

Справочник по цифровому регулированию



Совместно с:



Справочник по цифровому регулированию



© Международный союз электросвязи
и Всемирный банк, 2020 год

Некоторые права сохранены. Настоящая работа лицензирована для широкого применения на основе использования лицензии международной организации Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO (CC BY-NC-SA 3.0 IGO; <https://creativecommons.org/licenses/by-nc-sa/3.0/igo>).

По условиям этой лицензии допускается копирование, перераспределение и адаптация настоящей работы в некоммерческих целях, при условии наличия надлежащих ссылок на настоящую работу в указанном ниже порядке. При любом использовании настоящей работы не следует предполагать, что МСЭ или Всемирный банк поддерживает какую-либо конкретную организацию, продукты или услуги. Не разрешается несанкционированное использование наименований и логотипов МСЭ или Всемирного банка. При адаптации работы необходимо в качестве лицензии на работу применять ту же или эквивалентную лицензию Creative Commons. При создании перевода настоящей работы следует добавить следующую правовую оговорку наряду с предлагаемой ссылкой: "Настоящий перевод не был выполнен Международным союзом электросвязи (МСЭ) или Всемирным банком. Ни МСЭ, ни Всемирный банк не несут ответственности за содержание или точность настоящего перевода. Оригинальный английский текст должен являться имеющим обязательную силу и аутентичным текстом".

Любые процедуры посредничества в вопросе разрешения споров, возникших в связи с данной лицензией, должны осуществляться в соответствии с Правилами о посредничестве Всемирной организации интеллектуальной собственности (<https://www.wipo.int/amc/ru/mediation/rules/index.html>).

Документ для цитирования. Справочник по цифровому регулированию, Женева, Международный союз электросвязи и Всемирный банк, 2020 год. Лицензия: CC BY-NC-SA 3.0 IGO.

Материалы третьих сторон. Если вы желаете повторно использовать материалы из данной работы, принадлежащие третьим сторонам, такие как таблицы, рисунки или изображения, вы обязаны определить, необходимо ли для такого повторного использования разрешение, и получить такое разрешение у обладателя авторских прав. Риск предъявления претензий вследствие нарушения прав третьей стороны, которой принадлежит какой-либо компонент данного документа, возлагается исключительно на пользователя.

Общие оговорки. Употребляемые обозначения, а также изложение материала в настоящей публикации не означают выражения какого бы то ни было мнения со стороны МСЭ или Всемирного банка в отношении правового статуса какой-либо страны, территории, города или района, или их властей, а также в отношении делимитации их границ. Пунктирные и штриховые линии на географических картах обозначают приблизительные границы, в отношении которых пока еще может быть не достигнуто полное согласие.

Идеи и мнения, представленные в настоящей публикации, принадлежат авторам и не обязательно отражают точку зрения МСЭ и Всемирного банка. Упоминание конкретных компаний, продуктов или услуг не означает, что МСЭ или Всемирный банк одобряет или рекомендует их, предпочитая их другим компаниям, продуктам или услугам аналогичного характера, не упомянутым в настоящей работе. За исключением ошибок и пропусков названия проприетарных продуктов выделяются начальными заглавными буквами.

МСЭ или Всемирный банк приняли все разумные меры для проверки информации, содержащейся в настоящей публикации. Тем не менее публикуемый материал распространяется без каких-либо гарантий, четко выраженных или подразумеваемых. Ответственность за истолкование и использование материала несет читатель. Ни МСЭ, ни Всемирный банк ни при каких обстоятельствах не несут ответственности за ущерб, связанный с использованием этих материалов.

ISBN:

978-92-61-31664-8 (печатная версия)

978-92-61-31654-9 (электронная версия)

978-92-61-31674-7 (версия для EPUB)

978-92-61-31684-6 (версия для Mobi)

Современные цифровые технологии преобразуют практически все отрасли экономики, способствуя возникновению новых бизнес-моделей, внедрению инновационных продуктов и услуг и, в конечном счете, изменяя пути социально-экономического развития стран всего мира. Цифровые технологии, равно как и создаваемые ими преимущества, могут обеспечить доступ граждан к услугам и возможностям и помогают им строить лучшее будущее. Однако для эффективного функционирования рынков им должна сопутствовать благоприятная политическая и регуляторная среда.

Цифровая экономика, включающая в себя цифровую инфраструктуру, платформы, услуги, предприятия и навыки, стала важнейшим средством сокращения масштабов бедности и повышения качества жизни бедных и уязвимых слоев населения. Цифровые технологии и инфраструктура связи помогают находить инновационные решения сложных проблем в широком спектре отраслей, включая энергетику, здравоохранение, образование, транспорт, управление рисками бедствий и сельское хозяйство. Интернет и цифровые технологии оказывают сильное влияние на функционирование государственных органов и их взаимодействие с гражданами, способствуя повышению прозрачности и эффективности оказания услуг, и, в свою очередь, формируют потребность в расширении межотраслевого сотрудничества и выработке подхода к регулированию, основанного на взаимодействии. Нынешняя волна инноваций способна устранить множество препятствий, отделяющих людей (особенно представителей более бедных сообществ) от возможностей.

Цифровые технологии продолжают способствовать преобразованию рынков за счет конвергенции и реорганизации различных отраслей экономики. Однако некоторые серьезные рыночные пробелы и вопросы по-прежнему требуют рассмотрения; в их числе – вопросы обеспечения защиты прав граждан и персональных данных в интернете, а также поиск способов повсеместного предоставления недорогих услуг подключения к высокоскоростной широкополосной связи, в том числе в отдаленных районах.

Настоящее третье издание *Справочника по цифровому регулированию* станет полезным руководством, которое поможет регуляторным и директивным органам в принятии решений о надлежащих нормах цифрового регулирования и оценке действенности этих норм. Задача нового издания настоящего Справочника – обеспечить регуляторные органы в области ИКТ по всему миру сетевыми ресурсами и аналитическими данными, которые помогут им нарастить потенциал в области решения насущных регуляторных проблем и обмена передовым опытом в целях развития цифровой экономики.

Всемирный банк и Международный союз электросвязи рады представить вашему вниманию *Справочник по цифровому регулированию* и новую онлайн-платформу *Платформу цифрового регулирования*, разработанные в целях обновления и пересмотра *Комплекта материалов по регулированию в области ИКТ*. Данные ресурсы могут быть использованы в качестве справочных материалов и платформ для сотрудничества при создании благоприятной среды для всесторонней реализации преобразующего потенциала цифровых технологий, а также в качестве мощного инструмента, способствующего внедрению инноваций и достижению устойчивого развития в интересах всех слоев населения.

Бутейна Гермази

Директор по вопросам цифрового развития,
Всемирный банк

Дорин Богдан-Мартин

Директор Бюро развития электросвязи,
Международный союз электросвязи

Предисловие	iii
Список таблиц и рисунков.....	ix
Введение.....	xi
Выражение признательности/сведения об авторах.....	xiv
Глава 1. Регуляторное управление и регуляторная независимость	1
1.1 Введение	1
1.2 Политика и ее осуществление	2
Эволюция системы регулирования	2
Оценка потребности в модернизации и рационализации.....	4
1.3 Функции и институциональные модели регуляторных органов	5
Институциональная структура регуляторного органа	5
Традиционные сферы ответственности.....	6
Изменение мандатов/функций регуляторных и директивных органов в цифровую эпоху	6
Процессы принятия решений и установления правил в среде с участием многих заинтересованных сторон	10
1.4 Сотрудничество в сфере регулирования	13
Официальное и неофициальное сотрудничество между правительствами.....	14
1.5 Создание рамочных основ цифрового регулирования.....	18
Системы лицензирования сетей, услуг и приложений	18
Инновационные подходы к регулированию отрасли	20
1.6 Основные выводы.....	23
Разработка национальных цифровых стратегий и дорожных карт	23
Институциональная структура и функции регуляторного органа	23
Формирование систем цифрового регулирования	24
Справочные материалы.....	25
Глава 2. Конкуренция и экономика	29
2.1 Введение: преобразования в сфере регулирования в условиях цифровой экономики	29
2.2 Регулирование в цифровую эпоху	30
История вопроса	30
Тенденции последнего времени	31
Основные выводы.....	33
2.3 Регулирование рынков	34
История вопроса	34
Тенденции последнего времени	35
Основные выводы	35
2.4 Присоединение сетей.....	36
История вопроса	36
Тенденции последнего времени	37
Основные выводы.....	38
2.5 Совместное использование инфраструктуры	38
История вопроса	38
Тенденции последнего времени	39
Основные выводы	40
2.6 Регулирование цен.....	40
История вопроса	40
Тенденции последнего времени	41
Основные выводы.....	41

2.7	Урегулирование споров.....	42
	История вопроса	42
	Тенденции последнего времени	42
	Основные выводы.....	43
2.8	Выдача лицензий и разрешений.....	44
	История вопроса	44
	Тенденции последнего времени	44
	Основные выводы.....	45
2.9	Слияния и поглощения	45
	История вопроса	45
	Тенденции последнего времени	46
	Основные выводы.....	46
2.10	Налогообложение	47
	История вопроса	47
	Тенденции последнего времени	48
	Основные выводы.....	49
	Справочные материалы.....	50

Глава 3. Доступ для всех 52

3.1	Введение	52
3.2	Препятствия на пути к достижению универсального доступа к услугам широкополосной связи и цифровым услугам	54
3.3	Политика содействия обеспечению универсального доступа к услугам широкополосной связи и цифровым услугам	57
	Политика финансирования универсального доступа: решение проблем доступности.....	57
	Политика повышения ценовой доступности услуг широкополосной связи и цифровых услуг.....	60
	Политика содействия охвату цифровыми технологиями.....	62
3.4	Контроль и оценка воздействия политики в области универсального доступа.....	66
3.5	Основные выводы.....	67
	Справочные материалы.....	69

Глава 4. Вопросы, касающиеся потребителей 72

4.1	Введение в права потребителей цифровых услуг	72
	Почему нужно заботиться о правах потребителей?.....	72
	Права и обязанности потребителей в цифровом мире	75
	Общее и специальное законодательство о защите прав потребителей.....	78
	Среднестатистические потребители и уязвимые потребители	81
	Переход к использованию онлайн-данных.....	82
4.2	Система поддержки потребителей	82
	Задачи в области защиты потребителей цифровых услуг и расширении их прав и возможностей.....	82
	Взаимоотношения между потребителями и поставщиками услуг	83
	Функции регуляторных органов в области ИКТ	84
	Соответствующие международные органы	84
4.3	Конкретные проблемы, касающиеся потребителей	85
	Цена и качество услуг	85
	Контракты и предоплата	86
	Порядок выставления счетов и осуществления платежей	86
	Обслуживание клиентов, рассмотрение жалоб и возмещение ущерба	87
	Содействие потребителям в ориентации в цифровой экономике	88
	Положения, касающиеся потребителей с ограниченными возможностями	88
	"Умные" пользовательские устройства.....	89
	Для доверия необходима надежность	90
	Безопасность детей в онлайн-среде.....	91
	Безопасность взрослых в онлайн-среде.....	92
	Цифровая идентичность и автоматизированное принятие решений.....	92
4.4	Основные выводы.....	93

Введение в права потребителей цифровых услуг	93
Система поддержки потребителей	94
Конкретные проблемы, касающиеся потребителей	95
Справочные материалы.....	96
Глава 5. Защита данных и доверие	98
5.1 Введение	98
5.2 Режимы защиты данных.....	99
5.3 Регуляторные органы.....	100
5.4 Технологии и услуги	102
5.5 Последствия для трансграничной передачи данных и торговли.....	104
5.6 Конфиденциальность сообщений	105
5.7 Защита данных и информационная безопасность	107
Справочные документы.....	110
Глава 6. Управление использованием спектра	111
6.1 Введение	111
6.2 Часть 1. Руководство по регламентарной структуре для управления использованием спектра на национальном уровне	112
Международный контекст	112
Международные принципы, регулирующие использование спектра	113
Принципы использования спектра на национальном уровне	113
Использование спектра для радиовещания и для целей электросвязи в частном коммерческом и промышленном секторах	114
Предотвращение и устранение помех.....	115
Права и обязанности зарегистрированных пользователей	115
Прозрачность управления использованием спектра на национальном уровне	116
Взаимосвязь между регулированием на международном и национальном уровнях.....	116
Контроль за использованием спектра	117
Передовая практика управления использованием спектра на национальном уровне	117
6.3 Часть 2. Ключевые применения и нормативные аспекты, определяющие использование спектра в будущем	119
Введение	119
Основные тенденции в управлении использованием спектра для внедрения новых технологий	119
Технологические инновации, определяющие спрос на новые участки спектра.....	120
Управление использованием спектра и стандарты новых технологий.....	121
Лицензирование спектра на национальном уровне.....	124
Новые бизнес-модели и инновации в использовании спектра	131
6.4 Основные выводы	133
Справочные документы.....	134
Глава 7. Реагирование регуляторных органов на развитие технологий.....	138
7.1 Введение	138
7.2 Эволюция технологий.....	139
Облачные вычисления.....	140
Интернет вещей	141
Большие данные	142
Блокчейн	144
Искусственный интеллект	145
"Умные" функциональные возможности и защита данных.....	147
Защита данных как объединяющий фактор.....	148
7.3 Развитие цепочки создания стоимости в интернете	151
7.4 Эволюция бизнес-моделей в секторе ИКТ	152
7.5 Резюме	155
Справочные материалы.....	157

Глава 8. Техническое регулирование 159

8.1	Часть 1. Качество обслуживания	159
	Введение	159
	Выбор параметров	163
	Определение измерений	165
	Установление целевых значений	166
	Выполнение измерений	166
	Проверка измерений	168
	Публикация результатов измерений	168
	Стимулирование повышения качества	169
	Обзор достигнутых результатов	170
8.2	Часть 2. Нумерация, наименование, адресация и идентификация (ННАИ)	171
	Почему важны нумерация, наименование и адресация?	171
	Что такое ресурсы ННАИ?	171
	Управление ННАИ	171
	Глобальные ресурсы ННАИ	172
	Наступление цифровой эпохи	173
	Влияние новых технологий	173
	Какие инструменты может использовать регуляторный орган?	174
	Новые виды использования несут с собой новые проблемы	175
	Международные ресурсы ННАИ	176
	Будущие проблемы, связанные с ННАИ	176
	Справочные документы	178

Глава 9. Связь в чрезвычайных ситуациях 180

9.1	Введение	180
	Почему важны электросвязь/ИКТ в чрезвычайных ситуациях?	180
	Какие бывают виды опасностей?	181
	Что должен делать регуляторный орган?	183
	Что представляет собой процесс управления рисками бедствий?	184
9.2	Этап смягчения последствий	185
9.3	Этап обеспечения готовности	188
9.4	Этап реагирования	188
9.5	Этап восстановления	189
	Справочные документы	190

Список таблиц и рисунков

Таблицы

Таблица 1.1. Примеры областей сотрудничества регуляторных органов ИКТ и других ведомств.....	16
Таблица 1.2. Креативные подходы к разработке правил использования спектра	21
Таблица 3.1. Ключевые проблемы универсального доступа, с которыми сталкиваются развивающиеся страны	56
Таблица 4.1. Карта цифровых прав потребителей и граждан	77
Таблица 4.2. Ответственность за вопросы, связанные с защитой потребителей услуг ИКТ, и соответствующее законодательство в странах мира	80
Таблица 4.3. Круг задач в отношении защиты потребителей цифровых услуг	83
Таблица 6.1. Примеры лицензирования для локальных и частных сетей	129
Таблица 7.1. Источники больших данных	143
Таблица 7.2. Экосистема защиты данных.....	150
Таблица 7.3. Развитие цифровой бизнес-модели неизбежно	154
Таблица 7.4. Рентабельность по EBITDA во всей цепочке создания стоимости на основе проверенной финансовой отчетности (проценты)	155
Таблица 9.1. Уровни воздействия опасностей на инфраструктуру электросвязи	187

Рисунки

Рисунок 1.1. Поколения регулирования: от G1 к G5	2
Рисунок 1.2. Страны, в которых существуют/отсутствуют общие стратегии национального развития, цифровые повестки дня или стратегии стимулирования экономики, затрагивающие вопросы широкополосной связи	4
Рисунок 1.3. Примеры процессов принятия решений в Бразилии, Колумбии, Катаре и Сингапуре	10
Рисунок 1.4. Состояние сотрудничества в сфере регулирования между регуляторными органами ИКТ и другими ведомствами при условии наличия этих органов и ведомств и их функционирования в качестве отдельных структур, весь мир, 2018 год.....	15
Рисунок 1.5. Три основных вида систем лицензирования	18
Рисунок 1.6. Подходы к лицензированию: от менее жестких к более жестким.....	20
Рисунок 1.7. Элементы модели регуляторной "песочницы" во Франции и Таиланде	22
Рисунок 2.1. Сетевые эффекты цифровых платформ	31
Рисунок 2.2. Как рассчитываются цены на присоединение на основе затрат	37
Рисунок 2.3. Во главу угла в регуляторных моделях на основе затрат следует ставить цены доступа.....	38
Рисунок 2.4. Способы снизить риск возникновения споров по вопросам присоединения/ценообразования	42
Рисунок 2.5. Тенденция к переходу на единые лицензии/общие разрешения	45
Рисунок 2.6. Виды налогов, применяемых в секторе ИКТ, общемировые показатели (проценты), 2019 год	48
Рисунок 3.1. Количество физических лиц, пользующихся интернетом, и темпы роста этого показателя	53
Рисунок 3.2. Количество стран, в которых в определение УДО включен широкополосный доступ	55
Рисунок 4.1. Сообщения регуляторных органов ИКТ о деятельности, связанной с вопросами защиты прав потребителей, 2010 и 2019 годы.....	81
Рисунок 6.1. Технологии, определяющие спрос на спектр.....	120
Рисунок 6.2. Орган управления использованием спектра	123
Рисунок 6.3. Механизмы лицензирования спектра	125
Рисунок 6.4. Режимы совместного использования спектра.....	130
Рисунок 7.1. Экосистема цифрового регулирования	139
Рисунок 7.2. Связи между технологиями, рассматриваемыми в этой главе	140
Рисунок 7.3. Лицензированные сотовые соединения IoT в мире (млн.)	141
Рисунок 7.4. Блокчейн	144
Рисунок 7.5. Подход, ориентированный на наращивание функциональных возможностей	147
Рисунок 7.6. Пример, иллюстрирующий продажу Tesla за границу и использование данных	

третьими лицами	148
Рисунок 7.7. Цикл создания стоимости в интернете.....	151
Рисунок 7.8. Наглядные тенденции развития бизнес-моделей цифровой подвижной связи	153
Рисунок 7.9. Изменение регуляторных подходов с течением времени	156
Рисунок 8.1. Деятельность в рамках контроля QoS.....	162
Рисунок 8.2. Методы стимулирования повышения качества.....	170
Рисунок 9.1. Виды стихийных бедствий	181
Рисунок 9.2. Частота стихийных бедствий в мире, 1990–2020 годы ^а	182
Рисунок 9.3. Этапы управления рисками бедствий	185

Вставки

Вставка 1.1. Споры о юрисдикции в отношении видеоконтента ОТТ в Индии.....	7
Вставка 1.2. Обзор цифровых регуляторных органов в Австралии, Ирландии и Соединенном Королевстве.....	9
Вставка 1.3. Расширенное определение услуг электронной связи в Кодексе ЕЕСС	11
Вставка 1.4. Нидерланды: межотраслевое сотрудничество в сфере обеспечения соблюдения правовых норм.....	13
Вставка 1.5. Определение сотрудничества в сфере регулирования в соответствии с концепцией G5.....	14
Вставка 1.6. Правительство Сингапура развивает сотрудничество в сфере искусственного интеллекта	17
Вставка 3.1. Целевые показатели Комиссии по широкополосной связи в интересах устойчивого развития на период до 2025 года	53
Вставка 3.2. Эволюция политики в области универсального доступа и обслуживания.....	55
Вставка 3.3. Примеры эффективных ФУДО.....	59
Вставка 3.4. Различные подходы к развертыванию общедоступной сети Wi-Fi.....	61
Вставка 4.1. Заявление BEREC о стратегии расширения прав и возможностей потребителей	74
Вставка 4.2. Принципы, перечисляемые в принятых ГСР-14 Руководящих указаниях на основе примеров передового опыта по защите прав потребителей в цифровом мире	76
Вставка 5.1. Глобальная ассамблея по вопросам конфиденциальности.....	102
Вставка 5.2. Исследование конкретной ситуации: приложения для отслеживания COVID-19	103
Вставка 5.3. Цена утечки данных.....	108
Вставка 6.1. Руководящие принципы по ограничению воздействия электромагнитных полей на человека.....	124
Вставка 9.1. Этапы разработки национального плана электросвязи в чрезвычайных ситуациях	184

Всемирный банк и Международный союз электросвязи рады представить вашему вниманию *Справочник по цифровому регулированию*, являющийся результатом более чем двадцатилетнего сотрудничества между этими организациями. Цель Справочника заключается в том, чтобы предоставить доступ к практическим руководящим указаниям и передовому опыту директивным и регуляторным органам во всем мире, занимающимся вопросами использования преимуществ цифровой экономики и общества в интересах своих граждан и компаний. Справочник содержит не только сведения об основах регулирования в области ИКТ, обновленные с учетом масштабной цифровой трансформации в различных отраслях, но и информацию о новых аспектах и инструментах регулирования, на которые регуляторным органам ИКТ следует обратить внимание при принятии решений по вопросам регулирования. Справочник также станет полезным источником информации для других заинтересованных сторон, действующих в отрасли электросвязи, а также для учреждений, занимающихся вопросами развития, гражданских и потребительских групп и научных кругов.

Наряду со *Справочником по цифровому регулированию* разрабатывается новая онлайн-овая *Платформа цифрового регулирования*, предназначенная для обновления и пересмотра *Комплекта материалов по регулированию в области ИКТ*. Платформа опирается на материалы Справочника и дополняет его, предоставляя более подробные руководящие указания и исследуя конкретные случаи применения передового опыта в области регулирования цифровой экономики. Предполагается, что Справочник даст представление о текущем состоянии дел, сложившемся в 2020 году, в то время как Платформа станет динамичной и будет постоянно обновляться в предстоящие годы, с тем чтобы отражать быстрое изменение цифрового мира.

