Цифровая Европа», а также соразмерные инвестиции государств-членов.

Пилотные линии ориентированы на пять ключевых областей:

- передовые системы на кристалле с техпроцессом менее 2 нанометров;
- применение технологии FD-SOI (полностью обедненный кремний-на-изоляторе);
- передовое корпусирование;
- материалы, обладающие широкой запрещенной зоной;
- фотонные интегральные схемы.

Министерство цифровизации Польши разработало проект политики в полупроводниковой сфере[84]**,** направленный на привлечение инвесторов, развитие национальных компетенций и укрепление технологического суверенитета.

Определено 7 основных направлений развития полупроводниковой промышленности:

- Инфраструктура – инвестиции в современные лаборатории, производственные мощности и научно-исследовательские центры, которые поддерживают развитие полупроводниковых технологий;
- Импульс государства – инициирование проектов и внедрение новых технологий, внедрение польских полупроводниковых инноваций в общественные проекты и развитие экспорта польских технологических решений;
- Международное сотрудничество – построение прочных партнерских отношений с мировыми лидерами полупроводниковой промышленности;
- Инвестиции и финансирование – привлечение средств и обеспечение соответствующих условий для реализации отечественных проектов с высокой добавленной стоимостью, привлечение крупных международных инвесторов;
- Кадры и образование – инвестиции в образование, подготовка специалистов для работы в полупроводниковой промышленности;
- Доступность воды и энергии – обеспечение адекватными энергетическими и водными ресурсами, необходимыми для производства полупроводников;
- Доступность химических веществ и сырья – обеспечение стабильности цепочки поставок материалов, необходимых для производства полупроводников.

Бельгия, Хорватия, Чехия, Франция, Германия, Ирландия, Италия, Мальта, Нидерланды и Испания считают необходимым пересмотреть целевые показатели, содержащиеся в Стратегии Европейской комиссии в области производства микросхем (ожидалось, что к 2030 году ЕС займёт 20% мирового рынка) и прописанные в готовящемся новом законе о чипах (Chips Act 2.0)[85]. При этом «реально достижимые» показатели не называются.

По состоянию на 2022 год доля ЕС на глобальном рынке производства чипов была менее 10%. Евросоюз отстаёт по этому показателю от США и Тайваня.

Китай

Власти Китая начали антидемпинговое расследование в отношении американских чипов low-end[86], по результатам которого могут быть введены антидемпинговые пошлины.

Китай не будет облагать повышенными пошлинами чипы американских компаний, выпускаемые за пределами США другими производителями по контракту[87]. Страной происхождения чипов китайская таможня будет считать

государство, где расположена фабрика по производству полупроводниковых пластин для этих чипов.

В отношении чипов, произведенных на территории США, будут применяться ответные пошлины.

4 апреля Китай приостановил экспорт редкоземельных элементов[88] в рамках торговой войны с США.

Южная Корея

15 апреля Южная Корея объявила об увеличении пакета мер по поддержки полупроводниковой промышленности до 33 трлн вон (23 млрд долл. США)[89] в ответ на глобальную торговую войну. В 2024 году отрасли было предоставлено 26 трлн. вон (19 млрд долл. США).

TSMC объявила об инвестициях в строительство американских фабрик в размере $100 млрд долл. США[90]. Первые два предприятия комплекса должны начать выпуск микросхем в 2025 и 2028 годах.

Индия

Принято решение[91] возмещать расходы на тестирование и сертификацию стартапов, микро-, малых и средних предприятий в сфере телекоммуникаций в рамках обязательной/добровольной схемы тестирования и сертификации и опубликована Схема их возмещения[92].

В рамках программы будет производится возмещение расходов на тестирование и сертификацию, проводимые в телекоммуникационном центре Инженерный центр (TEC) / Национальный центр безопасности связи (NCCS) в назначенных/признанных лабораториях или в лабораториях, аккредитованных Национальной ассоциацией по безопасности пищевых продуктов (NABL). Возмещение части расходов на сертификацию и тестирование будет производиться в процентном отношении к общей сумме расходов в соответствии со следующей классификацией для:

- стартапов – до 75%;
- микропредприятий – до 60%;
- малых и средних предприятий – до 50%.