Работа по созданию исходного Справочника началась в 2000 году на фоне формировавшихся тогда тенденций приватизации и либерализации рынков электросвязи. Основной целью этой работы было содействие и обеспечение добросовестной конкуренции, и, таким образом, содержание Справочника касалось главным образом лицензирования, присоединения сетей, регулирования цен и универсального обслуживания. Десятое юбилейное издание Справочника, вышедшее десять лет спустя, в 2010 году, отразило растущее значение электросвязи для развития национальной экономики, а также влияние, которое быстрое распространение интернета и подвижной сотовой связи по всему миру оказало на формирование регуляторной среды; теперь акцент был сделан на управлении использованием спектра и дополнительных услугах. В настоящее время основополагающие аспекты регулирования электросвязи и ИКТ по-прежнему сохраняют свое значение, однако самые масштабные задачи в области регулирования связаны с формированием экономики, основанной на данных, ведущую роль в которой играют новые технологии и приложения, такие как большие данные, интернет вещей и связанные с ними новые бизнес-модели.

Цифровые приложения сегодня пронизывают все сферы экономики и жизни общества: благодаря им пользователи получают доступ к государственным услугам, осуществляют мобильные платежи, играют в компьютерные игры, слушают музыку, смотрят фильмы, эффективнее организуют свои поездки и так далее. Становится все очевиднее, что движущей силой этого цифрового мира является использование данных. Следовательно, важнейшая проблема, которая стоит перед нами сегодня, касается способов нормативного регулирования вопросов о том, кто несет ответственность за данные и как организуется сбор, хранение, обработка и распространение данных.

Цифровая трансформация затрагивает все стороны нашей жизни, и в связи с этим возникают новые задачи для регуляторных структур, которые традиционно ведали определенными отраслями или сферами. Например, вопросы защиты данных не являются исключительной прерогативой отрасли ИКТ, и в будущем нам понадобится разработать более гибкий подход, предусматривающий либо сотрудничество и взаимодействие отраслевых регуляторных органов, либо создание новых специализированных учреждений, которые займутся решением проблем, возникающих в ходе развития цифровой экономики. Эти и другие вопросы рассматриваются в *Справочнике по цифровому регулированию*, с тем чтобы помочь директивным и регуляторным органам разобраться в новых вызовах, связанных с процессами цифровой трансформации.

Соответственно, структура Справочника выглядит следующим образом.

В главе 1 "Регуляторное управление и регуляторная независимость" представлен перспективный анализ изменений регуляторного управления ИКТ в процессе его адаптации к развитию цифровых технологий. Эта глава содержит обзор эволюции методов регулирования и реализации политики в процессе перехода от традиционной среды электросвязи к ИКТ, а затем – к цифровым технологиям. Анализ ролей и институциональных моделей регуляторных органов охватывает регуляторные структуры, широко распространенные по всему миру, и традиционные области регулирования, включая характер возможных изменений мандата регуляторных органов в цифровой среде. В этой главе рассматривается один из ключевых элементов будущей модели регулирования – сотрудничество в сфере регулирования, предполагающее координацию действий различных отраслевых ведомств и государственных учреждений. Кроме того, рассматриваются и альтернативные модели регулирования, такие как саморегулирование или сотрудничество между отраслевыми и государственными структурами.

В главе 2 "Конкуренция и экономика" представлен обзор существенных пертурбаций на рынке и в сфере регулирования, вызываемых цифровой трансформацией. В этой главе рассматриваются существующие экономические проблемы, связанные с цифровым регулированием, а также вопросы, связанные с регулированием рынков, присоединением сетей, совместным использованием инфраструктуры, регулированием цен, разрешением споров, лицензированием и сертификацией, слияниями и приобретениями, а также налогообложением.

В главе 3 "Доступ для всех" рассматриваются ключевые проблемы и политика в отношении достижения целей по универсальному доступу в контексте цифровой трансформации. Обсуждение сосредоточено на трех темах: обеспечение возможности установления соединений, в связи с чем рассматриваются проблемы, имеющие отношение к финансированию расширения инфраструктуры широкополосной связи; ценообразование (обсуждаются ценовые барьеры, препятствующие распространению цифровых услуг и устройств конечных пользователей); а также охват цифровыми технологиями (рассматриваются меры политики по развитию цифровых навыков, преодолению гендерного неравенства и обеспечению доступности услуг для лиц с ограниченными возможностями, а также созданию местного цифрового контента).

В главе 4 "Вопросы, касающиеся потребителей" рассматривается система поддержки потребителей, в рамках которой действуют регуляторные органы ИКТ, а также, в связи с этим, – ориентированные на интересы потребителей меры, которые, скорее всего, станут прерогативой регуляторных органов ИКТ. В этой главе определяются основные проблемы потребителей, уже возникающие в условиях цифровой экономики, и вкратце описываются изменяющиеся перспективы и нужды потребителей.

В главе 5 "Защита данных и доверие" исследуется природа режимов защиты данных с уделением особого внимания их регуляторным аспектам. В ней изучается степень, в которой должны и могут затрагиваться появляющиеся технологии и услуги, а также меры контроля над трансграничным потоком персональных данных и вытекающие из этого последствия для торговли. Вопросы защиты данных и обеспечения конфиденциальности в значительной мере пересекаются при рассмотрении необходимости введения специальных правил, регулирующих коммуникативную деятельность. Кроме того, исследуется сложное соотношение между защитой данных и информационной безопасностью.

Глава 6 "Управление использованием спектра" состоит из двух частей. Первая часть представляет собой общее руководство по нормативной базе для управления использованием спектра на национальном уровне, начиная с определения международного контекста и процессов. Во второй части рассматриваются ключевые применения и нормативные аспекты, определяющие использование спектра в будущем, и выделяются некоторые основные моменты, которые предлагается рассмотреть регуляторным органам на национальном уровне, исходя из соответствующего опыта разных стран. В ней представлены некоторые механизмы распределения спектра и лицензирования нового спектра с должным учетом развития технологий. В ней также рассматриваются вопросы поощрения использования спектра для этих ключевых применений и бизнес-модели, способствующие укреплению существующих и новых подходов к развертыванию сетей беспроводной широкополосной связи.

В главе 7 "Реагирование регуляторных органов на развитие технологий" рассматривается общая тенденция к пересмотру функций различных регуляторных органов в ответ на появление технологий облачных вычислений, ИИ, блокчейн, больших данных и интернета вещей (IoT). Желаемые конечные результаты – добросовестная конкуренция, защита прав потребителей и экономическое развитие – остаются неизменными, однако способы их достижения изменяются со временем и отличаются друг от друга в разных странах. Цель этой главы – предложить базовую модель определения соответствующего подхода к регулированию в ответ на возникновение новых технологий.

В главе 8 "Техническое регулирование" рассматриваются два аспекта: качество обслуживания (QoS) и вопросы нумерации, наименования, адресации и идентификации (ННАИ). В части, посвященной QoS, описывается роль регуляторного органа в информировании пользователей, сдерживании операторов, имеющих сильные конкурентные позиции, обеспечении эффективного использования ограниченных ресурсов и оценке национальной инфраструктуры. Рассматривается деятельность регуляторных органов, связанная с контролем QoS, в том числе выбор показателей, определение измерений, установление целевых значений, выполнение измерений, их проверка и публикация их результатов, стимулирование повышения качества и обзор достигнутых результатов. В части, посвященной ННАИ, разъясняется значимость ННАИ, кратко излагаются главные цели управления ННАИ, рассматривается воздействие новых технологий на ННАИ и описываются инструменты, находящиеся в распоряжении регуляторного органа.

В главе 9 "Связь в чрезвычайных ситуациях" рассматриваются функции регуляторных органов в условиях различных бедствий, в том числе метеорологических явлений, таких как ураганы, наводнения и засухи, геологических катаклизмов, таких как землетрясения, извержения вулканов, и биологических угроз, в том числе эпидемий, а в последнее время еще и пандемий. В этой главе рассматриваются четыре этапа процесса управления рисками бедствий – смягчение последствий, обеспечение готовности, реагирование и восстановление, – а также роль ИКТ и электросвязи на каждом из этих этапов.

Выражение признательности/сведения об авторах

Справочник по цифровому регулированию был подготовлен группой авторов под эгидой Международного союза электросвязи (Нэнси Сандберг, Юлия Лозанова и Софи Мэдденс, Отдел регуляторной и рыночной среды, при общей координации Ын Чу Ким, временно исполняющей обязанности руководителя Департамента центра цифровых знаний, Бюро развития электросвязи МСЭ (БРЭ)) и Всемирного банка (Тим Келли, Року Фукуи и Ида Мбуб, Глобальная практика по вопросам цифрового развития) под руководством Дорин Богдан-Мартин, Директора Бюро развития электросвязи МСЭ, и Бутейны Гермази, Директора по вопросам цифрового развития, Группа Всемирного банка. Авторами глав Справочника являются:

Глава 1 "Регуляторное управление и регуляторная независимость" – Джанет Эрнандес, президент компании Telecommunications Management Group

Глава 2 "Конкуренция и экономика" – Дэвид Роджерсон, директор компании Incyte Consulting

Глава 3 "Доступ для всех" – Джанет Эрнандес, президент компании Telecommunications Management Group

Глава 4 "Вопросы, касающиеся потребителей" – Клэр Милн, партнер, компания Antelope Consulting

Глава 5 "Защита данных и доверие" – Ян Уолден, профессор информационного и коммуникационного права и директор Центра исследований коммерческого права, Лондонский университет королевы Марии

Глава 6 "Управление использованием спектра", часть 1 – 1-я Исследовательская комиссия МСЭ-R, Сектор радиосвязи МСЭ; часть 2 – Джеральдо Нето, старший советник по техническим вопросам и вопросам политики, компания Telecommunications Management Group

Глава 7 "Реагирование регуляторных органов на развитие технологий" – Кристоф Сторк, партнер, компания Research ICT Solutions

Глава 8 "Техническое регулирование", часть 1 "Качество обслуживания" – Роберт Милн, партнер, компания Antelope Consulting; часть 2 "Нумерация, наименование, адресация и идентификация (ННАИ)" – Фил Раштон, директор компании Rushton Communications Consulting Ltd, при участии Роберта Милна

Глава 9 "Связь в чрезвычайных ситуациях" – Хуан Ролдан, президент компании Luxon Consulting Group, LLC, при участии Роберта Милна, партнера, компания Antelope Consulting

Справочник выходит под редакцией Колина Блэкмена, директора компании Camford Associates

Кроме того, мы хотели бы выразить признательность следующим лицам за поддержку и содействие в анализе материалов настоящего Справочника: Мартину Адольфу, Кристине Буэти, Марице Дельгадо, Роберту Кларку, Жан-Жаку Массиме, Митили Менон, Кармен Прадо-Вагнер, Кристине Санд, Диане Томимуре, Джоан Уилсон, Мейке Хертогс и Цзе Чжан (МСЭ) и Жерому Беззине, Тане Берасо Гомес, Петеру Лундквисту и Дэвиду Сатолу (Группа Всемирного банка).

Глава 1. Регуляторное управление и регуляторная независимость



1.1 Введение

Нормативно-правовая база, регуляторное управление и регуляторная независимость учреждений являются основополагающими элементами эффективного регулирования. Сегодня перед регуляторными и директивными органами стоит ряд задач: они должны уделять внимание традиционным аспектам информационно-коммуникационных технологий (ИКТ) и определять подходящую им роль в решении регуляторных и политических вопросов, возникающих в связи с появлением новых цифровых технологий и услуг.

Наряду с более традиционными вопросами, такими как обеспечение возможностей установления соединений и развитие инфраструктуры, цифровая среда побуждает обращать внимание на более широкий круг отраслей за пределами ИКТ, включая здравоохранение, финансовый сектор, образование, транспорт и энергетику. К числу вопросов, требующих рассмотрения, относятся, среди прочего, вопросы регулирования контента, обеспечения конфиденциальности, защиты прав потребителей, конкуренции и использования искусственного интеллекта (ИИ). Традиционные регуляторные органы ИКТ могут, в зависимости от своих компетенций и возможностей, недостаточно хорошо разбираться в этих вопросах, располагать ограниченными ресурсами для их решения, не иметь четких полномочий для их решения или согласовывать свои действия по решению этих вопросов с другими учреждениями в соответствии со своими действующими мандатами.

В целом мировое сообщество пока находится на начальной стадии обсуждения этих вопросов. Некоторые страны уже пытаются найти цифровым технологиям место в своей нормативно-правовой базе, однако многим другим еще лишь предстоит приступить к этому процессу. Таким образом, у стран есть обширные возможности для инноваций, адаптации и развития. В отсутствие отработанного механизма, который без труда можно было бы применить в разных юрисдикциях, исключительно важное значение для привлечения заинтересованных сторон приобретают информационно-разъяснительная работа и открытые консультации, а каждой стране настоятельно необходимы процедуры принятия решений на основании фактических данных, позволяющие находить осуществимые, разумные и гибкие решения.

С учетом этих проблем в главе 1 *Справочника по цифровому регулированию* предложен перспективный анализ изменений регуляторного управления ИКТ в процессе его адаптации к развитию цифровых технологий. Глава начинается с обзора эволюции методов регулирования и реализации политики в процессе перехода от традиционной среды электросвязи к ИКТ, а затем — к цифровым технологиям. Анализ ролей и институциональных моделей регуляторных органов охватывает регуляторные структуры, широко распространенные по всему миру, и традиционные области регулирования. Затем внимание сосредоточивается на возможных изменениях мандата регуляторных органов в цифровой среде, при этом особо подчеркивается важность процесса принятия эффективных решений в интересах всех

слоев населения. Далее в этой главе рассматривается один из ключевых элементов будущей модели регулирования – сотрудничество в сфере регулирования, предполагающее координацию действий различных отраслевых ведомств и государственных учреждений. Кроме того, рассматриваются и альтернативные модели регулирования, такие как саморегулирование или сотрудничество между отраслевыми и государственными структурами. Наконец, особое внимание в этой главе уделено некоторым ключевым факторам формирования цифровых систем, в том числе вопросам, касающимся лицензирования сетей и услуг, выдачи разрешений на использование спектра, а также разработки инновационных подходов к отраслевому регулированию, основанных на фактических данных¹.

1.2 Политика и ее осуществление

Эволюция системы регулирования

В течение последних тридцати лет система регулирования отрасли претерпевала изменения, начавшиеся с развития нормативно-правовой базы регулирования электросвязи по мере того, как страны начали открывать свои рынки для конкуренции. Затем система регулирования расширилась: она охватила ИКТ и распространилась на новые технологии и услуги на базе интернета. В настоящее время идет процесс перехода от ИКТ к цифровому пространству, побуждающий директивные и регуляторные органы к изучению далеко идущих социальных и экономических последствий появления новых технологий, затрагивающих все отрасли экономики, в том числе онлайн-платформ, 5G, облачных вычислений и интернета вещей (IoT).

От среды традиционной электросвязи – к цифровому ландшафту

МСЭ разработал комплексную модель оценки изменений в сфере регулирования, позволяющую отслеживать смену поколений регулирования (см. рисунок 1.1). На примере перехода от поколения 1 (G1) к поколению 4 (G4) можно проследить эволюцию регулирования электросвязи и ИКТ: первоначальный режим управления и контроля, как правило, тесно связанный с государственными монополиями, последовательно заменили приватизация и либерализация и потребность в привлечении инвестиций, после чего произошел сдвиг в сторону достижения социально-экономических целей. Поколение 5 (G5) представлено в качестве последнего поколения, однако оно "рассматривается как дополнение к предыдущим поколениям", свидетельствуя о возрастающем значении более гибких совместно используемых нормативно-правовых баз, способных учитывать активное влияние цифровой экономики в различных отраслях (ITU 2020, 26).

Рисунок 1.1. Поколения регулирования: от G1 к G5



Источник: ITU, ICT Regulatory Tracker 2018, <https://www.itu.int/net4/itu-d/irt/#/generations-of-regulation>; ITU 2020.

Примечание. – Количественные показатели для поколений 1–4 определяются с помощью Инструмента отслеживания нормативно-правовой базы в области ИКТ (ICT Regulatory Tracker). Для определения количественных показателей поколения 5 используется Опорный показатель G5.

Аналогичным образом, Организация экономического сотрудничества и развития (ОЭСР) рекомендует "согласовывать политику в области цифровой трансформации между всеми политическими сферами и субъектами, затронутыми цифровой трансформацией (и затрагивающими ее)" (OECD 2019, 147). ОЭСР

¹ Затрагиваемые в этой главе вопросы подробнее рассматриваются в соответствующих тематических разделах *Платформы цифрового регулирования*.

также признает отсутствие универсальных управленческих решений и указывает, что управление надлежит адаптировать к институциональным возможностям и регуляторной культуре каждой страны, принимая во внимание тот факт, что эти структуры продолжают изменяться в будущем.

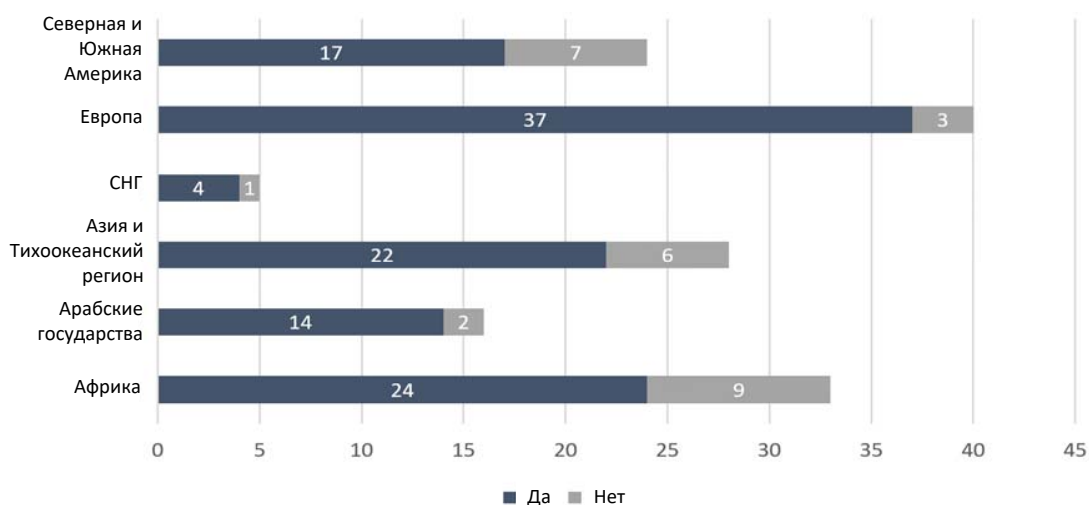
Важным средством содействия переходу к системам пятого поколения является внедрение адаптивного регулирования. Это предполагает разработку гибкого отраслевого законодательства и режима регулирования, призванных реагировать на быстрые изменения в сфере технологий, услуг и рынков (ITU 2019; World Bank and ITU 2021 (готовится к выпуску)). Директивные органы могут принять адаптивный регуляторный подход, предусматривающий сотрудничество с участниками отрасли в целях эффективного использования их знаний и опыта, что позволит регуляторным органам выступать в качестве партнеров или координаторов.

Несмотря на признание важности этого нового сдвига в представлениях о смысле регулирования, в системах регулирования многих стран все еще отсутствуют основополагающие компоненты. Эти ограничения препятствуют развитию их отраслей ИКТ. Комиссия по широкополосной связи в интересах устойчивого развития отметила в своем докладе *Состояние широкополосной связи, 2019 год*, что 72 страны до сих пор либо остаются на уровне G1 – базовом уровне регуляторной политики в области ИКТ с регулируемыми государственными монополиями и командно-административным режимом, либо переходят на уровень G2, начиная осуществлять либерализацию рынков, частичную либерализацию или приватизацию (Broadband Commission for Sustainable Development 2019). Эти страны могут упустить возможности в области развития, что приведет к их дальнейшему отставанию от тех стран, которые, достигнув уровней G3 и G4, обеспечили внедрение инноваций и интеграцию ИКТ в социально-экономическую политику. Как будет показано ниже, принятие комплексных цифровых стратегий имеет большое значение, но помимо этих мер также может потребоваться дальнейшее реформирование основополагающих систем и структур.

Осуществление комплексных и ориентированных на конкретные технологии цифровых стратегий

Цифровые стратегии, планы и дорожные карты помогают определять цели политики и устанавливать контрольные показатели. Цифровые стратегии или планы были приняты как минимум в 73 странах (ITU 2020), в том числе в Колумбии, Уругвае, Нигере и Кении. Например, в Колумбии Министерство связи и информационных технологий (MINTIC) обнародовало новый План в сфере ИКТ на 2018–2022 годы *Цифровое будущее для всех* (MINTIC 2018). Цифровая повестка дня на 2020 год в Уругвае также призвана содействовать устойчивой, отвечающей интересам всех слоев населения цифровой трансформации страны, причем одной из ее основных целей является обеспечение "близости правительства". "Близость правительства" предусматривает применение различных методов поддержания взаимосвязи между гражданами и государством, содействуя расширению прозрачности, подотчетности, участия, а также развитию более эффективных услуг. Достижение этой цели предполагает создание прямых каналов связи между гражданами и правительством и повышение качества предоставляемых услуг (AGESIC 2017). Цифровые планы разработали и многие страны Африканского региона. В 2017 году правительство Нигерии приняло *Проект развития "умной" цифровой экономики* в Нигерии, направленный на расширение экономических возможностей и конкуренции. Этот проект включает ряд инициатив в области ИКТ, в том числе инициативу по расширению возможностей установления широкополосных соединений. Приоритетное внимание в его рамках также уделяется цифровым решениям, таким как расширение системы электронного правительства, вовлечение нигерийской молодежи в инновационную деятельность, обучение инженеров разработке программного обеспечения и содействие развитию электронной торговли (World Bank 2019). В 2019 году Кения также приняла *Концептуальный проект цифровой экономики* в качестве дорожной карты цифровой трансформации в стране, чтобы претворить в жизнь выгоды, предоставляемые цифровой экономикой (Republic of Kenya 2019). В этом концептуальном проекте представлены пять компонентов, которые должны стать фундаментом развития цифровой экономики: цифровое правительство, цифровой бизнес, инфраструктура, ориентированное на инновации предпринимательство, а также цифровые навыки и ценности. Кроме того, помимо конкретных цифровых стратегий и планов, по меньшей мере в 118 странах действуют стратегии национального развития, цифровые повестки дня или стратегии стимулирования экономики, затрагивающие вопросы широкополосной связи (см. рисунок 1.2).

Рисунок 1.2. Страны, в которых существуют/отсутствуют общие стратегии национального развития, цифровые повестки дня или стратегии стимулирования экономики, затрагивающие вопросы широкополосной связи



Примечание. – На рисунке отмечены только те страны, по которым имеются данные.

Источник: МСЭ, данные глобального обследования политики и стимулов в области развития широкополосной связи.

Хотя в некоторых из этих цифровых стратегий могут отсутствовать определенные ключевые компоненты, например возможность применения стратегии в нескольких отраслях или меры по достижению международных целей в области развития, страны все чаще реализуют всеобъемлющие планы, охватывающие все отрасли. Кроме того, эти планы являются важнейшими механизмами определения задач и целей в области установления соединений и наглядно свидетельствуют о большом значении цифровой среды для всех сфер экономической и социальной жизни страны. Они также играют важную роль в распространении информации о совместном регулировании и привлечении многих заинтересованных сторон, тем самым способствуя принятию комплексного подхода к цифровому развитию и планированию.

В последнее время страны также стали активнее разрабатывать стратегии, ориентированные на конкретные технологии или вопросы, такие как автоматизация, робототехника, 5G, ИИ и IoT. Например, в 2017 году Министерство науки, технологий и инноваций Малайзии (MOSTI) приняло *Национальную стратегическую дорожную карту в области IoT*, определив в ней три основные цели: создание конкурентоспособной промышленной экосистемы IoT, укрепление потенциала предпринимателей в сфере новых технологий и превращение страны в региональный центр развития IoT (MOSTI 2017). Множество стран, в том числе Германия, опубликовали стратегии развития искусственного интеллекта. Австралия, Германия, Соединенное Королевство и Сингапур, равно как и другие страны, утвердили программные или стратегические документы по развитию 5G. В 2015 году правительство Японии опубликовало *Новую стратегию роботизации*, в которую входят меры по "осуществлению революции в сфере робототехники", а также пятилетний план решения межотраслевых и конкретных отраслевых вопросов (Headquarters for Japan's Economic Revitalization 2015).

Оценка потребности в модернизации и рационализации

Когда директивные органы начинают осуществлять свои планы цифрового развития и адаптировать системы нормативного регулирования к условиям цифровой экономики, чрезвычайно важно не допускать простой экстраполяции или распространения действия существующих, потенциально устаревших законов и норм на новых участников рынка или на новые области. Вместо этого директивным органам следует принимать меры – возможно, включая дерегулирование, саморегулирование или совместный подход к регулированию, – которые будут способствовать расширению масштабов инновационной деятельности, упрощению внедрения новых и появляющихся технологий, стимулированию инвестиций и ориентации на всеохватность и сотрудничество.

Это влечет за собой не только применение принципа оценки регуляторного воздействия к процессу принятия решений; следует провести обзор всего комплекса существовавших ранее, нынешних и возникающих рисков с точки зрения их влияния на достижение национальных целевых показателей.

Благодаря этому регуляторные органы будут располагать более эффективными возможностями для внедрения гибких мер политики, способствующих инвестициям и инновациям, а следовательно, и формированию устойчивой цифровой экономики (ICC 2016).

В этом смысле правительствам следует перейти от регулирования на основе правил к регулированию на основе принципов. В цифровую эпоху руководствоваться общими принципами "удобнее для поиска сбалансированных, надежных решений, особенно в сложных областях деятельности" (ITU 2020, 7). Например, в 2019 году палата лордов Соединенного Королевства предложила десять принципов регулирования цифровой среды, в том числе принципы равенства, подотчетности, обеспечения конфиденциальности и этического проектирования (House of Lords 2019).

1.3 Функции и институциональные модели регуляторных органов

Институциональная структура регуляторного органа

Существуют три основные институциональные модели регуляторных органов, осуществляющих надзор за отраслью ИКТ: отраслевой регуляторный орган, межотраслевой регуляторный орган и регуляторный орган в конвергентной среде. Специализированные отраслевые регуляторные органы были традиционно широко распространены в отрасли электросвязи. В современной среде ИКТ и цифровой среде регуляторные органы, занимающиеся только надзором за электросвязью, встречаются реже, чем конвергентные или межотраслевые регуляторные органы. Регуляторные органы электросвязи зачастую также занимаются вопросами управления почтовыми службами или отвечают за управление использованием спектра. Например, Регуляторный орган электросвязи Афганистана (ATRA) и Управление электросвязи Барбадоса (TU) занимаются как вопросами электросвязи, так и вопросами управления использованием спектра².

Кроме того, до либерализации отрасли электросвязи нередко создавались межотраслевые регуляторные органы, к числу которых традиционно принадлежали регуляторные органы сферы коммунальных услуг. Одним из примеров является Управление по вопросам регулирования в сфере коммунальных услуг (OUR) Ямайки, осуществляющее надзор над отраслями электросвязи, электроснабжения, водоснабжения и транспорта, тогда как вопросами управления использованием спектра и радиовещания занимаются два отдельных ведомства³. Следует отметить, что в период между 2014 и 2016 годами Ямайка подготовила законопроект о создании конвергентного регуляторного органа ИКТ, и Министерство науки, энергетики и технологий⁴ (MSET) продолжает стремиться к достижению этой цели (Angus 2014). К числу других стран, где действуют межотраслевые регуляторные органы, относится Дания (Управление энергетики Дании), Багамские Острова (Управление по вопросам регулирования и конкуренции в сфере коммунальных услуг) и Белиз (Комиссия по вопросам коммунальных услуг).

Принимаемые Ямайкой меры по созданию конвергентного регуляторного органа ИКТ находятся в русле многолетней тенденции к созданию конвергентных регуляторных органов, предусматривающей учреждение одного регуляторного органа, ответственного за сферы электросвязи, управления использованием спектра и радиовещания/средств массовой информации. В 2007 году конвергентные регуляторные органы составляли примерно треть от общего числа институциональных структур во всем мире (ITU 2018a). К 2017 году более 70% регуляторных органов во всем мире стали конвергентными. К числу стран, создавших конвергентные регуляторные органы в течение последних нескольких лет, относятся, в частности, Ботсвана и Сингапур. В Сингапуре создание конвергентного регуляторного органа позволило расширить возможности для управления "достижениями технического прогресса, способствовавшими размыванию границ между радиовещанием и электросвязью" (MCI 2016). Аналогичным образом, в 2013 году Ботсвана создала Регуляторный орган связи Ботсваны (BOCRA) на базе Управления электросвязи Ботсваны и Национального комитета по радиовещанию, препоручив новому органу решение всех вопросов, касающихся ИКТ, радиовещания, интернета, управления спектром и почтовых услуг (Botswana 2012).

² ITU, National Telecommunication Agencies. <https://www.itu.int/en/ITU-D/Statistics/Pages/links/nta.aspx>

³ *Ibid.*

⁴ Ministry of Science, Energy, and Technology (MSET). Invest in Technology. <https://www.mset.gov.jm/invest-in-technology/>

Традиционные сферы ответственности

В рамках трех первых поколений регулирования (G1–G3), а отчасти и в четвертом поколении в сферу ответственности регуляторных органов электросвязи или ИКТ в первую очередь входят вопросы установления и обеспечения выполнения относительно жестких правил, которые были сочтены необходимыми для защиты конкуренции и прав потребителей в процессе постепенного отказа стран от монопольных рынков электросвязи. Краеугольным камнем сферы ответственности регуляторных органов было лицензирование, зачастую предусматривавшее комплексные процедуры подачи и рассмотрения заявок, позволяющие убедиться, что новые участники рынка располагают необходимыми техническими и финансовыми возможностями для достижения успеха.

Обычно регуляторные органы также устанавливают широкий круг различных обязательств. Например, в соответствии с требованиями о раскрытии информации о тарифах поставщики услуг обязаны представлять расценки и тарифы на утверждение регуляторному органу; эти меры призваны защитить потребителей от незаконного взимания платы за оказываемые услуги. Регуляторные органы вводили обязательства в области присоединения и устанавливали тарифы на завершение вызова, чтобы предоставить операторам, особенно новым участникам рынка, возможность получать доступ к сетям друг друга. Эти меры также способствовали защите прав потребителей, предоставляя им возможность поддерживать связь с другими лицами вне зависимости от того, какой оператор их обслуживает. Регуляторные органы часто занимаются разрешением споров в тех ситуациях, когда стороны не могут заключить соглашение о присоединении, а также рассматривают жалобы потребителей.

К другим традиционным сферам регулирования относятся вопросы управления использованием спектра и радиовещания, хотя эти функции могут осуществлять и отдельные органы, не связанные с регуляторным органом ИКТ. Регулирование использования спектра исключительно важно с точки зрения обеспечения защиты от вредных помех и содействия эффективному использованию ресурсов спектра, в то время как регулирование радиовещания главным образом касается вопросов контента.

Изменение мандатов/функций регуляторных и директивных органов в цифровую эпоху

Ожидается, что в цифровой среде регуляторные органы во многом сохраняют свои традиционные сферы ответственности и институциональные модели. Однако практическое применение норм регулирования следует сделать менее строгим и более гибким. Кроме того, начиная с поколения G4 становится очевидным, что мандаты и функции регуляторных органов, возможно, потребуются скорректировать, чтобы привести их в полное соответствие с новыми цифровыми реалиями.

На фоне активного распространения цифровых услуг регуляторные органы сталкиваются с необходимостью решения множества новых вопросов и возможным возникновением новых сфер ответственности. Многие из них связаны с онлайн-услугами, такими как онлайн-передача голоса по протоколу Интернет (VoIP) или онлайн-видео, и с другими цифровыми платформами, а также с решением проблем IoT, ИИ, конфиденциальности данных, конкуренции, кибербезопасности и других проблем технологического характера.

Эти новые сферы ответственности далеко не всегда надлежащим образом отображаются в существующих нормативно-правовых базах. В настоящее время во многих странах обсуждается вопрос о том, обладают ли их регуляторные органы ИКТ и радиовещания юрисдикционными полномочиями для регулирования цифровых услуг, цифровых платформ и других появляющихся технологий. Во вставке 1.1 наглядно показано, что, когда страны начинают рассматривать вопрос об адаптации регулирования электросвязи или контента к цифровым услугам, определить границы полномочий регуляторного органа, не имея при этом четкой законодательной опоры, может оказаться непростой задачей.

Вставка 1.1. Споры о юрисдикции в отношении видеоконтента ОТТ в Индии

В Индии продолжается рассмотрение различными судебными инстанциями вопроса о том, распространяется ли на онлайн-видео действие Закона о кинематографе, а следовательно, регуляторные полномочия Министерства информации и телерадиовещания (MIB), в частности, в отношении требований к сертификации/лицензированию. В августе 2019 года Верховный суд штата Карнатака отклонил иск к нескольким поставщикам видеоконтента over-the-top (ОТТ), обосновав свое решение тем, что видео на основе технологии ОТТ не подпадает под действие Закона о кинематографе. Вместо принятия нормативно-правовой базы MIB заявило в марте 2020 года, что к середине 2020 года поставщикам видеоконтента ОТТ следует разработать кодекс поведения и создать орган, осуществляющий юрисдикцию (см. раздел "Модели саморегулирования").

Источник: Dutta 2020, Oka 2019.

Правительства по-разному подходят к предоставлению юрисдикционных полномочий регуляторным органам. Некоторые страны реформируют свою нормативно-правовую базу для приведения ее в четкое соответствие с новыми цифровыми услугами, как это сделал Европейский союз, приняв Европейский кодекс электронных средств связи (ЕЕСС) (см. раздел "Задачи поставщиков услуг: обеспечение соответствия требованиям регуляторных органов"). Есть и другой способ: изучить компетенции регуляторных органов, чтобы определить, что целесообразнее – расширить их мандат или создать новый цифровой регуляторный орган. Эти вопросы подробнее рассматриваются в разделе "Цифровые регуляторные органы".

Вне зависимости от того, принимает ли страна решение о расширении юрисдикционных полномочий регуляторного органа или о слиянии различных регуляторных органов, важно принять меры к тому, чтобы обеспечить регуляторный орган достаточными ресурсами для осуществления его функций. Сюда, в частности, относятся вопросы обеспечения кадрами – квалифицированными руководителями и подготовленными работниками. При слиянии существующих органов в объединенный регуляторный орган сотрудники, обладающие опытом в различных областях, например в сферах телерадиовещания и ИКТ, могут достаточно легко приступить к совместной работе. Без интеграции персонала невозможно создать сплоченную единую команду. При расширении мандата регуляторного органа крайне важно организовать профессиональную подготовку и наращивание потенциала, чтобы обеспечить понимание сотрудниками позиций различных заинтересованных сторон и соответствующей правовой и рыночной проблематики. Ключевую роль в формировании надежного, эффективного контингента сотрудников регуляторного органа играет проведение открытых консультаций и информационно-разъяснительной работы среди заинтересованных сторон, а также применение других механизмов совместного принятия решений на основании фактических данных. Если расширение мандата регуляторного органа не представляется целесообразным, можно использовать альтернативные способы повышения уровня знаний и увеличения объема ресурсов, применяя механизмы сотрудничества, способствующие налаживанию взаимодействия с другими ведомствами.

Совершенствование навыков сотрудников регуляторного органа, усиление его независимости и подотчетности

По данным МСЭ, по состоянию на конец 2018 года более чем в 80% стран регуляторные органы электросвязи и ИКТ не зависят от отраслевых министерств в вопросах финансирования, определения структуры и принятия решений⁵. На уровень автономии регуляторного органа могут существенно влиять его источники финансирования. Как правило, обладающий финансовой независимостью регуляторный орган получает прямое финансирование за счет установленных в законном порядке бюджетных ассигнований, что позволяет ему прозрачным образом формулировать свои потребности в бюджетных средствах. Помимо прямых бюджетных ассигнований, финансирование регуляторных органов может осуществляться за счет лицензионных и иных сборов. В частности, в тех случаях, когда лицензионные сборы являются единственным источником финансирования регуляторного органа, перед ним стоит задача установить надлежащие ставки, обеспечивающие возмещение расходов и достаточный уровень финансирования, но при этом не приводящие к взиманию неоправданно высокой платы за лицензирование. Существует

⁵ ITU, ICT-Eye: Key ICT Data and Statistics 2018. <https://www.itu.int/net4/itu-d/icteye/Topics.aspx?TopicID=12>

и третий механизм финансирования, предусматривающий направление государственных ассигнований министерству, в ведении которого находится регуляторный орган; оно, в свою очередь, предоставляет финансовые средства регуляторному органу. Однако применение этого механизма сопряжено с риском снижения независимости регуляторного органа, обусловленным вероятностью усиления политического влияния на процессы принятия регуляторных решений.

В традиционной, конвергентной и цифровой регуляторной среде независимый регуляторный орган является важнейшим компонентом обеспечения объективного, убедительно обоснованного и предсказуемого процесса принятия решений. В цифровую эпоху независимость регуляторного органа имеет особенно важное значение с точки зрения обеспечения условий для эффективного сотрудничества регуляторного органа с другими межотраслевыми учреждениями, а также для проведения открытых консультаций. Эти вопросы будут подробнее рассмотрены в разделе "Процессы принятия решений и установления правил в среде с участием многих заинтересованных сторон".

Наряду с независимостью регуляторные органы должны отчитываться о своей деятельности, сохраняя свободу от ненадлежащего политического или рыночного влияния. Одним из элементов подотчетности является опубликование всех законов, правил, руководящих указаний и других юридических документов – как проектов, так и окончательных текстов. В цифровой среде велика вероятность участия в этих процессах заинтересованных сторон из целого ряда отраслей, в силу чего публикация документов в интернете становится основным механизмом стимулирования всеобщего участия и совместного принятия решений.

Чтобы потенциал регуляторного органа как независимой и подотчетной структуры был реализован в полном объеме, его сотрудникам необходимы соответствующие навыки. Регуляторные органы должны учреждать механизмы своевременного информирования о развитии событий в отрасли как на национальном, так и на мировом уровне, чтобы иметь представление о финансовых, правовых, социальных и технических условиях, в которых они осуществляют свою деятельность. Кроме того, основой этих знаний должен быть опыт решения этих проблем, который будет служить не точной схемой, а примером решения новых задач. Затем они должны использовать эти знания на практике, применяя методы эффективного руководства. Как будет подробнее пояснено далее, такое эффективное руководство означает способность выбора пути, стимулирующего инновационную деятельность, и внедрение новых технологий в интересах потребителей на основании процессов принятия решений и установления правил в среде с участием многих заинтересованных сторон.

Надлежащая институциональная структура для цифровой среды

Некоторые правительства начали изучать вопрос о том, обладают ли их действующие регуляторные органы достаточными возможностями для решения вопросов, касающихся цифровой среды. Хотя обсуждение этого вопроса сейчас в основном находится на начальном этапе, анализ включает оценку целесообразности создания нового отдельного регуляторного органа, который будет заниматься исключительно цифровой проблематикой, либо расширения функций/мандата действующего регуляторного органа в области ИКТ и/или признания более удачной моделью сосуществование регуляторного органа ИКТ с другими органами государственной власти, отвечающими соответственно за защиту прав потребителей, защиту персональных данных и кибербезопасность. Как показано во вставке 1.2, примерами здесь могут служить Австралия, Ирландия и Соединенное Королевство. Эта тенденция может измениться в предстоящие годы по мере увеличения количества стран, приступающих к пересмотру мандатов действующих регуляторных органов с учетом цифровой трансформации.

Вставка 1.2. Обзор цифровых регуляторных органов в Австралии, Ирландии и Соединенном Королевстве

Австралия. В 2018 году Австралийская комиссия по вопросам конкуренции и прав потребителей (АССС) приступила к исследованию цифровых платформ, в рамках которого провела консультации по вопросам рыночного влияния цифровых платформ, в том числе социальных сетей, поисковых систем и других платформ с онлайн-контентом (АССС 2018). В обнародованном в июле 2019 года итоговом отчете АССС поставила перед собой задачу по решению проблем конкуренции в контексте деятельности цифровых платформ и наделила Управление по связи и средствам массовой информации Австралии (АСМА) рядом ключевых полномочий (АССС 2019).

Ирландия. В январе 2020 года правительство Ирландии представило в законодательный орган проект закона об обеспечении безопасности в онлайн-среде и регулировании средств массовой информации (DCCAE 2020). Одно из ключевых предложений, содержащихся в этом законопроекте, предусматривало замену существующего Управления телерадиовещания Ирландии (BAI) новой Комиссией по средствам массовой информации вместо создания нового регуляторного органа, который занимался бы регулированием цифрового контента. Комиссия по средствам массовой информации будет заниматься вопросами регулирования телерадиовещания, а также примет на себя дополнительные функции по регулированию отрасли аудиовизуальных средств массовой информации, включая онлайн-видео.

Соединенное Королевство. В апреле 2019 года Министерство цифровых технологий, культуры, средств массовой информации и спорта (DCMS) Соединенного Королевства начало консультации по вопросу о создании независимого регуляторного органа, которому были бы поручены разработка, контроль и обеспечение соблюдения предложенной новой нормативной модели решения проблем, связанных с распространением незаконного или вредного контента в онлайн-среде (DCMS 2019). В феврале 2020 года DCMS дало ответ на отклики, поступившие в ходе консультаций, в котором признало, что Ofcom, действующий регуляторный орган в области ИКТ, является единственным регуляторным органом, упоминаемым в качестве возможного кандидата для осуществления функций регуляторного органа по вопросам вредного воздействия в онлайн-среде. DCMS отметило, что расширение сферы ответственности регуляторного органа Ofcom вместо создания нового учреждения позволит Ofcom эффективно использовать накопленный опыт, избежать дробления регуляторного ландшафта и добиться быстрого прогресса в решении этих проблем (DCMS 2020).

Источник: АССС 2018; АССС 2019; Department of Communications, Climate Action and Environment (DCCAE), General Scheme Online Safety Media Regulation Bill 2019, <https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx>; DCMS 2019; DCMS, Online Harms White Paper: Initial Consultation Response, <https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response>.

Рассмотрение вопросов цифрового регулирования в Европейской комиссии (ЕК) также находится на начальном этапе. В своей Программе работы на 2020 год ЕК указала, что планирует опубликовать законопроект о цифровых услугах (DSA) в целях консультаций с общественностью в конце 2020 года (European Commission 2020). Законопроект предусматривает обновление Директивы Европейского союза (ЕС) об электронной торговле и, как ожидается, будет включать вопросы регулирования цифровых платформ. Согласно сообщениям средств массовой информации, опубликованным в августе 2019 года, ЕК по крайней мере изучила различные виды цифровых ведомств, призванных "обеспечить надзор и соблюдение норм": речь могла бы идти о "центральном регуляторном органе, децентрализованной системе или расширении полномочий действующих регуляторных органов" (Fanta 2019). Пока еще слишком рано судить о том, какую структуру этого органа ЕК предложит в DSA, однако внимание уже акцентируется на нескольких возможных вариантах.

Процессы принятия решений и установления правил в среде с участием многих заинтересованных сторон

Процесс принятия решений на основании фактических данных, анализ регуляторного воздействия, открытые консультации

Эффективные регуляторные органы обеспечивают взвешенность своих решений и их принятие максимально объективным образом в целях содействия регуляторной определенности и минимизации правовых проблем. Внушить заинтересованным сторонам доверие к регуляторным решениям способен целый ряд ключевых компонентов, включая процесс принятия решений на основании фактических данных, анализ регуляторного воздействия (АРВ), позволяющий оценить вероятное положительное и отрицательное воздействие предлагаемой нормы, публичные консультации и приверженность принципам прозрачности и недопущения дискриминации (OECD 2020). В основе всех этих методов лежат сбор и анализ данных – благодаря им регуляторные органы получают надежную высококачественную информацию от широкого круга заинтересованных сторон и, таким образом, могут подводить под свои решения надежное принципиальное обоснование. Напротив, решения, принятые наспех или после обсуждения за закрытыми дверями, могут подорвать доверие к регуляторному органу и произвести впечатление злоупотребления влиянием. На рисунке 1.3 представлены примеры эффективных процедур, действующих в Бразилии, Колумбии, Катаре и Сингапуре.

Рисунок 1.3. Примеры процессов принятия решений в Бразилии, Колумбии, Катаре и Сингапуре

Бразилия	Национальное агентство электросвязи (ANATEL) обязано проводить АРВ до принятия любых нормативных актов, за исключением ситуаций, в которых отсутствие необходимости проведения АРВ обосновано явным образом.
Колумбия	Комиссия по регулированию связи (CRC) обязана соблюдать конкретные процедуры принятия нормативно-правовых актов, предусматривающие публикацию проектов решений не менее чем за 30 дней до их принятия, чтобы общественность могла высказать свои замечания.
Катар	Регуляторный орган связи Катара (CRA) публикует материалы всех проводимых консультаций и заявляет, что его "решения должны основываться на фактических данных и учитывать мнения лиц и организаций, заинтересованных в результатах их принятия".
Сингапур	Управление по развитию информационно-коммуникационных технологий и средств массовой информации (IMDA) публикует материалы всех проводимых консультаций и регулярно привлекает заинтересованные стороны к участию в консультациях, с тем чтобы "обеспечить актуальность руководящих принципов, кодексов и стандартов и их соответствие общественным стандартам и социальным нормам".