Международные организаций в сфере связи и международное сотрудничество

ЕС и Япония в рамках третьего заседания Совета по цифровому партнёрству договорились о дальнейшем сотрудничестве в области основных цифровых технологий, таких как ИИ, 5G/6G, полупроводники, высокопроизводительные вычисления и квантовые технологии[93].

Они также укрепят сотрудничество в области управления данными и онлайн-платформ, подводных кабелей, подключения к Арктике, цифровых удостоверений личности, служб доверия и кибербезопасности.

Совет завершил работу со следующими ключевыми итогами:

- Полупроводники: ЕС и Япония подтвердили свою приверженность совместным исследованиям в области полупроводников. Они также обязались активизировать свои усилия по обеспечению устойчивости цепочек поставок полупроводников посредством обмена информацией и механизмов раннего оповещения.

- Исследование: партнёры договорились расширить сотрудничество в области исследований, выходящих за рамки 5G/6G, уделяя особое внимание совместному проекту 6G MIRAI-HARMONY, целью которого является разработка сетей на базе ИИ для ориентированных на пользователя коммуникаций.

- Квантовые вычисления и ИИ: ЕС и Япония объявили совместный исследовательский конкурс для совместных проектов по квантовым вычислениям с применением в таких областях, как биомедицина, материаловедение и моделирование климата. Они также подтвердили свою приверженность продвижению инновационного, безопасного, надёжного и заслуживающего доверия ИИ, в том числе в рамках процесса ИИ в Хиросиме.

- Цифровые удостоверения личности и сервисы доверия: ЕС и Япония работают над обеспечением совместимости и взаимного признания академических дипломов с помощью цифровых удостоверений личности и сервисов доверия.

- Управление данными: Партнеры начали работу по созданию возможной совместной рабочей группы для улучшения обмена данными и обеспечения совместимости пространств данных.

- Онлайн-платформы и цифровые рынки: ЕС и Япония проводят обмен опытом в области регулирования для содействия эффективному управлению

онлайн-платформами и справедливому функционированию цифровых рынков.

- Кибербезопасность: партнеры обменялись информацией о нормативных изменениях, в частности в области защиты критически важной инфраструктуры и безопасности продукции.

- Подводные кабели и подключение к сети: ЕС и Япония признали важность безопасных, устойчивых и экологичных глобальных подключений в области подводных кабелей. Они также признали важность разработки новаторского арктического маршрута для обеспечения надёжной передачи данных между Европой и Японией.

Четвёртый Совет по цифровому партнёрству запланирован на 2026 год.

В 2025 году ожидается ратификация Швейцарией пакета двусторонних соглашений с ЕС, что позволит Швейцарии участвовать в программах Союза, открытых для участия третьих стран, в т.ч.: «Горизонт Европы» (финансирование исследований и инноваций), «Цифровая Европа» (обеспечивает финансовую поддержку проектов в ключевых областях, в т.ч.: суперкомпьютеры, ИИ, кибербезопасность, продвинутые цифровые навыки, производство полупроводников[94]), «Программа исследований и обучения Евратома», ITER/F4E (проекты в области термоядерной энергетики).[95] С 1 января 2025 года Комиссия обеспечивает переходные механизмы, чтобы швейцарские организации могли участвовать в конкурсах программ с этой даты. Предусмотрено, что участие Швейцарии в этих программах прекратится, если пакет не будет ею ратифицирован.

Компании Sparkle и Turkcell подписали меморандум о взаимопонимании о строительстве 4 тыс. км подводного кабеля между Турцией и Европой[96] (между Измиром в Турции и Ханьей в Греции. Кабель будет поддерживать скорость более 25 Тбит/с на оптоволоконную пару и будет интегрирован с кабельной системой BlueMed компании Sparkle, что расширит возможности подключения от Ханьи до основных точек в Милане.

Идентификация абонентов

США

FCC в целях предотвращения незаконных роботизированных звонков американским потребителям опубликовала уведомление[97] о предлагаемом изменении правил, направленном на устранение пробелов в аутентификации при использовании системы аутентификации вызовов в своих сетях, отличных от IP.