Источник: National Agency of Telecommunications (ANATEL), Resolution 612/2013, <https://www.anatel.gov.br/legislacao/resolucoes/2013/450-resolucao-612>; Ministry of Information Technology and Communications (MINTIC), Decree 2696 of 2004, <https://www.mintic.gov.co/portal/inicio/14705:Decreto-2696-de-2004>; Communications Regulatory Authority (CRA), <https://www.cra.gov.qa/en/Regulatory-Framework/Public-Consultations>; Infocomm Media Development Authority (IMDA), <https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations>.

Особенно важно привлекать все заинтересованные стороны к участию в открытых консультациях при принятии норм регулирования цифровой сферы, поскольку в данном случае к затронутым сторонам относятся не только поставщики традиционных услуг электросвязи. В данной ситуации в число заинтересованных сторон входят потребители, цифровые платформы, коммерческие организации из других отраслей, таких как финансовый сектор, транспорт и здравоохранение, а также другие государственные ведомства с пересекающимися интересами и сферами компетенции.

Задачи регуляторного органа: управление внутренними процедурами и мониторинг

Одним из важных компонентов процесса принятия решений является определение порядка их реализации. Эффективные регуляторные органы обязаны управлять внутренними процедурами оценки соблюдения законодательства, что может быть осуществлено путем направления требований о представлении периодической отчетности или других запросов. Регуляторным органам следует также вести мониторинг

хода реализации принятых решений. Этот процесс включает мониторинг деятельности регулируемых структур с целью обеспечить соблюдение ими правовых норм, а также периодический обзор норм для оценки их эффективности и соответствия поставленным целям.

Проведение мониторинга может оказаться во многих странах непростой задачей, особенно в тех случаях, когда регуляторные органы сталкиваются с ограниченностью бюджета, штата сотрудников или иных необходимых ресурсов. Эти проблемы обостряются в цифровой среде, где требуется взаимодействовать со многими заинтересованными сторонами и вести мониторинг их деятельности. Таким образом, одним из важнейших условий эффективности регуляторного органа становится наращивание потенциала.

Задачи поставщиков услуг: обеспечение соответствия требованиям регуляторных органов

С точки зрения поставщиков услуг обеспечение соблюдения требований регуляторных органов может быть обременительным, особенно для новых участников рынка, не привыкших к строго регулируемым условиям деятельности в отрасли электросвязи. Эти проблемы усугубляются расширенными определениями услуг электросвязи. Например, в 2018 году ЕС провел серьезную модернизацию своей нормативно-правовой базы в области электросвязи, приняв Европейский кодекс электронных средств связи (ЕЕСС) (European Union 2018). Кодекс ЕЕСС содержит новое определение услуг электронной связи: к ним относятся все услуги голосовой связи, даже если при этом не используются телефонные номера общего пользования, а также услуги передачи данных для IoT, межмашинного взаимодействия, подключенных автомобилей и других видов цифровой деятельности, находящихся за пределами традиционной отрасли ИКТ (см. вставку 1.3). Государства – члены ЕС обязаны внести положения Кодекса ЕЕСС в национальное законодательство до конца 2020 года. Участники цифрового рынка должны будут самостоятельно определить, окажут ли (а если да, то каким образом) новые правила влияние на их деятельность.

Вставка 1.3. Расширенное определение услуг электронной связи в Кодексе ЕЕСС

Согласно определению, содержащемуся в статье 2 Кодекса ЕЕСС, под услугой электронной связи понимается "услуга, обычно предоставляемая за плату по сетям электронной связи, включающая в себя следующие виды услуг, за исключением услуг предоставления контента, передаваемого по сетям электронной связи или при помощи услуг электронной связи, и услуг осуществления редакторского контроля над этим контентом:

- a) услуги доступа в интернет;
- b) услуги межабонентской связи; и
- c) услуги, полностью или частично заключающиеся в транспортировке сигналов, такие как услуги передачи, используемые для предоставления услуг межмашинного взаимодействия или для осуществления радиовещания".

Услуги межабонентской связи (ICS), не предусматривающие использования телефонных номеров общего пользования, классифицируются как услуги межабонентской связи, не зависящие от использования телефонных номеров (NI-ICS). Хотя услуги NI-ICS подпадают под действие менее жесткого регулирования, чем услуги межабонентской связи на основе телефонных номеров (в частности, для предоставления услуг NI-ICS не требуется получение общего разрешения), многие поставщики онлайн-услуг VoIP сталкиваются с необходимостью выполнения незнакомых им прежде требований по обеспечению соблюдения регуляторных норм.

Источник: European Union 2018.

Нынешние и новые структуры, подлежащие регулированию, обязаны не только учитывать расширенное определение регулируемых услуг, но и соблюдать множество требований законодательства. Хотя сбор актуальной информации, такой как сведения о доходах, данные об абонентах и развертывании сетей, является важной функцией регуляторных органов с точки зрения понимания тенденций рынка, однако им следует отдавать себе отчет в том, что избыточные требования в отношении представления отчетности обременяют поставщиков услуг. Поэтому необходимо, чтобы требования о представлении отчетности носили упорядоченный характер и опирались на обоснованную, четко сформулированную потребность в информации. Кроме того, необходимо, чтобы обязательства по представлению отчетности и соблюдению

правовых норм отвечали поставленным целям и были ориентированы на соответствующие структуры. Например, в 2017 году Федеральная комиссия по связи США (ФКС) отменила обременительную обязанность по представлению ежегодной отчетности, в соответствии с которой поставщики международных услуг электросвязи были обязаны представлять данные о доходах и трафике (FCC 2017). ФКС десятилетиями использовала эти данные для мониторинга конкуренции среди международных операторов связи. ФКС заявила, что больше не видит необходимости в сборе этой информации у всех международных операторов связи, "поскольку расходы на сбор этих данных в настоящее время превышают получаемые в результате выгоды" (FCC 2017, 2). Вместо этого ФКС теперь пользуется данными, доступными на коммерческой основе, а при необходимости обращается с целевыми запросами о предоставлении данных к конкретным поставщикам услуг.

Новые заинтересованные стороны, действующие в цифровой регуляторной среде, также обязаны обеспечивать соблюдение нормативно-правовых требований потенциально в мировом масштабе. В отличие от поставщиков традиционных услуг электросвязи, создающих сети в тех странах, где они присутствуют на местах, участники цифрового рынка часто предоставляют свои услуги через интернет, позволяя получить доступ к своим услугам любому лицу, подключенному к интернету и находящемуся в любой точке планеты. Проблема заключается в том, что поставщики цифровых услуг могут подпадать под действие внутреннего законодательства, если страна сочтет, что для этого достаточно предоставлять онлайн-услуги находящимся в этой стране пользователям. В таких ситуациях новые участники рынка сталкиваются с дополнительными сложностями, лавируя между фрагментированными нормами регулирования в условиях принятия в различных юрисдикциях неодинаковых, а иногда и противоречащих друг другу норм. Это подчеркивает важное значение межправительственного взаимодействия и сотрудничества для обеспечения последовательности и предсказуемости норм для частного сектора.

Обеспечение соблюдения правовых норм и санкции в цифровой среде

Регуляторным органам следует подходить к обеспечению соблюдения правовых норм таким же образом, как и к процессу установления правил, то есть им следует действовать последовательно и объективно, четко указывая основания для принимаемых решений только после проведения тщательного изучения. Необходимо, чтобы все применяемые санкции были соразмерны нарушению, а сторонам, подпадающим под санкции, следует предоставлять доступ к своевременным процедурам пересмотра и апелляции, обеспечивающим и подотчетность регуляторных органов. Аналогичные принципы действуют и в отношении механизмов разрешения споров, надзор за которыми осуществляет регуляторный орган.

Важную роль в обеспечении соблюдения правовых норм играют директивные органы, даже если они не принимают непосредственного участия в наложении санкций. Из этого вытекает необходимость предоставить регуляторным органам достаточные правоприменительные полномочия, позволяющие им проводить необходимые расследования для выявления нарушений, а также полномочия по эффективному возмещению вызванного нарушениями ущерба. И у директивных, и у регуляторных органов может возникнуть необходимость уточнения процедур с другими регуляторными ведомствами, а иногда и судебными органами, если возникает пересечение полномочий различных отраслевых органов, в том числе органов, занимающихся вопросами защиты персональных данных, кибербезопасности, правоприменения, финансов, транспорта или конкуренции. Подобное межотраслевое сотрудничество, наглядно продемонстрированное во вставке 1.4, может предотвратить возникновение конфликта интересов в деятельности различных регуляторных органов.

Вставка 1.4. Нидерланды: межотраслевое сотрудничество в сфере обеспечения соблюдения правовых норм

Управление по вопросам потребителей и рынков (АСМ), регуляторный орган Нидерландов в области ИКТ, и Управление по обеспечению защиты данных (DPA) уже долгое время используют механизм сотрудничества в сфере обеспечения соблюдения норм, касающихся защиты персональных данных. Согласно Директиве ЕС о конфиденциальности и электронных средствах связи, АСМ занимается обеспечением соблюдения правил, касающихся файлов cookie. DPA отвечает за обеспечение соблюдения не относящихся к электронной связи положений Директивы о конфиденциальности и электронных средствах связи, а также закона о защите данных. Например, в 2017 году АСМ и DPA провели совместное расследование в отношении администратора веб-сайта по вопросам использования рекламных файлов cookie (DPA 2017). По итогам расследования к администратору веб-сайта не было применено никаких санкций, однако АСМ использовало свои правоприменительные полномочия, запретив администратору веб-сайта использовать файлы cookie без получения согласия пользователя. Поскольку администратор веб-сайта также обрабатывал данные, касающиеся политических предпочтений пользователей, DPA предписало ему проводить обработку этих данных только для рекламных целей и при наличии явно выраженного согласия пользователей.

Источник: DPA 2017.

1.4 Сотрудничество в сфере регулирования

Повсеместное распространение ИКТ во всех отраслях требует активизации сотрудничества в сфере регулирования между министерствами, отраслевыми и межотраслевыми регуляторными органами, а также целым рядом заинтересованных сторон в целях эффективного решения возникающих проблем и содействия дальнейшей цифровизации. Разработанная МСЭ концепция сотрудничества в сфере регулирования, опирающаяся на модель пяти поколений регулирования, предусматривает механизмы и целевые показатели развития сотрудничества в сфере регулирования на национальном, региональном и международном уровнях.

На Глобальном симпозиуме для регуляторных органов 2016 года (ГСР-16) МСЭ представил концепцию совместного регулирования, или регулирования G5, обрисовав в ней межотраслевой подход к регулированию, позволяющий заинтересованным сторонам создавать единое цифровое будущее (ITU 2016). Как было отмечено ранее, регулирование G5 предусматривает не ужесточение регулирования, а создание более интегрированного, основанного на фактических данных и ориентированного на принятие решений механизма регулирования с участием регуляторного органа ИКТ и других отраслевых учреждений.

Вставка 1.5. Определение сотрудничества в сфере регулирования в соответствии с концепцией G5

Под сотрудничеством в сфере регулирования понимается тесное взаимодействие регуляторного органа ИКТ с аналогичными регуляторными органами в других отраслях. Его определяющими характеристиками являются:

- 1) масштабы сотрудничества – сотрудничество между регуляторным органом ИКТ и органами, занимающимися вопросами конкуренции, защиты прав потребителей, финансирования, энергетики, радиовещания, управления использованием спектра и использования интернета;
- 2) уровень сотрудничества – наличие неофициального сотрудничества, официального сотрудничества или иных гибридных механизмов сотрудничества с участием регуляторных органов.

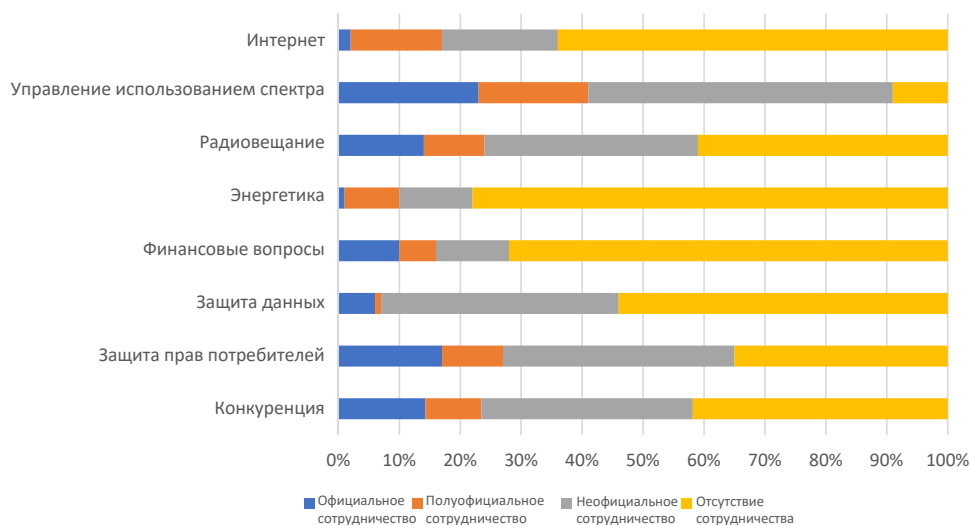
Источник: ITU 2018a, 129.

В соответствии с этим определением правительствам следует стремиться к налаживанию действенного и устойчивого сотрудничества в сфере регулирования между регуляторными органами ИКТ и другими регуляторными органами.

Официальное и неофициальное сотрудничество между правительствами

Государственные органы могут осуществлять совместную деятельность с использованием разнообразных механизмов неофициального, полуофициального и официального сотрудничества. Неофициальное сотрудничество возникает на основании контактов между регуляторными органами, обусловленных вопросами, представляющими взаимный интерес, и вопросами наращивания потенциала, а не на основе институционально оформленной модели плановых контактов. Напротив, официальное сотрудничество "...предполагает систематические усилия по развитию сотрудничества и определению условий взаимодействия...", например, на основе меморандумов о взаимопонимании или законодательных актов (ITU 2018a). Полуофициальное сотрудничество включает в себя компоненты как официального, так и неофициального сотрудничества и зачастую является одним из этапов перехода от неофициальной структуры к официальной. На рисунке 1.4 представлен обзор состояния сотрудничества в сфере регулирования между регуляторными органами ИКТ и ведомствами, занимающимися иными вопросами, в различных странах мира. Далее представлено более подробное описание характера их взаимоотношений. Эти данные основаны на информации, представленной самими ведомствами в рамках Обследования МСЭ по вопросам регулирования в области всемирной электросвязи/ИКТ за 2017 и 2018 годы (ITU 2018b).

Рисунок 1.4. Состояние сотрудничества в сфере регулирования между регуляторными органами ИКТ и другими ведомствами при условии наличия этих органов и ведомств и их функционирования в качестве отдельных структур, весь мир, 2018 год



Источник: ITU 2018a, 130–150.

Примечание. – Размеры выборки стран по строкам сверху вниз: 48, 22, 92, 116, 172, 72, 101, 92.

Конкуренция

Ведомства, занимающиеся вопросами конкуренции, и регуляторные органы ИКТ нередко опираются на устоявшийся порядок взаимодействия для решения вопросов в частично совпадающих сферах компетенции, в особенности вопросов слияния или доминирования на рынках в отрасли электросвязи и ИКТ. Официальное сотрудничество уже стало нормой для многих регуляторных органов, в том числе в Намибии, Сербии и Соединенном Королевстве⁶. В ряде стран, в том числе в Ирландии, Румынии и Саудовской Аравии, ведомства, занимающиеся вопросами конкуренции, и регуляторные органы в сфере ИКТ осуществляют совместные программы или взаимодействуют в рамках совместных комитетов⁷.

Защита прав потребителей

Как правило, органы защиты прав потребителей не ограничиваются в своей деятельности какой-либо отдельной отраслью и при выполнении своих функций в значительной степени полагаются на сотрудничество с другими регуляторными органами в конкретной отрасли и/или на поддержку этих органов. Почву для сотрудничества между регуляторными органами ИКТ и органами защиты прав потребителей подготовили тенденции в области конфиденциальности и защиты данных, сетевого нейтралитета и использования потребителями услуг ИКТ. По состоянию на 2018 год две трети действующих регуляторных органов в сферах ИКТ и защиты прав потребителей поддерживают сотрудничество в том или ином виде, причем половина из них – в рамках неофициальных механизмов⁸. В Хорватии, Доминиканской Республике, Арабской Республике Египет, Иране и Молдове сотрудничество носит неофициальный характер, тогда как в Армении, на Ямайке, в Норвегии и Таиланде существуют официальные механизмы сотрудничества⁹.

⁶ Действующие на сегодняшний день в Соединенном Королевстве механизмы взаимодействия были созданы на основании Закона о предпринимательстве и реформе регулирования 2013 года и вступили в силу 1 апреля 2014 года. Данные соглашения послужили основой для создания нормативно-правовой базы, благодаря которой Управление по вопросам конкуренции и рынков (СМА) и отраслевые регуляторные органы могут вместе принимать более эффективные меры, направленные на совершенствование конкуренции и обеспечение соблюдения антимонопольного законодательства в регулируемых отраслях.

⁷ Эти вопросы подробнее рассматриваются в главе 2 "Конкуренция и экономика" и в главе 8 "Техническое регулирование".

⁸ ITU, ICT Regulatory Tracker 2018. <https://www.itu.int/net4/itu-d/irt/#/generations-of-regulation>

⁹ Эти вопросы подробнее рассматриваются в главе 4 "Вопросы, касающиеся потребителей".

Защита данных

В основе процессов цифровизации лежат потоки данных. Создание возможностей для сбора и обработки информации, используемой в коммерческих, государственных, медицинских или иных институциональных целях, является неотъемлемым условием развития цифровой экономики, но при этом необходимо обеспечить защиту прав потребителей на неприкосновенность частной жизни. С учетом роли данных во всех аспектах цифровой экономики сотрудничество между органами защиты данных и другими регуляторными органами, действующими в конкретных областях/отраслях, жизненно необходимо для создания должным образом унифицированной системы цифрового регулирования с надлежащим охватом. В странах мира разработаны разнообразные нормативно-правовые системы защиты данных, причем тенденцию на международном уровне задает модель ЕС, основанная на Общем регламенте по защите данных (GDPR) (European Union 2016). Согласно Регламенту GDPR, вступившему в силу в мае 2018 года, устанавливает правила и обеспечивает их выполнение самостоятельный орган защиты данных (DPA). Как правило, DPA обладает четко сформулированным мандатом, не допускающим существенного совпадения юрисдикций с регуляторным органом ИКТ. Некоторые регуляторные органы ИКТ и DPA могут поддерживать сотрудничество, однако большинство этих органов не имеет действующих официальных механизмов сотрудничества, как видно из рисунка 1.3. Осуществляемое на практике сотрудничество, как правило, является неофициальным. Во многих юрисдикциях независимые DPA появились сравнительно недавно, поэтому в будущем можно ожидать дальнейшего развития сотрудничества в этой сфере¹⁰.

Иные отрасли

Важное значение имеет и сотрудничество между регуляторными органами ИКТ и другими отраслевыми регуляторными органами. ИКТ способствуют ускорению темпов внедрения инноваций, преобразующих деятельность всех отраслей и рынков и изменяющих их облик. Правительствам следует тщательно проанализировать значение ИКТ в каждой отрасли и определить необходимый уровень сотрудничества между регуляторными органами. В таблице 1.1 перечислены некоторые вопросы, которые регуляторным органам ИКТ следует рассматривать в сотрудничестве с другими регуляторными органами¹¹.

Таблица 1.1. Примеры областей сотрудничества регуляторных органов ИКТ и других ведомств

Регуляторные органы отраслей, не относящихся к ИКТ	Области потенциального сотрудничества с регуляторными органами ИКТ
Коммерция/торговля	Цифровое налогообложение, онлайн-услуги
Кибербезопасность	Использование данных, устройства конечного пользователя, IoT
Образование	Защита детей в онлайн-среде, цифровой разрыв
Энергетика	ИИ, технология блокчейн, IoT
Финансы	Технология блокчейн, кибербезопасность, охват финансовыми услугами, мобильные финансовые услуги, обеспечение конфиденциальности
Транспорт	Кибербезопасность, IoT, обеспечение конфиденциальности

Источник: TMG 2020.

Как показано во вставке 1.6, в последнее время в Сингапуре активизировалось сотрудничество регуляторного органа ИКТ и учреждения по защите данных в целях повышения эффективности взаимодействия в области развития ИИ.

¹⁰ Дополнительные сведения см. в главе 5 "Защита данных и доверие".

¹¹ Эти вопросы подробнее рассматриваются в главе 7 "Реагирование регуляторных органов на развитие технологий".

Вставка 1.6. Правительство Сингапура развивает сотрудничество в сфере искусственного интеллекта

В январе 2019 года Комиссия по защите персональных данных (PDPC) и Управление по развитию информационно-коммуникационных технологий и средств массовой информации (IMDA) совместно опубликовали первое издание *Рамочной модели управления искусственным интеллектом* в качестве основы для обсуждения задач и возможных решений в сфере ответственного использования потенциала ИИ. Цель этой рамочной модели состоит в определении комплекса принципов, их распределении по ключевым темам и их использовании в качестве основы для создания понятной и применимой на практике структуры. В ней изложены руководящие указания в отношении мер, побуждающих организации к ответственному применению ИИ в следующих четырех ключевых областях: структуры и меры внутреннего управления, определение модели принятия решений в области ИИ, управление операционной деятельностью и управление взаимоотношениями с клиентами.

Источник: TMG 2020.

Модели саморегулирования

Модель саморегулирования позволяет государству передать немалую часть своих регуляторных полномочий участникам рынка, на которых регулирование влияет сильнее всего. Толчком к появлению подобных моделей часто служит "ультиматум" государства: либо отрасль надлежащим образом осуществляет самостоятельное регулирование, либо государство берет процессы регулирования на себя. Например, в Индии Министерство информации и телерадиовещания поддерживает использование модели саморегулирования в отношении онлайн-услуг передачи потокового видеоконтента. В связи с этим некоторые члены Ассоциации интернета и подвижной связи Индии (IAMAI) разрабатывают Добровольный кодекс поведения, за соблюдением которого будет следить Совет по рассмотрению жалоб в отношении цифрового контента – он станет судебным органом, рассматривающим вопросы использования цифрового контента.

Сотрудничество компаний отрасли и государства

Сотрудничество между компаниями отрасли и регуляторным органом представляет собой переходное звено между саморегулированием и традиционным полноценным регулированием и дает государству определенный контроль над отраслью при сохранении ее автономии. В частности, значение сотрудничества между компаниями отрасли и регуляторным органом еще нагляднее проявилось в условиях пандемии COVID-19. Чтобы обеспечить стабильную работу сетей в условиях, когда беспрецедентное число людей были вынуждены работать, учиться и находиться в самоизоляции в своих домах, государства стремились повысить гибкость своих систем регулирования и полагались на меры, принимавшиеся при ведущей роли отрасли. Например, 19 марта 2020 года ЕК и Совет европейских регуляторных органов в области электронной связи (BEREC) опубликовали совместное заявление о путях удовлетворения возросшего спроса на сети широкополосной связи в результате пандемии COVID-19. BEREC и ЕК заявили, что поставщики услуг интернета уполномочены принимать все необходимые меры для снижения перегрузки сетей, и это заявление стало свидетельством перехода к применению регуляторного подхода, основанного на более широком сотрудничестве (BEREC 2020, European Commission 2020). Одновременно с этими мерами поставщики цифровых услуг, такие как Netflix, Facebook, Microsoft и Google, предприняли шаги по сужению полос пропускания, необходимых для оказания их услуг, действуя как по собственной инициативе, так и по запросу регуляторных органов. Следует также обратить внимание на то, что МСЭ начал сбор информации о других примерах подобных действий и способствовал проведению совместных обсуждений в рамках своей инициативы Reg4Covid¹².

¹² ITU, Reg4Covid (по состоянию на 13 мая 2020 года). <https://reg4covid.itu.int/>

1.5 Создание рамочных основ цифрового регулирования

Процессы расширения цифровых услуг способны повлиять на принципы определения и регулирования услуг электросвязи. Комплекс подлежащих регулированию видов деятельности может быть расширен за счет внесения поправок, предусматривающих включение новых цифровых услуг в определение средств электросвязи. Например, одним из предметов политической дискуссии во всем мире стал вопрос о том, подлежат ли регулированию различные типы услуг VoIP, и если подлежат, то каким образом следует осуществлять это регулирование. Хотя правительства могут склониться к использованию мягкого регуляторного подхода, изменения в перечне подлежащих регулированию услуг и видов регулирования оказывают более широкое воздействие на обязательства в сфере лицензирования, конкуренции и соблюдения других регуляторных норм¹³.

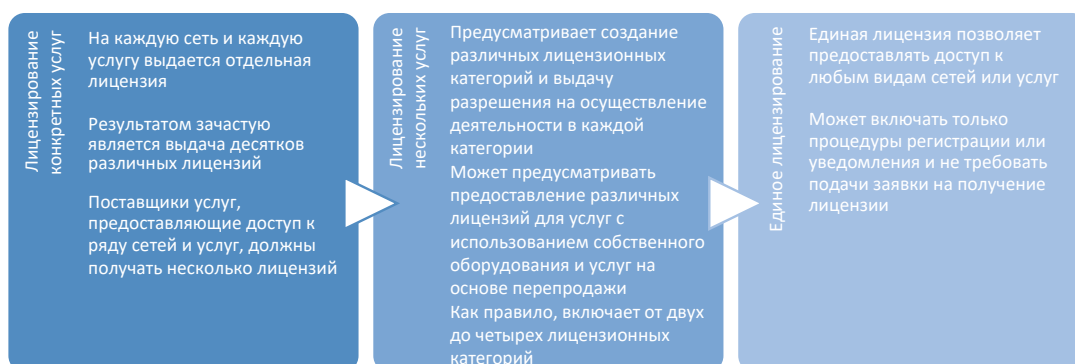
Системы лицензирования сетей, услуг и приложений

Системы лицензирования и подходы к лицензированию являются ключевыми факторами, определяющими простоту или сложность выхода на рынок в данной стране. Как правило, решения о выборе режимов лицензирования и подходов к лицензированию принимаются на высоком политическом уровне и закрепляются в законодательстве в области электросвязи, а затем осуществляются на основании правил и норм регулирования.

Лицензирование сетей/услуг

Выбранная страной система лицензирования способна оказать непосредственное воздействие на развитие отрасли. Система лицензирования конкретных услуг может привести к возникновению ограничений, препятствующих выходу на рынок, поскольку в данном случае обладатель лицензии обязан получать новую лицензию каждый раз, когда он хочет добавить новую позицию к предлагаемым им сетям или услугам. Хотя системы лицензирования конкретных услуг по-прежнему используются по всему миру, примером применения международного передового опыта стали появляющиеся системы лицензирования нескольких услуг и единые системы лицензирования, поскольку они позволяют эффективнее упорядочить процедуры лицензирования, способствуют технологической конвергенции и развитию конкуренции. Основные особенности этих систем лицензирования показаны на рисунке 1.5.

Рисунок 1.5. Три основных вида систем лицензирования



Источник: TMG.

Например, в период между 2013 и 2015 годами Мьянма провела реформу отрасли электросвязи, осуществив переход от использования режима лицензирования конкретных услуг к режиму лицензирования нескольких услуг, предусматривающему наличие трех основных лицензионных категорий, которые различаются между собой в зависимости от того, предоставляется ли услуга с использованием собственного оборудования (Seint Seint Aye 2015). Следствием этих реформ стал бурный рост цифровых услуг в Мьянме: в стране резко возросли показатели проникновения подвижной связи – с 13% в 2014 году до 124% в 2019 году (Liu 2019).

¹³ Эти вопросы подробнее рассматриваются в главе 2 "Конкуренция и экономика" и в главе 7 "Реагирование регуляторных органов на развитие технологий".

Эти системы лицензирования ориентированы скорее на среду электросвязи, чем на цифровую среду. Как отмечается в разделе "Изменение мандатов/функций регуляторных и директивных органов в цифровую эпоху", ответ на вопрос о том, подпадают ли цифровые услуги под действие лицензионных схем, зависит от характерных особенностей этих услуг, а также от того, находится ли вообще регулирование цифровых услуг в ведении регуляторного органа ИКТ.

Лицензирование спектра

Существует множество различных способов выдачи разрешений на использование спектра, в том числе индивидуальное лицензирование спектра по принципу "первым пришел – первым обслужен"; предоставление административной лицензии; использование конкурентного механизма, например, проведение аукционов или конкурсов; предоставление лицензии на класс или комплексных лицензий, разрешающих использование большого количества устройств (например, терминалов спутниковой широкополосной связи или спутниковых телевизионных антенн); или выделение определенных полос частот, предусматривающих освобождение от лицензии или применение безлицензионного режима. Например, в июне 2019 года Европейская конференция администраций почт и электросвязи (СЕПТ) рекомендовала европейским регуляторным органам разрешить безлицензионное использование диапазона 60 ГГц для услуг 5G на определенных технических условиях¹⁴ (СЕПТ 2019).

В целом директивные органы используют процедуры конкурсного отбора для выдачи разрешений на использование спектра в тех случаях, когда спрос на него превышает предложение. Например, разрешения на использование спектра подвижной связи, как правило, выдаются на основании аукциона или конкурса ввиду высокого спроса на данный спектр и его высокой значимости. Принимая во внимание широкие возможности технологий 5G, страны во всем мире, в том числе Германия, Япония, Сингапур и Республика Корея, выдают разрешения на использование больших объемов спектра для 5G¹⁵ (MIC 2019; IMDA 2020; MSIT 2018).

Альтернативные подходы к лицензированию

Воздействие на условия выхода на рынок, конкуренцию и доступность сетей и услуг оказывают не только системы лицензирования, но и подходы к лицензированию и регулированию. Необходимо, чтобы выбранный подход опирался на анализ международного передового опыта и соответствовал потребностям в сфере регулирования, но не предусматривал обременительных требований, создающих необоснованные препятствия для выхода на рынок. Даже при использовании систем единого лицензирования со сжатыми сроками рассмотрения заявок (до одной недели) новые участники рынка могут потратить большое количество ресурсов – времени и денег – только для подготовки форм заявок из-за избыточных требований к предоставлению информации.

В некоторых случаях возможно использование более жестких подходов, направленных на достижение конкретных целей государственной политики, например, включение в лицензии на подвижную связь обязательств по обеспечению покрытия. Тем не менее в целом предпочтение отдается мягким подходам, способствующим более активному развитию отрасли и предусматривающим применение целенаправленных и обоснованных мер регуляторного вмешательства. Таким образом, основная задача заключается в применении наименее жестких регуляторных мер, обеспечивающих достижение политических целей. На рисунке 1.6 представлены несколько подходов к использованию систем лицензирования и механизмов лицензирования и к обеспечению выхода на рынок, расположенных по степени возрастания жесткости требований.

¹⁴ В главе 6 "Управление использованием спектра" рассматриваются различные механизмы выдачи разрешений на использование спектра, а также преимущества и недостатки каждого подхода.

¹⁵ Bundesnetzagentur (BNetzA). Frequenzauktion 2019. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html?nn=267664; Infocomm Media Development Authority (IMDA), Close of 5G Call for Proposal. <https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/Close-of-5G-Call-for-Proposal>

Рисунок 1.6. Подходы к лицензированию: от менее жестких к более жестким

Подход	Менее жесткий	Более жесткий
Система лицензирования электросвязи	- Общий режим выдачи лицензий - Уведомительный принцип, без подачи или рассмотрения предварительной заявки	- Подробные бизнес-планы/технические планы - Необходимо повторно проходить процедуру получения лицензии для каждой новой сети или услуги
Механизм лицензирования	- Подача заявки в любое время - Подача заявки в электронной форме - Принцип "первым пришел – первым обслужен" - Нет ограничений на количество лицензий	- Обязательное проведение открытых консультаций - Заявки подаются в бумажной форме - Количество лицензий ограничено - Требуется несколько уровней разрешений
Выход на рынок	- Нет ограничений на иностранное владение - Размер лицензионных платежей зависит от административных расходов	- Ограничения на иностранное владение - Высокие лицензионные платежи

Инновационные подходы к регулированию отрасли

Простое применение существующего – и потенциально устаревшего – регулирования к новым технологиям и услугам способно затормозить внедрение инноваций. Стремясь идти в ногу с развитием технологий, директивные органы изучают различные меры, позволяющие разработать четкие, гибкие и объективно применяемые правила, не препятствующие прогрессу. Эти модели цифрового регулирования включают инновационные подходы к использованию спектра, лицензированию новых технологий и обеспечению универсального доступа.

Инновационные правила использования спектра

Появление новых беспроводных технологий, соседствующих с существующими услугами, способствует непрерывному повышению спроса на спектр, в том числе для коммерческой связи 5G, спутниковых услуг и услуг фиксированной беспроводной связи, а также расширению потребности в спектре для использования государственными органами. Сейчас как никогда прежде возникает острая необходимость разработки правил, обеспечивающих эффективное использование дефицитных ресурсов спектра. В таблице 1.2 представлено краткое описание некоторых креативных подходов к использованию спектра, в том числе совместное использование спектра, использование нелицензируемого спектра и предоставление лицензий на использование спектра для применения IoT в частных целях¹⁶.

¹⁶ Эти и другие вопросы использования спектра подробнее рассматриваются в главе 7 "Реагирование регуляторных органов на развитие технологий" и в главе 6 "Управление использованием спектра".

Таблица 1.2. Креативные подходы к разработке правил использования спектра

Правила использования спектра	Описание	Выгодные стороны	Проблемы
Совместное использование спектра	Несколько пользователей, применяющих различные приложения/технологии, совместно используют одну и ту же полосу частот	Целый ряд пользователей получают возможности для более эффективного использования спектра	Необходим определенный уровень управления для устранения возможных помех
Использование нелицензируемого спектра	Отсутствие ограничений на число пользователей, использующих освобожденную от лицензирования полосу частот	Обеспечение легкого доступа к спектру для использования в новых и разнообразных целях	Отсутствие управления использованием спектра повышает возможность возникновения помех
Применение IoT в частных целях	Обеспечение использования локальных сетей для деятельности в конкретных отраслях, например в горнодобывающей промышленности, портовом хозяйстве или здравоохранении	Создание условий для применения IoT в целом ряде отраслей при относительно низком риске возникновения помех, обусловленном локализованным использованием	Возможное ограничение доступного спектра 5G для использования в более широких коммерческих целях

Источник: Sayed 2019, Bedi 2018, LVM 2020.

Использование креативных подходов к лицензированию, стимулирующих активное распространение появляющихся технологий

Правительства стремятся к созданию новых моделей лицензирования, с тем чтобы побудить участников рынка, в том числе не принадлежащих к числу операторов традиционной электросвязи, тестировать и развивать технологии. Эти модели предусматривают, в частности, использование экспериментального режима регулирования (регуляторной "песочницы") и упорядочение выдачи демонстрационных или пробных лицензий. Регуляторная "песочница", пришедшая в отрасль электросвязи из сферы финансовых технологий, используется для тестирования технологий и бизнес-моделей на протяжении определенного периода времени. Экспериментальные лицензии, как правило, не подпадают под действие полноценного регуляторного режима, однако, регуляторный орган может представлять в отношении этих лицензий больше руководящих указаний, чем в отношении стандартных лицензий. Этот гибкий подход можно также использовать в условиях кризиса в качестве временной меры для экспериментального применения инновационных решений, обеспечивающих возможность установления соединений. Регуляторные органы могут также снизить или отменить плату для дополнительного поощрения участников рынка. Как показано на рисунке 1.7, к числу стран, использующих подобный подход, относятся, в частности, Франция и Таиланд.

Рисунок 1.7. Элементы модели регуляторной "песочницы" во Франции и Таиланде

Элементы регуляторной "песочницы"	Франция	Таиланд
Обеспечение соблюдения регуляторных норм	Полное или частичное освобождение от соблюдения регуляторных норм (определяется на индивидуальной основе)	Соблюдение регуляторных норм в сокращенном объеме, запрет на взимание платы или подключение к сетям
Сроки	Экспериментальная лицензия действительна на срок до двух лет	Экспериментальная лицензия действительна на срок до двух лет
Руководящие указания регуляторного органа	Регуляторный орган оказывает содействие в осуществлении административных процедур до момента получения полноценной лицензии	Обладатели лицензий должны каждые три месяца представлять регуляторному органу отчеты о достигнутых результатах
Примеры	Аэрокосмическая компания, проводящая испытание средств связи на борту воздушных судов	Предприятие коммунального хозяйства, проводящее испытание микросети для оказания услуг электро- и водоснабжения

Источник: Regulatory Authority for Electronic Communications and Posts (ARCEP). Bac à sable réglementaire (Regulatory Sandbox), <https://www.arcep.fr/professionnels/startups-entrepreneurs/bac-a-sable-reglementaire.html>; NBTC 2019.

Креативные механизмы обеспечения универсального доступа

В целях обеспечения доступа к цифровым технологиям и услугам правительства продолжают использовать традиционные программы универсального обслуживания, опирающиеся на фонды универсального доступа и обслуживания (ФУДО) и другие механизмы финансирования. Тем не менее многие страны сталкиваются с затруднениями, касающимися предоставления отчетности или осуществления надзора за деятельностью ФУДО, что вынуждает их отдавать предпочтение другим механизмам финансирования, таким как заключение соглашений по принципу "плати или играй" или использование "умных" субсидий.

Таким образом, страны могут использовать рыночные решения, такие как взносы в натуральной форме, в качестве дополнения к традиционным инициативам на основе ФУДО или в качестве замены этих инициатив в целях содействия росту спроса и снижению расходов операторов. Например, победившие участники аукциона 5G, состоявшегося в Германии в 2019 году, обязаны соблюдать масштабные обязательства по обеспечению покрытия, в том числе обязательство по установке 500 базовых станций в необслуживаемых сельских районах, называемых "белыми пятнами" (BNetzA 2019). Обладатели лицензий обязаны разместить базовые станции в районах "белых пятен" до конца 2022 года.

В целях обеспечения доступа в период кризиса, вызванного COVID-19, некоторые страны на временной основе осуществляли присвоение спектра операторам востребованных услуг подвижной связи. Например, в апреле 2020 года Независимое управление связи Южной Африки (ICASA) объявило о временном присвоении спектра в диапазоне 700 МГц, 800 МГц, 2600 МГц и 3500 МГц действующим операторам сетей подвижной связи (MNO) "до тех пор, пока в стране действует чрезвычайное положение, в целях снижения нагрузки на сеть, сохранения высокого качества услуг широкополосной связи и предоставления обладателям лицензий возможности снизить стоимость доступа к своим услугам для потребителей"¹⁷.

В главе 3 "Доступ для всех" изложены подробные сведения о механизмах универсального доступа и обслуживания (УДО), а также представлен анализ тенденций и передового опыта в области обеспечения соединения для тех, кто его не имеет.

¹⁷ Independent Communications Authority of South Africa (ICASA), Emergency Release of Spectrum to Meet the Spike in Broadband Services Demand due to COVID-19. <https://www.icasa.org.za/news/2020/emergency-release-of-spectrum-to-meet-the-spike-in-broadband-services-demand-due-to-covid-19>

1.6 Основные выводы

Разработка национальных цифровых стратегий и дорожных карт

- Осуществляемые во многих странах национальные меры политики в области ИКТ и цифровые стратегии являются ключевыми механизмами определения задач и целей в области возможности установления соединений и свидетельствуют о большом значении цифровой среды для всех сфер экономической и социальной жизни страны. Кроме того, они играют важную роль в распространении информации о совместном регулировании и привлечении многих заинтересованных сторон, тем самым способствуя принятию комплексного подхода к цифровому развитию и планированию.

Институциональная структура и функции регуляторного органа

- Регуляторному органу ИКТ, вне зависимости от институциональной структуры, необходима надлежащая независимость в части финансирования, повседневного функционирования и принятия решений, однако нормы, регламентирующие его деятельность, должны признавать, что он играет определенную роль – иногда главную, иногда второстепенную – в сотрудничестве по разработке надлежащей нормативно-правовой базы для цифровой среды, и стимулировать это сотрудничество.
- С учетом влияния ИКТ на различные отрасли и широкого круга проблем, обусловленных возникновением цифровой экономики, развитие цифровой среды определяется моделью совместной и взаимозависимой деятельности регуляторного органа, других соответствующих органов власти, компаний отрасли и других ключевых заинтересованных сторон.
- Правительствам необходимо создать официальные и неофициальные механизмы сотрудничества с компаниями отрасли и объединениями потребителей в целях выработки политики, правил и руководящих указаний. Многие разворачиваемые технологии и инновационные решения пока находятся в зачаточном состоянии и нуждаются в смягченной регуляторной среде, позволяющей проводить эффективную оценку надлежащих средств для развития инноваций, обеспечивая при этом защиту потребителей от ущерба.
- Прежде чем принимать меры, имеющие обязательную силу, регуляторным органам следует по мере возможности побуждать компании отрасли к разработке своих собственных руководящих указаний и кодексов поведения, так как участники отрасли зачастую располагают большими возможностями для решения динамично изменяющихся и новых проблем.
- Директивным и регуляторным органам следует расценивать формирование цифровой среды в качестве возможности для переоценки существующих, потенциально устаревших законов и регуляторных норм и принять меры – возможно, включая отмену регулирования, саморегулирование или совместный подход к регулированию, – которые будут способствовать расширению масштабов инноваций, упрощению внедрения новых и появляющихся технологий, стимулированию инвестиций и приоритетной ориентации на интеграцию и сотрудничество.
- Регулирование G5, или совместное регулирование, является ключевым компонентом процесса разработки инклюзивной политики в цифровой среде, но при этом регуляторный орган ИКТ должен сохранить в сфере своего основного ведения ряд основополагающих инструментов регулирования, включая разработку регуляторных норм, направленных на обеспечение возможности установления соединений, развитие инфраструктуры и поддержку конкурентоспособности отрасли.
- Регуляторным органам следует сохранять практику принятия решений на основании фактических данных после проведения публичных консультаций. Широкие консультации являются неотъемлемой частью цифрового регулирования, охватывающего различные заинтересованные стороны, в том числе из отраслей, не принадлежащих к числу традиционных участников рынка электросвязи.
- Важно наладить практическую реализацию регуляторных норм и мониторинг их соблюдения, чтобы убедиться как в том, что подлежащие регулированию структуры соблюдают правила, так и в том, что сами правила обеспечивают достижение поставленных целей. Следует тщательно рассмотреть возможность распространения действия правил на цифровые услуги, в том числе учитывая потенциальные последствия применения фрагментированной системы регулирования.

- Следует проводить систематическое и объективное изучение процесса соблюдения регуляторных норм, прежде чем налагать санкции, а также обеспечить соразмерность средств правовой защиты совершенному нарушению. Сотрудничество с другими отраслевыми ведомствами полезно для достижения согласованных результатов.

Формирование систем цифрового регулирования

- Следует разработать как можно более рациональные системы лицензирования сетей и услуг, уделяя особое внимание обеспечению беспрепятственного выхода на рынок с опорой на передовой опыт использования систем единого лицензирования или лицензирования нескольких услуг. В области использования ресурсов спектра существует несколько механизмов выдачи разрешений, каждый из которых удовлетворяет различные потребности в области политики.
- Вне зависимости от используемой системы лицензирования регуляторным органам следует применять подходы к лицензированию, позволяющие достигать целей в области регулирования, не предъявляя при этом обременительных требований, препятствующих выходу на рынок и развитию рынка. В целом следует отдавать предпочтение мягкому подходу к регулированию, особенно когда речь идет о цифровом регулировании, охватывающем в настоящее время широкий круг участников рынка.
- Развитию появляющихся технологий и услуг могут способствовать инновационные подходы к регулированию, такие как совместное использование спектра, создание регуляторных песочниц или использование механизмов, альтернативных механизмам ФУДО, для обеспечения универсального обслуживания. Регуляторные органы обладают необходимыми возможностями для принятия четко сформулированных, гибких и объективно применяемых правил в целях стимулирования инноваций.