Ранее FCC потребовала от всех поставщиков голосовых услуг, промежуточных звеньев и шлюзов внедрить систему аутентификации по идентификатору вызывающего абонента STIR / SHAKEN на всех IP-участках своих сетей. Это позволяет провайдерам проверять, соответствует ли номер вызывающего абонента информации об идентификаторе вызывающего абонента, передаваемой при вызове. Проверка помогает операторам блокировать звонки, которые, скорее всего, были совершены с помощью незаконной подмены.

Однако платформа STIR / SHAKEN работает только в телекоммуникационных сетях на базе IP. Таким образом, любая не-IP-часть пути вызова создаёт брешь в платформе. В соответствии с Законом FCC требует от провайдеров, которые используют технологию, отличную от IP принять разумные меры для внедрения эффективной системы аутентификации вызовов в своих сетях, отличных от IP. В настоящее время в отношении таких провайдеров действует переходный период.

FCC предлагает установить критерии для оценки системы аутентификации по идентификатору вызывающего абонента, не связанные с IP, чтобы определить, являются ли они достаточно развитыми, разумно доступными и эффективными, чтобы оправдать отмену переходного периода для поставщиков, использующих технологии, не связанные с IP.

Применяя критерии – что система аутентификации по идентификатору вызывающего абонента, отличная от IP, «разработана», «разумно доступна» и «эффективна» – FCC предлагает заключить, что два существующих стандарта соответствуют этим требованиям: внутриполосная аутентификация (ATIS-1000095.v002) и внеполосная аутентификация с несколькими STI-CPS (ATIS-1000096). В NPRM запрашиваются комментарии о том, соответствует ли критериям третий стандарт — внеполосная согласованная аутентификация STI-CPS (ATIS-1000105).

Это означает, что все поставщики голосовых услуг, промежуточных звеньев и шлюзов, которые имеют сегменты сети, отличные от IP, должны будут внедрить один из двух стандартов аутентификации по идентификатору вызывающего абонента, отличных от IP. Кроме того, FCC предлагает потребовать от этих

поставщиков подтвердить, что они внедрили один из этих стандартов в своих заявках в базу данных Robocall по смягчению последствий.

FCC предлагает двухлетний переходный период для провайдеров, чтобы они либо полностью завершили переход на IP-адреса и внедрили STIR / SHAKEN, либо внедрили одну или несколько доступных систем аутентификации по идентификатору вызывающего абонента, отличных от IP.

Индия

Введены новые правила получения SIM-карт в Индии. Перед получением новых SIM-карт необходимо пройти биометрическую верификацию[98] в Aadhaar[99], что обеспечит привязку новых SIM-карт к подтвержденным учетным записям.

При верификации через Aadhaar (системы e-KYC и Self-KYC) в сети Интернет или у авторизованного дилера бумажные документы для приобретения SIM-карт не потребуются[100].

Стоимость онлайн-проверки через E-KYC на основе Aadhaar составляет 1 рупию (1 цент).

Доступ правоохранительных органов к данным операторов связи

США

В рамках реализации «Закона о национальной горячей линии по борьбе с самоубийствами от 2018 года» запрошены комментарии[101] по потенциальным проблемам конфиденциальности, связанным с геомаршрутизацией текстовых сообщений, отправленных на номер 988 («Телефон доверия»). Геомарштуризация необходима, чтобы служба «Телефона доверия» могла перенаправлять полученные сообщения в кризисные центры по месту нахождения отправителя. В частности, поднят вопрос о возможных угрозах конфиденциальности в случае, если поддержка геомаршрутизации при передаче текстовых сообщений станет обязательной для поставщиков услуги.

FCC опубликовала предлагаемое правило, об ужесточении требований, направленное на повышение точности определения местоположения для системы 911[102], в том числе по оси Z в формате с использованием единиц измерения «высота над уровнем земли» (AGL), вместо требуемой в настоящее время «высоты над эллипсоидом» (HAE). Это будет способствовать определению местоположения вплоть до комнаты, в том числе в многоэтажных зданиях.