Справочные материалы

- ACCC (Australian Competition and Consumer Commission). 2018. *Digital Platforms Inquiry: Issues Paper*. Canberra: ACCC. <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry/issues-paper>
- AGESIC (Electronic Government and Information and Knowledge Society Agency). 2017. *Digital Agenda 2020*. Montevideo: AEGSIC. https://uruguaydigital.uy/wps/wcm/connect/urudigital/44f1500c-6415-4e21-aa33-1e5210527d94/Download+Digital+Agenda+%28English+Version%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=44f1500c-6415-4e21-aa33-1e5210527d94
- ANATEL (National Agency of Telecommunications). 2013. *Resolution 612/2013*. Brazil: ANATEL. <https://www.anatel.gov.br/legislacao/resolucoes/2013/450-resolucao-612>
- Angus, Garfield. 2014. "Laws Far Advanced to Modernize ICT Sector". Jamaica Social Investment Fund. June 11. <https://jis.gov.jm/laws-far-advanced-modernize-ict-sector/>
- Bedi, Iqbal. 2018. *Setting the Scene for 5G: Opportunities and Challenges*. Discussion Paper. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2018/documents/DiscussionPaper_Setting%20the%20scene%20for%205G_GSR18.pdf
- BEREC (Body of European Regulatory for Electronic Communications), European Commission. 2020. *Joint Statement from the Commission and the Body of European Regulators for Electronic Communications (BEREC) on coping with the increased demand for network connectivity due to the Covid-19 pandemic*. March 19. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9236-joint-statement-from-the-commission-and-_0.pdf (по состоянию на 16 апреля 2020 года).
- Botswana Government. 2012. *Communications Regulatory Authority Act 2012*. <https://www.bocra.org.bw/sites/default/files/documents/COMMUNICATIONS%20REGULATORY%20ACT%2C%202012.pdf>
- Broadband Commission for Sustainable Development. 2019. *State of Broadband Report 2019*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf
- CEPT (European Conference of Postal and Telecommunications Administrations). 2019. *ERC Recommendation 70-03 Relating to the Use of Short-Range Devices (SRD)*. Copenhagen: CEPT. [https://cept.org/DocumentRevisions/srd/mg---short-range-devices/11630/SRDMG\(17\)153_Rec%2070-03%20October%202017](https://cept.org/DocumentRevisions/srd/mg---short-range-devices/11630/SRDMG(17)153_Rec%2070-03%20October%202017)
- DCCAE (Department of Communications, Climate Action and Environment). 2020. *General Scheme Online Safety Media Regulation Bill 2019*. Ireland: DCCAE. <https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx>
- DCMS (Department for Digital, Culture, Media and Sport). 2019. *Online Harms White Paper: Consultation*. DCMS: London. <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper>
- DPA (Authority for Personal Data). 2017. "Toezichthouders ACM en AP treden op tegen StemWijzer.nl". Press Release. February 8. <https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezichthouders-acm-en-ap-treden-op-tegen-stemwijzer.nl>
- Dutta, Sweta. 2020. "Curb your OTT Instincts: Government Gives 100 days to Set Up an Adjudicatory Body and Finalize a Code of Conduct". *Mumbai Mirror* March 3. <https://mumbaimirror.indiatimes.com/mumbai/cover-story/curb-your-ott-instincts/articleshow/74449516.cms>
- European Commission. 2020. *Commission Work Programme 2020*. Brussels: European Commission. https://eur-lex.europa.eu/resource.html?uri=cellar%3A7ae642ea-4340-11ea-b81b-01aa75ed71a1.0002.02/DOC_1&format=PDF
- European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Brussels:

- EU. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504>
- European Union. 2018. *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. Brussels: Official Journal of the European Union.
- Fanta, Alexander. 2019. "Leaked Document: EU Commission Mulls New Law to Regulate Online Platforms". *Netzpolitik*, July 16. <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>
- FCC (Federal Communications Commission). 2017. *In the Matter of Section 43.62 Reporting Requirements for U.S. Providers of International Services*. Washington, DC: FCC. https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db1024/FCC-17-136A1.pdf
- Headquarters for Japan's Economic Revitalization. 2015. *New Robot Strategy: Japan's Robot Strategy – Vision, Strategy, Action Plan*. https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/robot_honbun_150210EN.pdf
- ICC (International Chamber of Commerce). 2016. *Regulatory Modernization in the Digital Economy: Developing an Enabling Policy Environment for Innovation, Competition, and Growth*. Paris: ICC. <https://iccwbo.org/content/uploads/sites/3/2016/05/ICC-Digital-Economy-Commission-Policy-Statement-on-Regulatory-Modernization-in-the-Digital-Economy-1.pdf>
- IMDA (Infocomm Media Development Authority). 2020. *Internet of Things (IoT) Cyber Security Guide*. <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf>
- ITU (International Telecommunication Union). 2018a. *Global ICT Regulatory Outlook 2018*. <http://handle.itu.int/11.1002/pub/81234575-en>
- ITU (International Telecommunication Union). 2018b. *ITU World Telecommunication/ICT Regulatory Survey 2018*. Geneva: ITU. https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/ITU_Telecommunication-Regulatory-Survey-2018_E.pdf
- ITU (International Telecommunication Union). 2019. *Digital Infrastructure Policy and Regulation in Asia-Pacific Region*. Geneva: ITU. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/RRITP2019/ASP/ITU_2019_Digital_Infrastructure_5Sep2019FNL.pdf
- ITU (International Telecommunication Union). 2020. *Global ICT Regulation Outlook 2020*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2020-PDF-E.pdf
- Liu, John. 2019. "Telecom Sector Fuels Myanmar's Economy." *Myanmar Times*, December 18. <https://www.mmtimes.com/news/telecom-sector-fuels-myanmars-economy.html>
- LVM (Ministry of Transport and Communications). 2020. "More Frequencies for 5G – Consultation Round on the Terms of the Spectrum Auction Launched". Press Release, February 2. <https://www.lvm.fi/en/-/more-frequencies-for-5g-consultation-round-on-the-terms-of-the-spectrum-auction-launched-1032878>
- Maddens, Sofie. 2016. *Building Blocks for Smart Societies in a Connected World: A Regulatory Perspective on Fifth Generation Collaborative Regulation*. GSR-16 Discussion Paper. Geneva: ITU. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_BuildingBlocksReg_GSR16.pdf (по состоянию на 22 апреля 2020 года).
- Mathew, R., 2020. "Netflix to Slash Traffic Across Europe to Relieve Virus Strain on Internet Providers". *Reuters*, March 22. <https://uk.reuters.com/article/us-health-coronavirus-netflix/netflix-to-slash-traffic-across-europe-to-relieve-virus-strain-on-internet-providers-idUKKBN21906P> (по состоянию на 22 апреля 2020 года).
- MCI (Ministry of Communications and Information). 2016. "MCI Restructures IDA and MDA to Seize New Opportunities". Press Release, January 18. <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2016/1/formation-of-infocomm-media-development-authority-and-government-technology-organisation?page=25>

- MIC (Ministry of Internal Affairs and Communications). 2019. *Approval of specific base station opening plan for introduction of 5th generation mobile communication system*. Japan: Mobile Communications Division of MIC. https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000378.html
- MINTIC (Ministry of Information Technology and Communications). 2018. *Plan TIC 2018-2022: El Futuro Digital es de Todos* (ICT Plan 2018-2022: The Digital Future is for Everyone). https://www.mintic.gov.co/portal/604/articles-101922_Plan_TIC.pdf
- MOSTI (Ministry of Science, Technology and Innovation). 2017. *National Internet of Things (IoT) Strategic Roadmap*. Kuala Lumpur: MOSTI. <https://www.mestec.gov.my/web/wp-content/uploads/2017/02/IoT-Strategic-Roadmap-1.pdf>
- MSIT (Ministry of Science and ICT). 2018. *Final Result of 5G Mobile Communication Frequency Auction*. Seoul: MSIT. [https://www.msit.go.kr/cms/www/policyCom/report/_icsFiles/afieldfile/2018/06/18/180618%20%EC%A6%89%EC%8B%9C%20\(%EB%B3%B4%EB%8F%84\)%205%EC%84%B8%EB%8C%80\(5G\)%20%EC%9D%B4%EB%8F%99%ED%86%B5%EC%8B%A0%EC%9A%A9%20%EC%A3%BC%ED%8C%8C%EC%88%98%20EA%B2%BD%EB%A7%A4%20%EC%B5%9C%EC%A2%85%20EA%B2%B0%EA%B3%BC.pdf](https://www.msit.go.kr/cms/www/policyCom/report/_icsFiles/afieldfile/2018/06/18/180618%20%EC%A6%89%EC%8B%9C%20(%EB%B3%B4%EB%8F%84)%205%EC%84%B8%EB%8C%80(5G)%20%EC%9D%B4%EB%8F%99%ED%86%B5%EC%8B%A0%EC%9A%A9%20%EC%A3%BC%ED%8C%8C%EC%88%98%20EA%B2%BD%EB%A7%A4%20%EC%B5%9C%EC%A2%85%20EA%B2%B0%EA%B3%BC.pdf)
- NBTC (National Broadcasting and Telecommunications Commission). 2019. *Compliance Guide regarding the criteria for granting the use of radio frequency for the development and testing of innovations in a specific regulatory area (Regulatory Sandbox)*. Bangkok: NBTC. http://www.nbtc.go.th/getattachment/spectrum_management/38995/02-%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD-%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%95%E0%B8%B2%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8-Sandbox.pdf.aspx
- OECD (Organisation for Economic Co-operation and Development). 2019. *Going Digital: Shaping Policies, Improving Lives*. Paris: OECD Publishing. <https://www.oecd-ilibrary.org/docserver/9789264312012-en.pdf?expires=1587947608&id=id&accname=guest&checksum=B0115274823F0FB61E9045106E89E38B>
- OECD (Organisation for Economic Co-operation and Development). 2020. *OECD Best Practice Principles for Regulatory Policy: Regulatory Impact Assessment*. Paris: OECD Publishing. <https://www.oecd.org/gov/regulatory-policy/regulatory-impact-assessment-7a9638cb-en.htm>
- Oka, Abhay. 2019. *Writ Petition No. 6050 of 2019 (C) PIL*. High Court: Karnataka. <http://judgmenthck.kar.nic.in/judgmentsdsp/bitstream/123456789/292918/1/WP6050-19-07-08-2019.pdf>
- Republic of Kenya. 2019. *Digital Economy Blueprint: Powering Kenya's Transformation*. Nairobi: Republic of Kenya. <https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf>
- Sayed, Tamer. 2019. "Spectrum Management: Strategic Planning and Policies for Wireless Innovation". Presentation at ITU-D meeting on **Spectrum Management: Strategic Planning and Policies for Wireless Innovation**, Algeria, December 1-5, <https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2019/SPP4WI/Session%2013%20Spectrum%20policies%20for%20wireless%20Innovation%20Spectrum%20and%20infrastructure%20sharing.pdf>
- Seint Aye. 2015. *Telecommunication Licensing Framework in Myanmar*. Myanmar: Posts and Telecommunications Department of the Ministry of Transport and Communication. https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Myanmar/Session6_2%20SeintAye_Myanmar%20licensing.pdf
- Select Committee on Communications. 2019. *Regulating in a Digital World*. 2nd Report of Session 2017–19, HL Paper 229. London: House of Lords. <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>
- SSEACP (State Secretary for Economic Affairs and Climate Policy). 2019. *2019 Procedure on the Provision of Information by ACM*. The Hague: SSEACP. <https://www.acm.nl/sites/default/files/documents/2018-01/procedure-on-the-provision-of-information-by-acm.pdf>
- TMG (Telecommunications Management Group). 2020. *Overview of AI Policies and Development in Latin America*. Arlington, VA: TMG. <https://www.tmgtelecom.com/publications/overview-of-ai-policies-and-developments-in-latin-america/>

World Bank. 2019. *Nigeria Digital Economy Diagnostic Report*. Washington, DC: World Bank. <http://documents.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf>

World Bank and ITU. 2021 (forthcoming). *Regulatory Watch Initiative*.

Глава 2. Конкуренция и экономика



2.1 Введение: преобразования в сфере регулирования в условиях цифровой экономики

Цифровая трансформация стала в последние 10 лет причиной существенных пертурбаций на рынке и в сфере регулирования. Эта тенденция к изменениям, которая сохранится надолго, затрагивает практически все сферы экономики и вызвана прежде всего переходом к ориентированным на обработку данных бизнес-моделям на базе цифровых платформ (ITU 2020a).

В настоящее время цифровые платформы закрепляют за собой доминирующее положение на рынке, при этом погоня за ростом и расширением масштабов ведет к формированию транснациональных рынков. Это означает, что вопросы регулирования все в большей мере выходят за рамки полномочий отдельных национальных регуляторных органов (НРО)¹. Чтобы сохранить эффективность, национальным регуляторным органам в других сферах приходится налаживать сотрудничество в масштабах регионов. Это может происходить в рамках наднациональных или региональных организаций (например, Европейской комиссии), или же отдельные НРО могут опираться на опыт других подобных органов, проявивших инициативу в деле регулирования платформ и контента. С серьезными проблемами сталкиваются регуляторные органы в микросоударствах², поскольку масштабы их национальных рынков недостаточны для поддержания конкурентных моделей предложения и, кроме того, их ресурсов (прежде всего, в плане готовности и кадрового потенциала) может быть недостаточно для регулирования деятельности доминирующего поставщика.

Традиционные национальные услуги по-прежнему существуют, и классическое регулирование услуг и цен продолжится в течение некоторого времени, однако потребность в подобном регулировании в пределах национальных границ снижается. Это происходит потому, что приложения over-the-top (OTT) на транснациональных цифровых платформах ограничивают предоставление традиционных услуг.

¹ Регуляторные органы ИКТ или их аналоги в других сферах государственного аппарата (например, министерства или антимонопольные органы).

² См. тематический раздел "Особенности конкуренции и регулирования в микросоударствах" *Платформы цифрового регулирования*.

Во всяком случае, из-за цифровой трансформации традиционные подходы к регулированию подвергаются все большему давлению.

- Конвергенция услуг фиксированной и подвижной связи, голосовой связи и передачи данных, а также традиционных услуг и услуг ОТТ усложняет задачу определения и анализа рынка. Кроме того, процесс регулирования обычно столь длителен, что он оказывается малоэффективным в условиях быстро развивающихся рынков, а многим регуляторным органам не хватает ресурсов для проведения анализа рынка в целом. Существует настоятельная необходимость упрощения процедуры рыночного анализа, с тем чтобы он мог проводиться оперативно, но при этом был достаточно обоснованным, чтобы можно было противостоять оспариванию его результатов в суде.
- Присоединение по-прежнему крайне важно там, где сосуществуют несколько сетей, однако тарифы на завершение вызова можно упростить, установив их на нулевом или близком к нулевому уровне, зачастую не прибегая к сложным методикам и моделям расчета цен.
- Лицензирование все чаще будет проводиться путем выдачи общего разрешения на предоставление услуг и симметричного регулирования *ex post*, то есть применения одинаковых норм в отношении всех поставщиков услуг, а не только тех из них, которые обладают значительным влиянием на рынке (SMP). Так, например, регуляторные органы должны следить, чтобы не применялась ущемляющая конкуренцию практика пакетирования услуг, и ограничивать слияния и поглощения, способные существенно снизить уровень конкуренции. Чтобы обеспечить действенность этих преобразований в сфере регулирования, понадобятся новые полномочия, а возможно – и новые ведомства по защите конкуренции.

Хотя все цифровые платформы и услуги функционируют в режиме международных рынков, для организации поставок и взаимодействия с клиентами им по-прежнему необходимо иметь доступ к национальной инфраструктуре. Соответственно, НРО следует уделить особое внимание обеспечению наличия такого доступа с достаточной пропускной способностью, приемлемым качеством обслуживания (QoS) и на справедливых условиях.

Постоянно растущий спрос на данные создает трудности для национальной сетевой инфраструктуры, прежде всего для сетей доступа. Потребности в инвестициях, необходимых для обеспечения достаточной полосы пропускания, могут оказаться несовместимыми с требованиями конкуренции (особенно в наименее развитых странах, развивающихся странах, не имеющих выхода к морю, малых островных развивающихся государствах, а также в сельских и изолированных районах), и в этом случае залогом успешного решения проблемы являются требования к лицензированию и условия предоставления государственного финансирования. Кроме того, национальным регуляторным органам следует изучить модели партнерств, в рамках которых цифровые платформы принимают на себя часть расходов по поддержанию национальной инфраструктуры ИКТ (при этом возникает необходимость пересмотреть применение этой концепции и принципы внешних сетевых факторов).

Для разработки надлежащих требований к сети доступа необходимо проводить моделирование затрат и анализ бизнес-плана развертывания сети (ITU 2019a). Регулирование предполагает отслеживание хода работы с применением заранее определенных ключевых показателей деятельности (KPI). Возможность наложения санкций по-прежнему имеет большое значение, хотя штрафы никогда не приводят к удовлетворительному решению проблемы.

В более общем плане, чтобы цифровые платформы приносили доход странам, необходима адаптация политики в сфере налогообложения – возможно, с использованием в качестве основы количества абонентов и объема продаж, а не дохода. Полученные средства следует направлять на финансирование развертывания сетей и повышения качества доступа – либо непосредственно, либо используя альтернативный механизм финансирования развития цифровых технологий, создавая, тем самым, возможности для дальнейшего развития цифровой экономики.

2.2 Регулирование в цифровую эпоху

История вопроса

До начала цифровой революции сети, услуги и рынки электросвязи были, как правило, национальными с точки зрения масштабов и методов предоставления конечным пользователям ограниченного и стандартизованного набора услуг электросвязи. Большинству стран уже удалось преодолеть ограничения,

связанные с монопольным предложением, обеспечив некоторый уровень конкуренции и предоставив потребителям возможность выбора. Вместе с тем вплоть до последнего времени предоставление услуг электросвязи в основном выглядело как односторонняя операция на одностороннем рынке.

Под эгидой НРО, контролирующих квазиконкурентный рынок, цепочка поставок была разделена на оптовый и розничный компоненты. В отношении оптовых поставщиков применялись меры экономического регулирования, особенно в тех случаях, когда они контролировали узкие места сетей или обладали значительным влиянием на рынке. Деятельность розничных поставщиков, как правило, не регулировалась или регулировалась лишь незначительно (за исключением защиты прав потребителей³), поскольку реальная конкуренция могла быть обеспечена за счет предоставления равного доступа к оптовым входным ресурсам.

Тенденции последнего времени

Появились и быстрыми темпами развиваются двусторонние и многосторонние цифровые платформы (например, Facebook, Google). Привлекательными в глазах клиентов их делает предложение инновационных услуг, которые, как кажется клиентам, не стоят им ничего (или обходятся очень дешево). Это верно, если говорить именно о цене, однако бизнес-модель цифровых платформ предполагает использование данных клиентов (хотя зачастую они обезличены и агрегированы) для извлечения выгоды, которая может быть монетизирована на другой стороне платформы (например, за счет рекламодателей или поставщиков контента). Таким образом, цифровые платформы выступают в качестве торговых площадок, объединяющих различные группы клиентов и удешевляющих транзакции между ними.

Речь в данном случае идет о мощном сетевом внешнем воздействии (эффекте)⁴. Сетевые эффекты описывают воздействие дополнительного пользователя какой-либо услуги на ценность этой услуги в глазах других пользователей. Эти внешние факторы могут действовать на одной стороне платформы или по всей платформе и могут быть как позитивными, так и негативными. Воздействие внешних факторов усиливается, если платформа является операционной (то есть обеспечивает возможность проведения операций между клиентами, находящимися по обе стороны платформы).

Рисунок 2.1. Сетевые эффекты цифровых платформ



Источник: ITU 2018a.

³ См. главу 4 "Вопросы, касающиеся потребителей".

⁴ См. тематический раздел "Разъяснение воздействия внешних факторов на цифровые платформы" *Платформы цифрового регулирования*.

В целом, следствием воздействия мощных позитивных внешних факторов при взаимодействии между группами на цифровых платформах стали:

- погоня за наращиванием масштабов. Масштабы играют важнейшую роль в увеличении объемов услуг и снижении затрат. Первопроходцы получают значительные преимущества, и для защиты своего доминирующего положения устоявшиеся платформы нередко приобретают вновь возникающие компании-конкуренты;
- концентрация влияния на рынке. Менее крупным платформам сложнее конкурировать, поскольку их затраты выше и они не в состоянии без труда обеспечивать такую же потребительскую ценность, что и повсеместно распространенные платформы;
- транснациональные и глобальные рынки. Чем ближе охват платформы к общемировому, тем сильнее воздействие внешних сетевых факторов;
- дробление традиционного регулирования сетей электросвязи. Цифровые платформы действуют вне традиционного регулируемого пространства, и государственные границы не являются для них преградой; тем не менее они конкурируют с поставщиками услуг сетей электросвязи и в некоторых случаях подрывают их позиции (например, деятельность поставщиков услуг ОТТ серьезно влияет на традиционные доходы поставщиков услуг сетей электросвязи).

Все эти обстоятельства могут быть источниками проблем для экономического регулирования. Они создали ситуацию, в которой:

- цифровые платформы не имеют границ: они слишком велики и слишком широки для того, чтобы их можно было регулировать;
- уровень рыночной концентрации оказался чрезмерным: конкуренция столь ограничена, что можно говорить о фактическом формировании монополий;
- данные потребителей являются источником непрозрачного и потенциально вредоносного финансирования системы;
- цифровые платформы не вносят соответствующего пропорционального вклада в развитие национальной инфраструктуры, на которую они опираются.

Однако потребители, как правило, не жалуются. Им нравятся предлагаемые услуги, равно как и их низкая или вообще нулевая стоимость. Даже если потребителей беспокоит вопрос о том, как используются их персональные данные, они готовы принимать (как правило, не читая) любые условия, навязываемые поставщиками платформ. Именно здесь свое слово должно сказать регулирование, предоставляя меры защиты, отслеживая операции и, при необходимости, налагая санкции⁵.

Сетевой нейтралитет – эта та область регулирования, которая привлекает к себе особое внимание. Под сетевым нейтралитетом понимается обработка всех пакетов данных на равной основе, вне зависимости от приложения, пользователя или цены. Ниже приведено краткое изложение ключевых принципов сетевого нейтралитета (FCC 2015).

- **Запрет блокирования:** операторы сетей не имеют права блокировать доступ к не запрещенным законом услугам, контенту, приложениям или не являющимся вредоносными устройствам.
- **Запрет ограничения скорости:** операторы сетей не имеют права нарушать или снижать не запрещенный законом интернет-трафик на основании контента, приложений, услуг или не являющихся вредоносными устройств.
- **Запрет установления приоритетов на платной основе:** операторы сетей не имеют права отдавать предпочтение тому или иному не запрещенному законом интернет-трафику в сравнении с другим не запрещенным законом трафиком в обмен на вознаграждение в какой-либо форме; иными словами, "полосы быстрой передачи" запрещены. Данное правило также запрещает ПУИ устанавливать какие-либо приоритеты в отношении контента и услуг аффилированных с ними структур.

Перед операторами сетей электросвязи по-прежнему стоит задача обеспечивать ширину полосы, достаточную для поддержки всех приложений, которые предлагаются в интернете и являются востребованными у потребителей. Возможности операторов по установлению расценок для конечных

⁵ См. главу 4 "Вопросы, касающиеся потребителей" и главу 5 "Защита данных и доверие".

пользователей жестко ограничиваются, поэтому они могут пытаться получить оплату на "другой стороне" рынка. Однако сегодня позиции цифровых платформ на рынке столь прочны, что оператор сети может оказаться не в состоянии добиться дополнительного дохода. Соответственно, столкнувшись с недостатком поступлений с обеих сторон рынка, оператор может попытаться вместо этого заблокировать контент, уменьшить скорость обработки запросов или отдать приоритет платному трафику просто для того, чтобы покрыть свои расходы.

Хотя Федеральная комиссия по связи США (ФКС) позднее пересмотрела свое решение (FCC 2018), регуляторные органы по всему миру продолжают руководствоваться принципами, которые она сформулировала в 2015 году. Так, например, в аналогичном Регламенте Европейского парламента (EU 2015) содержится требование, согласно которому "при предоставлении услуг доступа в интернет поставщики услуг по обеспечению доступа в интернет обрабатывают весь трафик одинаково, без дискриминации, ограничения или помех и независимо от того, кто является отправителем или получателем, а также независимо от контента, к которому предоставляется доступ или который распространяется, используемых или предоставляемых приложений или услуг либо используемого окончательного оборудования", хотя это не препятствует применению "разумных мер по управлению трафиком"⁶.

На деле принципы сетевого нейтралитета действуют не как регулирование *ex ante*, а в качестве руководства по мерам *ex post*, принимаемым по мере необходимости с учетом особенностей каждого конкретного случая. В одной из статей⁷ в связи с этим даются следующие разъяснения:

"Между поставщиками услуг широкополосного доступа и поставщиками интернет-контента существует симбиоз – они живут за счет друг друга, и каждая из сторон нуждается в другой стороне, помогающей ей получать доходы и прибыль. С точки зрения экономики, существование все более влиятельных поставщиков интернет-контента создает уравновешивающее потребительское влияние, необходимое для сдерживания доминирования действующих поставщиков услуг по предоставлению доступа на национальных рынках, тогда как запрос на двусторонний рынок означает, что поставщики контента не могут позволить себе использовать свою экономическую мощь в ущерб организациям, обеспечивающим их связь с теми самыми конечными пользователями, которые и создают эту мощь. В будущем роль регуляторного органа будет заключаться скорее в мониторинге соблюдения договоров, нежели во вмешательстве в ценообразование или определении уровней качества обслуживания. Соответственно, правила сетевого нейтралитета являются в первую очередь руководством по разрешению споров *ex post* – именно это и предлагается в приказе ФКС об открытом интернете".

В Европе Совет европейских регуляторных органов в области электронной связи принял рекомендации для национальных регуляторных органов по осуществлению правил обеспечения сетевого нейтралитета (BEREC 2016) и после этого представляет ежегодные отчеты о применении этих рекомендаций, обращая особое внимание на появляющиеся технологии 5G во взаимосвязи с принципом сетевого нейтралитета.

Основные выводы

- Регулирование традиционных сетей продолжится – хотя по сравнению с поставщиками цифровых платформ операторы сетей, возможно, не столь влиятельны, однако они по-прежнему контролируют доступ к потребителю, – однако, чтобы регулирование оставалось актуальным и эффективным, приоритетное внимание в его рамках необходимо во все большей мере уделять открытому и недискриминационному доступу к инфраструктуре.
- Регуляторным органам следует с осторожностью подходить к выдаче поставщикам цифровых платформ разрешений на создание сетевой инфраструктуры, чтобы не допустить злоупотребления влиянием на рынке доступа к сетям, однако при этом следует подумать о способах привлечения цифровых платформ к покрытию расходов на развертывание и эксплуатацию инфраструктуры доступа.
- Регулирование следует во все большей мере проводить *ex post*, сосредоточив внимание на мониторинге соблюдения договоров и урегулировании споров между операторами сетей электросвязи и цифровыми платформами на основе четких принципов, в частности принципов сетевого нейтралитета.

⁶ См. EU 2015, 8 (Article 3).

⁷ См. Rogerson, Holmes, and Seixas 2016, 9.

- НРО необходимо сотрудничать друг с другом и с антимонопольными органами, чтобы обеспечить последовательное и эффективное регулирование цифровых платформ. Региональные/международные органы, такие как МСЭ и региональные ассоциации регуляторных органов⁸, будут играть в этих вопросах ведущую роль, обеспечивая скоординированное и согласованное регулирование. НРО в развивающихся странах могли бы также использовать опыт других структур, проявивших инициативу в области регулирования платформ и контента, например подходы к регулированию цифровых платформ, применяемые Австралийской комиссией по вопросам конкуренции и прав потребителей (АССС⁹), равно как и опыт работы по регулированию услуг ОТТ в Индии¹⁰.

2.3 Регулирование рынков

История вопроса

В основе экономического регулирования всегда лежала процедура анализа рынка, включающая три составные части¹¹.

- Определение рынков.** Для целей регулирования определение рынков дается исходя из взаимозаменяемости спроса и предложения; при этом границы рынка определяются на основании поведенческой реакции на небольшое, но существенное и не носящее временного характера увеличение цены (SSNIP) гипотетическим монополистом, поставляющим на этот рынок один основной продукт. По умолчанию рынки обычно определяются на национальном уровне (в отдельных случаях – с региональными вариантами).
- Оценка доминирующего положения или значительного влияния на рынке (SMP).** Хотя на формирование или поддержание доминирующего положения на рынке влияет множество экономических факторов, в законодательстве и в практике работы регуляторных органов основное внимание уделяется оценке доли рынка (как правило, исходя из величины доходов), поскольку этот показатель проще всего рассчитать и оценить. Иногда регуляторные органы учитывают и другие соответствующие факторы, например степень концентрации рынка, доступ к финансам, эффект диверсификации, внедрение технических новшеств и перспективы уравнивающего влияния покупателей.
- Принятие соразмерных мер воздействия.** Меры воздействия в отношении поставщиков, обладающих значительным влиянием на рынке, принимаются *ex ante*, чтобы не допустить с их стороны подрывающих конкуренцию действий, которых можно обоснованно ожидать от них в отсутствие регулирования. Следует избирать такие меры воздействия, которые, предполагая минимальное вмешательство, позволяли бы должным образом решать выявленные конкретные проблемы в сфере конкуренции. Применяемые обычно меры воздействия можно разделить на следующие основные категории:
 - обязательство осуществлять поставки;
 - недопущение дискриминации;
 - прозрачность (например, публикация стандартных предложений);
 - ценообразование на основе затрат.

При выявлении конкретных действий, направленных на подрыв конкуренции (например, установление демпинговых цен, вытеснение конкурентов, привязывание услуг к пакетам или их предоставление исключительно в пакетах), можно применять и меры воздействия *ex post*¹². Процедура анализа рынка, которой надлежит придерживаться, аналогична регулированию *ex ante*: цель состоит в том, чтобы принять соразмерные меры воздействия в отношении поставщиков, обладающих значительным влиянием на рынке. Вместе с тем регулирование *ex post* налагает на регулятора обязанность доказать,

⁸ См. веб-сайт МСЭ. https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RA_Portal/Home.aspx

⁹ См. тематический раздел "Обзор подходов АССС к регулированию цифровой платформы" *Платформы цифрового регулирования*.

¹⁰ См. тематический раздел "Регулирование услуг ОТТ в Индии" *Платформы цифрового регулирования*.

¹¹ Полное описание см. в Blackman and Srivastava 2011, 32ff; и МСЭ 2016.

¹² Полное описание см. в Blackman and Srivastava 2011, 38ff.

что определенное поведение подрывало конкуренцию или проводилось с этим намерением, а затем принять меры воздействия, которые устранят любой причиненный ущерб и возместят его.

Удачным примером является анализ рынка, проведенный в Молдове: он показывает, как НРО смог воспользоваться прочными основами, заложенными в ходе первого раунда анализа рынка, так что последующее обновление данных велось по упрощенной, но надежной процедуре¹³.

Тенденции последнего времени

Развитие цифровых платформ и последующий рост конкуренции со стороны поставщиков услуг, не связанных с операторами сетей электросвязи, кардинально изменили условия на рынках, которые пытаются анализировать регуляторные органы. В частности:

- Рынки нельзя более по умолчанию считать национальными с точки зрения охвата; в результате НРО становится сложнее проводить анализ рынка, поскольку они не могут запрашивать или без проблем получать актуальные данные у участников глобального рынка.
- Определение рынка становится сложнее из-за существования двусторонних цифровых платформ¹⁴ – непонятно, идет ли речь о едином рынке, охватывающем обе стороны платформы, или о двух разных рынках.
- Тест SSNIP сложно проводить на рынках, где услуги часто предоставляются бесплатно, в пакете или по ценам, не зависящим от интенсивности использования. На какую цену следует ориентироваться? Что рассматривать как SSNIP, если базовая цена является нулевой?
- Возможна ситуация, когда наличие одного доминирующего участника на рынке более не рассматривается как нежелательное положение дел (или как то, чего можно избежать). Одна платформа, занимающая большую долю рынка, может являться способствующей улучшению показателей рыночной структурой, свидетельствующей о значительном сетевом эффекте. Резкий рост спроса на данные, влекущий за собой масштабные инвестиции в сеть, может во многих случаях оказаться несовместимым с моделями конкурентного рынка.
- Соответственно, определять SMP (и меры регулирования в его отношении) необходимо исходя из гораздо более широкого набора показателей (например, дифференцирование услуг, перегрузка сети, доступность данных, инновации, препятствия для выхода на рынок и препятствия для роста).
- Многие модели поведения, ранее считавшиеся подрывающими конкуренцию, сегодня представляют собой неотъемлемый элемент полноправных бизнес-моделей; например, установление определенных цен ниже предельных издержек и привязка некоторых услуг к пакетам являются общей отличительной чертой цифровых платформ. Обеспокоенность по поводу установления демпинговых цен и вытеснения конкурентов остается, однако выявлять подобные случаи и доказывать, что они имели место, будет все сложнее.

Основные выводы

- Традиционное регулирование *ex ante*, основывающееся на определении рынка, доминирующем положении и применении мер воздействия, будет и далее сохранять свое значение, особенно в части регулирования доступа к сетевой инфраструктуре.
- В более общем плане регулирование конкуренции претерпит изменения, постепенно превращаясь в симметричное регулирование *ex post* (в рамках которого в отношении всех поставщиков действуют одни и те же нормы); при этом регуляторные органы будут принимать меры в отношении конкретных случаев ущерба для конкуренции, а также активно развивать межсекторальное сотрудничество в сфере регулирования.
- Эти изменения необходимы, поскольку:
 - традиционное регулирование, исходящее из определения SMP, имело целью предоставить всем остальным возможности для добросовестной конкуренции, однако сегодня в некоторых

¹³ См. тематический раздел "Анализ рынка в Молдове" *Платформы цифрового регулирования*.

¹⁴ См. тематический раздел "Подход к определению рынка в контексте цифровых платформ" *Платформы цифрового регулирования*.

случаях цифровые платформы, сети доступа и даже национальные широкополосные сети в целом эффективнее всего работают, будучи виртуальными монополиями;

- даже при наличии конкуренции становится все сложнее определять рынки, устанавливать пороговые значения для SMP, а также разрабатывать и применять необходимые меры воздействия;
- в нынешних условиях некоторые трансграничные операторы, являющиеся слишком большими, чтобы потерпеть крах, и/или слишком крупными, чтобы им можно было нанести урон, могут действовать и действуют, не опасаясь санкций со стороны регуляторных органов.
- В основу симметричного регулирования будут положены общие принципы регулирования, например справедливый, разумно необходимый и недискриминационный доступ к ресурсам.
- Чтобы обеспечить эффективность регулирования *ex post*, странам следует создавать отдельные антимонопольные органы и предоставлять им необходимое финансирование (или наделять такими же полномочиями НРО).

2.4 Присоединение сетей

История вопроса

Полная взаимоподключаемость была основополагающим требованием для вновь либерализованных рынков электросвязи, гарантирующим всем пользователям возможность установить соединение друг с другом вне зависимости от сетевого оператора¹⁵. Соответственно, взаимодействие между конкурирующими сетями играло здесь ключевую роль, и, поскольку силы операторов, занимающих существенное положение в сети связи, и новых участников рынка были неравными, прийти к справедливым, разумным и содействующим конкуренции договоренностям в ходе коммерческих переговоров было невозможно.

Сфера применения принципа регулируемого присоединения была расширена, с тем чтобы под его действие подпадал оптовый доступ к любому технически или коммерчески обоснованному компоненту сети традиционного оператора или оператора SMP. Задача заключалась в создании "равных условий", когда новые участники рынка могли бы делать беспристрастный выбор между созданием собственной инфраструктуры и арендой у традиционного оператора посредством получения доступа или присоединения. Поскольку доступ к необходимым оптовым входным ресурсам являлся предметом регулирования, новые участники рынка могли воспроизводить розничные предложения SMP-поставщика.

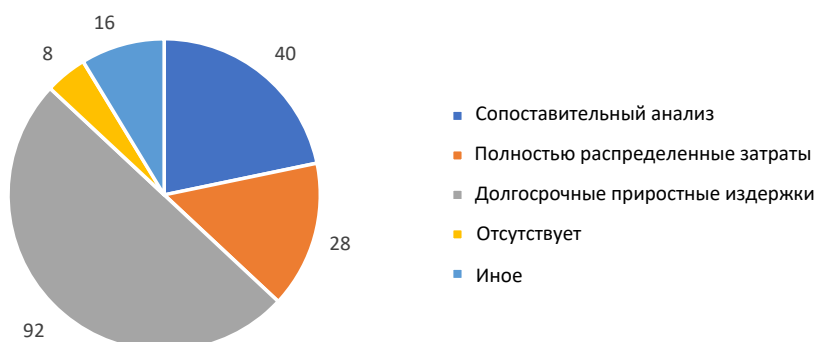
Чтобы новый участник рынка мог принимать беспристрастное решение о том, "создавать или покупать", необходимо, чтобы плата за регулируемый доступ и присоединение устанавливалась на основе затрат. Чтобы определить наиболее экономически эффективный стандарт, была проделана масштабная теоретическая и практическая работа, и постепенно чаша весов склонилась к использованию модели долгосрочных приростных издержек с надбавкой на общие накладные расходы (LRIC+). Большинство регуляторных органов разрабатывали собственные модели расчета затрат по принципу "снизу вверх" (bottom-up) (то есть моделируя работу реально существующих сетей с учетом наиболее эффективных экономических и инженерных подходов), что привело к широкому распространению стандарта затрат, сокращенно названного BU-LRIC+. Вместе с тем в некоторых местах (прежде всего, в странах Европейского союза¹⁶) для завершения вызовов применялись и более низкие ставки, в основу которых были положены "чистые LRIC". Чистые LRIC рассчитываются как разность общих затрат с учетом и без учета услуги завершения вызовов, деленная на количество минут завершения вызова.

¹⁵ Полное описание см. в Blackman and Srivastava 2011, 119ff.

¹⁶ История установления платы за присоединение в Европейском союзе описана в тематическом разделе "Снижение тарифов и падение цен на завершение вызовов в сетях подвижной связи в Европе" *Платформы цифрового регулирования*.

Рисунок 2.2. Как рассчитываются цены на присоединение на основе затрат

Подход к установлению платы за регулируемое присоединение (количество стран, 2019 год)



Источник: МСЭ.

Тенденции последнего времени

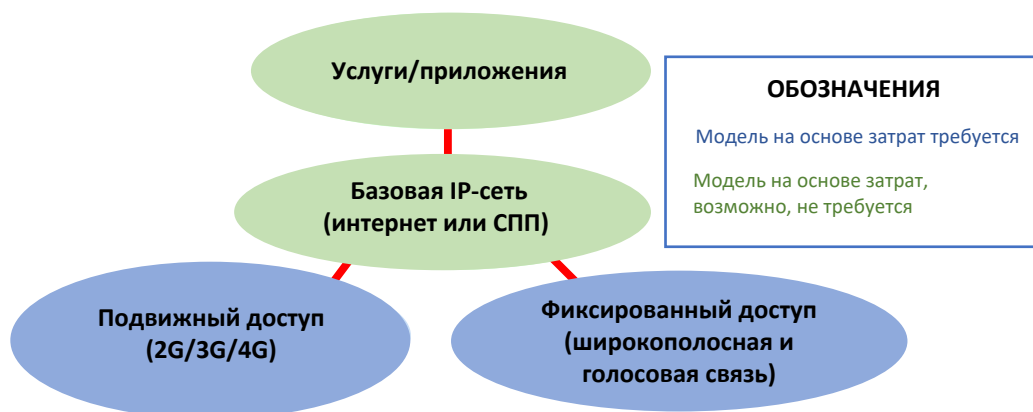
Присоединения для передачи голосовых сообщений и SMS по-прежнему играют важную роль, особенно в странах, где наиболее распространенной технологией для сетей и/или для устройств и услуг является 2G (например, в Африке). Вместе с тем сети, ориентированные на передачу данных и работающие на основе протокола Интернет (IP), коренным образом изменили цепочку поставки услуг, что повлияло на издержки и цены и потребовало пересмотра традиционной практики регулирования. Тенденцией развития сетей на основе IP является сокращение числа сетевых узлов, функциональная централизация услуг и использование различных каналов передачи для одного и того же соединения. Все это ведет к высоким фиксированным и низким переменным издержкам, и, таким образом, взимание платы по факту использования приобретает несколько умозрительный характер.

Переход на IP-сети влияет на основное условие для регулирования на основе затрат, особенно в части услуг присоединения. В мире IP доминирует передача данных: на голосовую связь приходится сокращающаяся и незначительная часть общих сетевых мощностей, и поэтому определение платы за завершение голосового вызова на основе затрат играет минимальную роль¹⁷. Возможно, что регуляторные модели на основе затрат для базовой IP-сети не понадобятся вообще; по мере роста конкуренции количество SMP, вероятно, сократится, и регулирование *ex ante* будет востребовано все меньше.

Если потребность в регулировании присоединений на основе затрат снижается, то потребность в регулировании доступа на основе затрат растет. Поставщикам приложений необходим открытый доступ к цифровой инфраструктуре, поскольку только эта инфраструктура предоставляет им возможность связи с их клиентами. Во многих случаях, особенно если речь идет о приложениях с интенсивным использованием полосы пропускания, например видео, необходим доступ к инфраструктуре с высокой пропускной способностью. Это требует от поставщика доступа инвестиций (например, в развертывание волоконных линий для сетей фиксированной связи или технологий подвижной связи 4G/5G), покрывать которые придется либо непосредственно за счет клиентов, либо через поставщика прикладных услуг.

¹⁷ См. тематический раздел "Как рост объемов данных влияет на плату за присоединение" *Платформы цифрового регулирования*.

Рисунок 2.3. Во главу угла в регуляторных моделях на основе затрат следует ставить цены доступа



Источник: ITU 2019b.

Основные выводы

- Эффективная политика и регулирование в сфере ИКТ предполагает не только продолжение поддержки присоединения традиционных сетей с коммутацией каналов, но и содействие в развертывании сетей с очень большой пропускной способностью (VHCN), таких как волоконные сети, кабельные сети со спецификацией интерфейса службы передачи данных по кабелю (DOCSIS) и сети подвижной связи 5G. Сроки такого развертывания в разных странах будут отличаться.
- Для решения этих задач используются две основные модели:
 - единая национальная широкополосная сеть, либо принадлежащая государству, либо действующая в рамках государственно-частного партнерства (например, *Red Compartida*¹⁸ в Мексике);
 - регуляторная среда, стимулирующая ориентированное на потребности рынка развертывание высокоскоростных сетей широкополосной связи (например, Европейский кодекс электронных средств связи¹⁹).
- Какая бы модель ни использовалась, цены доступа необходимо регулировать, чтобы обеспечить инвестиционную прибыль в сетях VHCN, а также для создания стимулов к повторному и совместному использованию пассивной инфраструктуры там, где это возможно (см. раздел "Совместное использование инфраструктуры" ниже и МСЭ 2018с), и для обеспечения приемлемости в ценовом отношении.
- Ценообразование по модели BU-LRIC+ остается актуальным, однако при этом необходимо больше внимания уделять доступу к инфраструктуре и гораздо меньше – завершению голосовых вызовов. Например, в Европейском союзе плата за завершение голосовых вызовов рассчитывается в настоящее время исходя из "евроставок" – стандартных ставок, устанавливаемых с учетом затрат и применяемых во всех государствах-членах²⁰.

2.5 Совместное использование инфраструктуры

История вопроса

На ранних стадиях либерализации постоянно велись споры о сравнительных преимуществах конкуренции на основе технических средств и конкуренции на основе услуг. В рамках первой модели первостепенное внимание уделялось конкурентному предложению инфраструктуры, даже если это ограничивало выбор поставщиков услуг для потребителей. Считалось, что затраты на дублирование инфраструктуры будут небольшими в сравнении с выгодами, которые получают потребители за счет возможности выбора и

¹⁸ См. тематический раздел "Сеть Red Compartida" *Платформы цифрового регулирования*.

¹⁹ См. тематический раздел "Европейский кодекс электронных средств связи" *Платформы цифрового регулирования*.

²⁰ См. тематический раздел "Снижение тарифов и падение цен на завершение вызовов в сетях подвижной связи в Европе" *Платформы цифрового регулирования*.

инноваций, сопряженных с применением моделей конкурентного предложения инфраструктуры. Соединенное Королевство и Соединенные Штаты стали в 1980-е и 1990-е годы первыми странами, отдавшими предпочтение конкуренции на основе технических средств.

Однако, поощряя конкуренцию на основе технических средств, регуляторные органы вскоре обнаружили, что барьеры для выхода на рынок слишком высоки, и была предложена теория "инвестиционной лестницы" (Cave 2006). Идея состояла в том, что при наличии разных вариантов доступа к инфраструктуре инвесторы смогут выбирать для себя точку входа и затем постепенно наращивать объем инвестиций, становясь в итоге операторами, имеющими полнофункциональное собственное оборудование. Для этого необходимо было обеспечить техническую и коммерческую доступность всех точек сети, создавая, тем самым, полный набор различных вариантов совместного использования инфраструктуры, в том числе пассивных (инженерно-строительных) ресурсов, активного электронного оборудования и радиочастотного спектра.

Тенденции последнего времени

Потребность в совместном использовании инфраструктуры растет по мере увеличения объемов инвестиций, необходимых для создания и эксплуатации широкополосной цифровой инфраструктуры. Именно в тот момент, когда складывались условия для преобразований, ведущих к формированию цифровой экономики, мировой финансовый кризис 2008–2009 годов снизил доступность инвестиционных ресурсов; аналогичная динамика наблюдается и сегодня, когда потребность в инвестициях в сети подвижной связи 5G и интернет вещей (IoT) наложилась на глобальную рецессию, вызванную пандемией COVID-19.