Источники

[1] https://docs.fcc.gov/public/attachments/DOC-408580A1.pdf

[2] https://matsui.house.gov/sites/evo-subsites/matsui.house.gov/files/evo-media-document/matsui_008_xml.pdf

[3] https://www.congress.gov/119/bills/hr2449/BILLS-119hr2449rfs.pdf

[4] https://www.congress.gov/119/bills/hr1765/BILLS-119hr1765ih.pdf

[5] https://allen.house.gov/uploadedfiles/spectrum_pipeline_act_of_2025.pdf

[6] https://docs.fcc.gov/public/attachments/FCC-25-12A1.pdf

[7] https://www.federalregister.gov/documents/2025/01/29/2025-01535/wireless-telecommunications-bureau-seeks-to-supplement-the-record-on-proposed-rules-to-re-allocate

[8] https://www.ntia.gov/report/2025/18-ghz-band-report

[9] https://www.ntia.gov/blog/2025/ntia-nasa-recommend-18-ghz-band-allocation-bolster-commercial-space-activities

[10] https://docs.fcc.gov/public/attachments/FCC-25-24A1.pdf

[11] https://docs.fcc.gov/public/attachments/DA-25-274A1.pdf

[12] https://docs.fcc.gov/public/attachments/DOC-411203A1.pdf

[13] https://docs.fcc.gov/public/attachments/DA-25-387A1.pdf

[14] https://docs.fcc.gov/public/attachments/FCC-25-13A1.pdf

[15] https://www.lee.senate.gov/services/files/2598798F-6E85-46EA-AB0B-767F6AD549CD

[16] https://www.lee.senate.gov/services/files/EC6BDF4A-9ACF-41C5-98BA-40D42F5A8638

[17] https://dig.watch/updates/5g-advanced-is-now-live-nationwide-with-t-mobile

[18] https://www.ntia.gov/press-release/2025/more-90-applications-requesting-nearly-3-billion-submitted-wireless-innovation-fund-s-third-round; https://www.ntia.doc.gov/other-publication/2025/ntia-extends-innovation-fund-application-deadline

[19] https://broadbandusa.ntia.doc.gov/sites/default/files/2022-05/BEAD%20NOFO.pdf

https://brandergroup.net/bead-proposal-progress-dashboard-internet-for-all/

[20] https://www.washingtontimes.com/news/2024/jun/18/bidens-425-billion-rural-high-speed-internet-plan-/

[21] https://www.ntia.gov/press-release/2025/biden-harris-administration-approves-nevada-s-internet-all-final-proposal

[22] https://www.ntia.gov/press-release/2025/biden-harris-administration-approves-delawares-internet-all-final-proposal

[23] https://www.ntia.gov/press-release/2025/biden-harris-administration-approves-louisiana-s-internet-all-final-proposal

[24] https://www.ntia.gov/press-release/2023/biden-harris-administration-approves-louisiana-s-internet-all-initial-proposal

[25] https://www.internetforall.gov/news-media/biden-harris-administration-announces-more-127-million-louisiana-increase-digital

[26] https://www.ntia.gov/press-release/2025/statement-us-secretary-commerce-howard-lutnick-bead-program

[27] https://www.ntia.gov/press-release/2025/biden-harris-administration-recommends-award-more-162-million-expand-internet-use-tribal-lands

[28] https://www.ntia.gov/press-release/2025/biden-harris-administration-announces-nearly-18-million-internet-all-grants-tribal-lands

[29] https://www.ntia.gov/press-release/2025/biden-harris-administration-awards-117-million-wireless-innovation

[30] https://www.ntia.gov/press-release/2025/biden-harris-administration-awards-19-million-wireless-innovation

[31] https://www.ntia.gov/press-release/2025/biden-harris-administration-recommends-award-more-369-million-invest-digital-skills

[32] https://dig.watch/updates/ofcom-backs-broadband-competition-to-expand-full-fibre-coverage

[33] https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2025/004-wissing-gigabitfoerderung-glasfaserausbau.html

[34] https://techblog.comsoc.org/2025/02/13/itu-r-wp-5d-progresses-reports-on-imt-2030-6g-minimum-technology-performance-requirements-evaluation-criteria-methodology/

[35] https://www.nextias.com/ca/current-affairs/12-12-2024/bharat-6g-vision-document; https://dot.gov.in/bharat-6g

[36] https://www.nextias.com/ca/current-affairs/12-12-2024/bharat-6g-vision-document

[37] https://trai.gov.in/sites/default/files/2025-01/PR_No.03of2025.pdf

[38] https://economictimes.indiatimes.com/industry/telecom/telecom-news/trai-proposal-on-private-5g-network-raises-hopes-again-for-big-enterprises/articleshow/118512134.cms

[39] https://trai.gov.in/notifications/press-release/trai-releases-draft-telecommunication-tariff-71st-amendment-order-2025

[40] https://d-russia.ru/wp-content/uploads/2024/12/om-gmpcs-security-instructions_0.pdf

[41] https://www.federalregister.gov/documents/2025/01/08/2024-29967/spectrum-rules-and-policies-for-the-operation-of-unmanned-aircraft-systems

[42] https://docs.fcc.gov/public/attachments/FCC-25-7A1.pdf

[43] Advanced Air Mobility (AMM) могут быть с экипажем или без него, при этом персонал управляет воздушным судном дистанционно либо с помощью автоматизированных технологий

[44] полосы частот 6625–454,9875 МГц и 459,6625–459,9875 МГц (вместе «полоса частот 450 МГц»

[45] https://kcc.go.kr/user.do;jsessionid=uKEk477wGiaPUMJitttWeZooFRixHikVUH-pNF_s.servlet-aihgcldhome20?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=65589

[46] https://corp.mobile.rakuten.co.jp/english/news/press/2025/0120_01/

[47] https://www.ntia.gov/press-release/2025/biden-harris-administration-awards-117-million-wireless-innovation; https://www.ntia.gov/page/what-they-re-saying-biden-harris-administration-awards-grant-wireless-innovation-fund-0

[48] https://www.ntia.gov/page/what-they-re-saying-biden-harris-administration-awards-grant-wireless-innovation-fund-0

[49] https://dig.watch/updates/us-launches-national-security-unit-to-combat-cyberattacks-on-telecom-sector

[50] https://docs.fcc.gov/public/attachments/FCC-25-9A1.pdf

[51] https://www.federalregister.gov/documents/2025/01/21/2025-00495/resilient-networks-disruptions-to-communications

[52] веб-система, созданная FCC для сбора информации о состоянии и восстановлении инфраструктуры связи от операторов во время крупных чрезвычайных ситуаций и в период ликвидации их последствий

[53] https://wittman.house.gov/uploadedfiles/fact_01_xml.pdf

[54] https://dig.watch/updates/uk-government-announces-new-cyber-bill-to-strengthen-national-defences-and-protect-critical-infrastructure

[55] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_580

[56] https://digital-strategy.ec.europa.eu/en/news/commission-launches-new-cybersecurity-blueprint-enhance-eu-cyber-crisis-coordination

[57] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_907

[58] https://japannews.yomiuri.co.jp/politics/defense-security/20250119-233928/

[59]https://kcc.go.kr/user.do;jsessionid=R9PN6tzt-NMCCVVJEP1DC06vZqeqcpNYPjhT-snL.servlet-aihgcldhome20?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=66057

[60]https://www.kcc.go.kr/user.do?boardId=1058&page=E04010000&dc=E04010000&boardSeq=66937&mode=view

[61] https://www.itu.int/hub/2025/03/un-agencies-warn-of-satellite-navigation-jamming-and-spoofing/

[62]https://kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=2&boardSeq=65918

[63] https://tcpablog.com/category/dnc/

[64] https://www.federalregister.gov/documents/2025/03/24/2025-04811/advanced-methods-to-target-and-eliminate-unlawful-robocalls

[65] https://kcc.go.kr/user.do;jsessionid=uKEk477wGiaPUMJitttWeZooFRixHikVUH-pNF_s.servlet-aihgcldhome20?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=65563

[66] https://trai.gov.in/notifications/press-release/trai-strengthens-consumer-protection-amendments-tcccpr-2018; https://trai.gov.in/sites/default/files/2025-02/PR_No.11of2025.pdf

[67]https://www.outlookbusiness.com/corporate/telcos-disappointed-with-new-trai-rules-to-curb-spam-calls-heres-why; https://cxotoday.com/press-release/coai-statement-on-amendment-to-tcccp-regulation-2018-issued-by-trai/

[68] https://economictimes.indiatimes.com/industry/telecom/telecom-policy/trai-issues-definition-of-overseas-sms-traffic/articleshow/116184523.cm

[69] https://docs.fcc.gov/public/attachments/DOC-410318A1.pdf

[70] https://www.kommersant.ru/doc/7851858

[71] https://www.whitehouse.gov/briefings-statements/2025/05/joint-statement-on-u-s-china-economic-and-trade-meeting-in-geneva/

[72] https://edition.cnn.com/2025/04/13/business/tariffs-economy-trump-china/index.html

[73] https://www.cnews.ru/news/top/2025-05-14_administratsiya_trampa_otmenila

[74] https://www.reuters.com/business/trump-administration-will-rescind-biden-era-ai-chip-export-curbs-bloomberg-news-2025-05-07/

[75] https://www.federalregister.gov/documents/2025/04/16/2025-06591/notice-of-request-for-public-comments-on-section-232-national-security-investigation-of-imports-of

[76] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/december/ustr-initiates-section-301-investigation-chinas-acts-policies-and-practices-related-targeting

[77] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2025/march/public-hearing-regarding-section-301-investigation-chinas-acts-policies-and-practices-related

[78] https://www.nytimes.com/2025/04/15/technology/nvidia-h20-chip-china-restrictions.html

[79] https://www.bis.gov/media/documents/general-prohibition-10-guidance-may-13-2025.pdf

[80] https://www.tbsnews.net/worldbiz/usa/us-curbs-chip-design-software-chemicals-other-shipments-china-1154401

[81] https://www.tomshardware.com/pc-components/gpus/u-s-inks-bill-to-force-geo-tracking-tech-for-gpus-and-servers-high-end-gaming-gpus-also-subject-to-tracking

[82] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_557

[83] https://digital-strategy.ec.europa.eu/en/news/chips-europe-initiative-milestone-event-first-pilot-lines

[84] https://www.gov.pl/web/cyfryzacja/polska-w-grze-o-przyszlosc--7-filarow-polityki-dla-sektora-polprzewodnikow

[85] https://uk.news.yahoo.com/eu-member-states-ask-commission-134347207.html

[86] https://www.interfax.ru/world/1003227

[87] https://www.reuters.com/technology/us-chipmakers-outsourcing-manufacturing-will-escape-chinas-tariffs-2025-04-11/

[88] https://www.independent.co.uk/asia/china/trade-war-china-rare-earth-export-b2732710.html

[89] https://www.reuters.com/technology/south-korea-unveils-23-billion-support-package-chips-amid-us-tariff-uncertainty-2025-04-14/?utm_source=Sailthru&utm_medium=Newsletter&utm_campaign=Technology-Roundup&utm_term=041525&lctg=6538bab754ae15a71908d403

[90] https://qz.com/tsmc-invest-100-billion-chip-plants-us-arizona-ai-trump-1851767408

[91]https://dot.gov.in/sites/default/files/Notification%20letter%20of%20Scheme%20for%20reimbursement%20of%20Testing%20and%20certification%20charges.pdf

[92]https://dot.gov.in/sites/default/files/Guidelines%20for%20implementation%20of%20Scheme%20for%20reimbursement%20of%20Testing%20and%20Certification%20Charges%20for%20Start-ups%20and%20Telecom%20MSEs.pdf

[93] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1185

[94] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[95] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6562

[96] https://www.wirecable.in/sparkle-turkcell-to-launch/

[97] https://docs.fcc.gov/public/attachments/FCC-25-25A1.pdf

[98] https://tech.hindustantimes.com/tech/news/aadhaarbased-biometric-verification-now-mandatory-for-new-sim-cards-to-combat-fraud-and-cybercrime-activities-71737035497192.html

[99] Онлайн-сервис аутентификации государственного Агентства Индии по уникальной идентификации. Организации (банки, правительственные учреждения и т.д.) передают в Aadhaar-номер и считанные биометрические данные пользователя (один или несколько шаблонов отпечатка пальца либо радужки глаза). В ответ сервис выдаёт ответ «да/нет».

[100] https://www.jaagrukbharat.com/new-sim-card-rules-in-india-ekyc-and-selfkyc-for-airtel-jio-bsnl-and-vi-1401166

[101] https://www.federalregister.gov/documents/2025/03/04/2025-03399/implementation-of-the-national-suicide-hotline-act-of-2018

[102] https://www.federalregister.gov/documents/2025/05/07/2025-06865/wireless-e911-location-accuracy-requirements