В связи с этим совместное использование инфраструктуры, по-видимому, навсегда останется характерной чертой сферы электросвязи. Во всем мире наблюдается тенденция к разрешению совместного использования инфраструктуры, а зачастую – и к предписанию обязательного совместного использования критических элементов в цепочке поставок: абонентских линий, кабельных каналов, вышек и площадок. Хорошим примером служит Бруней-Даруссалам, где все сети фиксированной и подвижной связи объединены в одну новую структуру, равный доступ к которой имеют все поставщики услуг²¹. Как правило, активы не переводятся в общую собственность, однако при этом сохраняется необходимость обеспечивать открытый и недискриминационный доступ к совместно используемой инфраструктуре (например, к подводному кабелю на Сейшельских Островах).

В большинстве юрисдикций условия совместного использования инфраструктуры определяются в ходе коммерческих переговоров, однако регуляторные органы могут публиковать рекомендации, а также привлекаться к урегулированию споров (см. раздел "Урегулирование споров" ниже). В основе передовых методов регулирования совместного использования инфраструктуры лежат следующие принципы²².

- Систему регулирования следует применять в отношении всех участников отрасли.
- Следует разрешать все виды совместного использования, не оказывающие негативного влияния на конкуренцию.
- Всем участникам отрасли следует предоставить право подавать запросы на совместное использование инфраструктуры, в отношении которой имеется разрешение на такое использование.
- Все участники отрасли обязаны в случае получения соответствующего запроса провести переговоры о совместном использовании своей (подлежащей такому использованию) инфраструктуры.
- Операторы, отнесенные к категории SMP на рынке пассивной или активной инфраструктуры, обязаны опубликовать утвержденное НРО стандартное предложение.
- Необходимо, чтобы коммерческие условия совместного использования инфраструктуры были прозрачными, справедливыми/экономически целесообразными и недискриминационными.
- Необходимо, чтобы процедура утверждения новых объектов инфраструктуры была оперативной и эффективной и поощряла совместное использование инфраструктуры.

²¹ См. тематический раздел "Единая интегрированная оптовая широкополосная сеть в Брунее" *Платформы цифрового регулирования*.

²² По материалам ITU 2018b, 59, на основании рекомендаций, разработанных МСЭ для Ассоциации регуляторных органов в области связи стран юга Африки (CRASA) в 2016 году.

- Урегулирование споров следует проводить на межотраслевой основе, с необходимым документальным оформлением, своевременно и эффективно.
- Система регулирования совместного использования инфраструктуры должна учитывать национальный план развития широкополосной связи, политику фонда универсального доступа и обслуживания (ФУДО) и дальнейшее развитие технологий.

Основные выводы

- Цифровая экономика требует крупных инвестиций и широкого географического охвата, что исключает возможность полномасштабной конкуренции на основе технических средств. В силу этого вопрос совместного использования инфраструктуры становится прерогативой регуляторных органов.
- Оптимальным является установление цен на совместное использование инфраструктуры в ходе коммерческих переговоров, позволяющее закрепить коммерческую норму прибыли на инвестиции, однако регуляторные органы должны иметь возможность контролировать условия договоров, не допуская злоупотребления доминирующим положением на рынке со стороны владельцев инфраструктуры.
- Всем поставщикам услуг, включая цифровые платформы, в наибольшей степени нуждающиеся в инфраструктуре с высокой пропускной способностью, следует вносить пропорциональный вклад в погашение затрат на создание такой инфраструктуры, выплачивая соответствующую установленную регуляторным органом плату за доступ²³.

2.6 Регулирование цен

История вопроса

До либерализации рынка правительства устанавливали все цены на услуги электросвязи в рамках годового бюджета²⁴. Спектр услуг был ограничен, цены из года в год оставались примерно одинаковыми и, как правило, были высокими, поскольку электросвязь являлась источником доходов.

После либерализации правительства задались целью расширять сектор путем конкуренции и получать доходы от него прежде всего за счет выдачи лицензий и разрешений и налогообложения (см. разделы ниже). При этом контроль цен осуществлялся главным образом на оптовом уровне (см. раздел "Присоединение"), а регулирование розничных цен было смягчено – насколько именно, зависело от уровня конкуренции, но обычно основное внимание уделялось SMP-поставщикам. Основным инструментом регулирования был отказ от применения принудительных мер: вмешательство осуществлялось лишь в необходимых случаях – во избежание чрезмерного завышения цен или применения антиконкурентных цен.

Обычно регуляторные органы применяют два стандарта регулирования розничных цен.

- Утверждение цены – при таком подходе цена должна быть официально утверждена регуляторным органом до выхода на рынок. Метод утверждения цены наиболее эффективен только применительно к значимым тарифам тех обладателей лицензий, которые занимают доминирующее положение на рынке соответствующих услуг. Если нет разумных причин для возражений в отношении какого-либо тарифа, регуляторному органу следует утверждать тарифы оперативно, чтобы не препятствовать нормальному функционированию рынка.
- Уведомление о цене – при таком подходе сведения о тарифах передаются регуляторному органу только для информации. Этот подход уместен там, где поставщик услуг не обладает значительным влиянием на рынке, где соответствующая услуга имеет относительно небольшое значение, а также в случае краткосрочных рекламных предложений.

Хорошим примером применения этих процедур является регулирование тарифов в Иране²⁵.

²³ См., например, Digicel 2019.

²⁴ Полное описание см. в Blackman and Srivastava 2011, 150ff.

²⁵ См. тематический раздел "Процедуры утверждения цен и уведомления о ценах в Иране" *Платформы цифрового регулирования*.

Тенденции последнего времени

Целью традиционного регулирования розничных цен является вмешательство лишь в тех ситуациях, когда поставщики, обладающие значительным влиянием на рынке, могут в противном случае использовать свое положение на рынке в ущерб потребителям. Однако рост прямой и косвенной конкуренции со стороны нерегулируемых цифровых платформ оказывает серьезное сдерживающее воздействие на розничные тарифы всех поставщиков услуг электросвязи, даже поставщиков SMP.

Соответственно, в настоящее время роль регулирования цен изменяется – теперь она заключается скорее в обеспечении добросовестной конкуренции между поставщиками услуг с собственным оборудованием, нежели в прямой защите конечных пользователей. Регуляторный риск заключается не в завышении цен, а в установлении демпинговых цен, приводящем к недофинансированию развития сетей. Тарификация услуг широкополосной связи представляет собой сложную задачу (на нее влияют такие факторы, как средняя и минимальная скорость скачивания и загрузки, предельные объемы использования и срок контракта), и это дает поставщикам, занимающим доминирующее положение, дополнительные возможности для антиконкурентного ценообразования (например, навязывания клиентам долгосрочных контрактов или постоянного несоблюдения заявленных скоростей загрузки/скачивания данных).

Кроме того, в ответ на вызов со стороны поставщиков услуг ОТТ операторы сетей электросвязи все чаще применяют "нулевой рейтинг" и пакетные тарифы (например, пакет "четыре в одном" – сочетание услуг широкополосного доступа к интернету, телевидения, фиксированной телефонной связи и беспроводной связи) и активнее предлагают в рекламных целях льготные цены, чтобы обойти наследие прошлого – меры контроля ценообразования со стороны регуляторных органов. Многие подобные процессы отвечают интересам потребителей и не должны приводить к вмешательству регуляторных органов. Вместе с тем регуляторным органам необходимо проводить проверки на предмет применения методов, подрывающих конкуренцию²⁶.

Основные выводы

- В вопросе регулирования розничных цен позиция регуляторных органов должна сводиться в основном к активному мониторингу и сбору информации: меры следует принимать решительно, однако по принципу *ex post*.
- В большинстве случаев мер регулирования *ex post* в ответ на жалобу или претензию (например, на демпинговые цены или уменьшение маржи) может быть достаточно.
- Поставщики услуг обязаны регулярно предоставлять данные о количестве абонентов, тарифах на услуги и их объемах, чтобы регуляторные органы могли оперативно принимать меры в случае необходимости.
- Особое внимание следует уделять продуктам начального уровня (прежде всего, в отношении доступа в интернет), обеспечивая их приемлемость в ценовом отношении, включая применение "нулевого рейтинга", если это не является недобросовестной конкуренцией в сфере услуг.
- Поскольку в некоторых странах (например, с низкой плотностью населения, островных государствах или странах, не имеющих выхода к морю) обеспечение доступа в интернет сопряжено с более высокими издержками (A4AI 2018, s4.2), особую важность приобретают меры политики, помогающие снижать эти издержки (например, путем предоставления государственных инвестиций, целевых субсидий или налоговых каникул), а также расширять доступ в интернет и обеспечивать его приемлемость в ценовом отношении²⁷.

²⁶ См. тематический раздел "Как регулировать ценовые пакеты" *Платформы цифрового регулирования*.

²⁷ Комиссия ООН по широкополосной связи сформулировала целевой показатель "1 за 2": цена 1 Гб данных должна быть ниже 2% месячного валового национального дохода на душу населения (см. Broadband Commission for Sustainable Development 2019, 34).

2.7 Урегулирование споров

Предметом рассмотрения в данном разделе являются споры между операторами, в первую очередь споры, касающиеся присоединения и ценообразования²⁸.

История вопроса

Законодательство часто возлагает на национальный орган по регулированию ИКТ ответственность за урегулирование споров между обладателями лицензий, как описано в главе 1 "Регуляторное управление и регуляторная независимость"²⁹. Соглашение Всемирной торговой организации (ВТО) об основных услугах электросвязи (WTO 1996) предписывает странам-членам создавать независимые органы по урегулированию споров, и обычно такие обязанности возлагаются на регуляторные органы. Как правило, вместо принятия обязывающих решений, которые могут быть оспорены в суде, регуляторные органы стремятся принимать на себя роль посредников в спорах между операторами, добиваясь приемлемых для всех сторон договоренностей.

Основными причинами использования альтернативных механизмов урегулирования споров являются стремление избежать высоких издержек, неопределенность исхода судебных разбирательств и сопряженные с ними потери времени. В случаях, когда принимаемое регуляторным органом решение вызывает разногласия, действенным конечным арбитром может стать независимый орган (например, Апелляционный совет по делам, касающимся ИКТ, в Папуа – Новой Гвинее или Апелляционный трибунал по делам о мультимедиа в Кении)³⁰. Однако иногда утвержденная процедура столь схожа с официальным судопроизводством, что говорить о каком-то выигрыше с точки зрения расходов, затраченного времени и нормативной определенности практически не приходится.

Хотя альтернативная система урегулирования споров может быть предпочтительнее официальной судебной процедуры, гораздо лучше вообще избегать возникновения споров. Урегулированию множества споров способствовали прозрачные процедуры (например, публичные консультации), обоснованность позиций и использование услуг внешних консультантов.

Рисунок 2.4. Способы снизить риск возникновения споров по вопросам присоединения/ценообразования



Тенденции последнего времени

Для отрасли электросвязи характерно большое количество судебных разбирательств: здесь часто возникают споры, связанные с крупными суммами, однако та или иная процедура официального урегулирования споров применяется в отношении лишь немногих из них. Исследование, проведенное недавно Лондонским университетом королевы Марии (QMUL 2016), показало, что споры в отрасли электросвязи возникали чаще и по поводу более значительных сумм, нежели в других отраслях, а компании электросвязи, как правило, предпочитают для разрешения споров обращаться в суд, а не к услугам арбитража. Дело, которое недавно рассматривалось в Нидерландах, свидетельствует о тенденции к обращению в суд в случае споров по вопросам конкуренции и установления цены на доступ. При рассмотрении этого дела Верховный суд Нидерландов отменил решение национального регуляторного органа, констатировавшего

²⁸ О спорах между операторами (или поставщиками услуг) и конечными пользователями см. главу 4 "Вопросы, касающиеся потребителей".

²⁹ Полное описание см. в Blackman and Srivastava 2011, 147ff, и в Bruce and others 2004.

³⁰ При этом всегда имеется возможность обратиться в суд по вопросам правового характера или по вопросу о том, насколько правильно судебный орган определил сферу собственной юрисдикции.

совместное доминирование операторов двух основных сетей фиксированной связи и потребовавшего от них обеспечить доступ к своим сетям на основе покрытия затрат³¹.

Хотя разбирательство в суде более популярно, несколько ключевых особенностей арбитража делают его особенно удобным для урегулирования споров в сфере электросвязи:

- возможность обеспечить исполнение – стороны с самого начала договариваются согласиться с любым решением, которое вынесет арбитраж;
- возможность избежать иностранной юрисдикции – это особенно полезно в случае споров с участием международных компаний, например цифровых платформ;
- участие экспертов в принятии решения – при арбитраже решения принимаются, как правило, группой экспертов, приемлемой по своему составу для сторон и включающей специалистов, обладающих необходимым опытом в правовой, экономической и технической сферах;
- обеспечение конфиденциальности – иногда конфиденциальным может считаться сам факт спора; в других случаях результат может быть обнародован без раскрытия всех деталей.

Благодаря наличию подобных характеристик 82% представителей отрасли, участвовавших в обследовании, который проводил Лондонский университет королевы Марии, выразили уверенность, что в ближайшие годы услуги международного арбитража станут более востребованными (QMUL 2016, 25).

Регуляторные органы осознают, что им предстоит сыграть ключевую роль в создании стимулов для более активного использования арбитража. Так, например, в Соединенном Королевстве регуляторный орган Ofcom обычно принимает к рассмотрению только споры с участием какого-либо оператора, обладающего значительным влиянием на рынке, тогда как для разрешения всех прочих споров применяются альтернативные методы. Ofcom официально приступает к рассмотрению спора только после того, как будет достигнуто согласие по поводу предмета спора, и после представления сторонами заявления о том, что было сделано все возможное для урегулирования спора путем коммерческих переговоров.

Основные выводы

- В качестве альтернативы судебному разбирательству следует разработать официальную процедуру арбитража, в рамках которой будут рассматриваться вопросы конкуренции, присоединения, доступа и тарифов. В некоторых странах спорные вопросы могут сразу передаваться на рассмотрение арбитражного органа, тогда как другие, возможно, предпочтут сначала выносить их на рассмотрение регуляторного органа в области связи. В обоих случаях арбитражу следует рассмотреть апелляции на решения, вынесенные регуляторным органом в области связи.
- Процедуры арбитража особенно важны для развивающихся стран, где суды (и сам регуляторный орган), возможно, хуже разбираются в предмете спора, чем являющиеся его сторонами операторы или поставщики услуг.
- На более крупных и развитых рынках предпочтение, возможно, следует отдавать национальной процедуре арбитражного разбирательства, что означает, что сам арбитраж проводится в соответствии с национальным законодательством и предоставляет сторонам возможность в случае необходимости обжаловать вынесенное решение в местном суде. В случае применения национального арбитража обязательство участвовать в процедуре арбитража должно быть для международных компаний, таких как структуры цифровых платформ, условием для получения доступа к работе в стране.
- В менее крупных и развивающихся странах предпочтение, по всей видимости, будет отдано международному арбитражу; вопрос о его применении легче согласовать с международными компаниями. В этих случаях необходимо позаботиться о том, чтобы место арбитражного разбирательства находилось в стране, подписавшей Нью-Йоркскую конвенцию, – международный договор, предусматривающий взаимность в обеспечении выполнения решений арбитража.

³¹ Более подробную информацию об этом деле см. в тематическом разделе "Отмена судом решения регуляторного органа Нидерландов о совместном доминировании" *Платформы цифрового регулирования*.

2.8 Выдача лицензий и разрешений

История вопроса

Выдача лицензий получила широкое распространение в отрасли электросвязи как рациональный способ подбора поставщиков для рынка, выход на который был сопряжен с большими сложностями, но который сам по себе открывал широкие перспективы для развития конкуренции³². Выдача лицензий ограниченному числу поставщиков дает правительствам возможность привлекать частный сектор к инвестициям в инфраструктуру и услуги. Лицензирование создавало нормативную определенность, необходимую для инвестиций, а также было способом обеспечить достижение целей публичной политики (например, в отношении покрытия сети, качества обслуживания или цен).

Вместе с тем в некоторых странах выдачу лицензий стали считать скорее средством увеличить государственные доходы, в связи с чем начался бурный рост количества лицензий и/или их стоимости (например, разовая плата и лицензионные платежи). Может показаться, что многообразие типов лицензий (и платежей по ним) выгодно для правительства с точки зрения получения доходов, однако оно препятствует конвергенции и подрывает конкуренцию в отрасли. В этих условиях затраты предприятий отрасли резко увеличиваются, а ее структура, как правило, чрезмерно усложняется и дробится.

Тенденции последнего времени

В последние годы растет осознание того, что сложные правила лицензирования и чрезмерно высокие лицензионные платежи тянут отрасль вниз и угрожают цифровой экономике в целом. Дело не только в том, что лицензионные сборы препятствуют потенциальным инвестициям в инфраструктуру; это означает, что отрасли, отличительными чертами которой являются динамизм и экономия за счет масштабов и диверсификации производства, навязывают далекую от оптимальной, статичную структуру рынка. В недавнем отчете GSMA (GSMA 2016, 8) сделан вывод, что "эффективное регулирование требует комплексного подхода, который учитывал бы многообразие всех соответствующих платформ", и что "оно должно способствовать, а не препятствовать экономии за счет масштабов и диверсификации производства, обеспечивающей реальное сокращение расходов потребителей".

Эти соображения дали толчок к движению в сторону открытой конкуренции (в рамках которой лицензирование не требуется) или выдачи общего разрешения (предполагающего равное применение ограниченного свода правил в отношении всех поставщиков услуг, относящихся к определенной категории). Как показано на рисунке 2.5, в большинстве стран по-прежнему применяется лицензирование определенных услуг, однако при этом здесь резко возросло и количество лицензий на несколько услуг и единых лицензий, а в некоторых случаях с появлением некоторых нелицензируемых категорий нужна в выдаче лицензий отпала вовсе³³. Параллельно с этим наблюдается тенденция к упрощению процедуры получения такого разрешения (иногда именуемого лицензией на класс услуг) – зачастую при этом предполагается только прохождение простой процедуры регистрации без уплаты какого-либо лицензионного сбора. В отчете МСЭ "Глобальные регуляторные перспективы в области ИКТ, 2020 год" (ITU 2020b, 26)³⁴ сделан вывод, что применение общего режима выдачи разрешений является одним из ключевых условий для использования потенциала широкополосной связи в полном объеме.

Однако при этом имеют место исключения, в первую очередь в том, что касается лицензирования сетей. В результате конвергенции в секторе ИКТ осталось лишь небольшое число операторов сетей, а некоторые страны и территории в целях экономии за счет масштабов и диверсификации производства и для обеспечения социально-экономической интеграции в общенациональном масштабе вернулись к системе сетевой монополии³⁵.

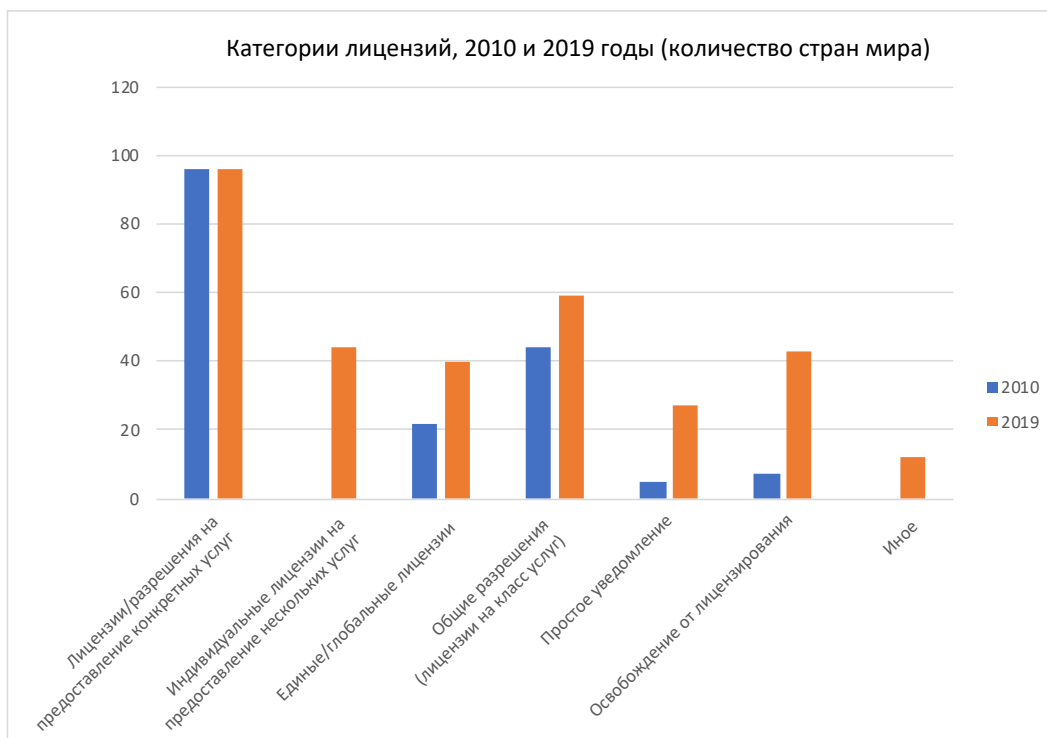
³² Полное описание процесса выдачи лицензий и разрешений см. в Blackman and Srivastava 2011, 63ff. Обсуждение вопроса о категориях и типах лицензий см. в главе 1 "Регуляторное управление и регуляторная независимость".

³³ В дополнение к данным, представленным на рисунке 2.5, в 2019 году 116 стран сообщили о применении безлицензионного режима в отношении устройств для беспроводной широкополосной связи.

³⁴ К числу других ключевых условий относятся открытая конкуренция в сфере услуг и международных шлюзов, совместное использование инфраструктуры, регулирование SMP и иностранное участие/владение.

³⁵ См., например, тематический раздел "Единая интегрированная оптовая широкополосная сеть в Брунее" *Платформы цифрового регулирования*.

Рисунок 2.5. Тенденция к переходу на единые лицензии/общие разрешения



Источник: МСЭ.

Основные выводы

- Целью лицензирования является обеспечение результативного и эффективного оказания услуг ИКТ.
- Оптимальная структура лицензирования и условия лицензий в разных странах будут отличаться, однако во главу угла никогда не следует ставить извлечение максимальной прибыли.
- Предпочтение следует отдавать общим разрешениям, а сборы устанавливать на максимально низком уровне, только для покрытия административных расходов, чтобы не создавать препятствий для инвестиций и инноваций, а также повышать ценовую доступность для потребителей.
- В случае выдачи индивидуальных лицензий операторам, имеющим собственное оборудование, количество таких лицензий должно быть ограничено во избежание ненужного дублирования инвестиций, однако предоставлять их следует на условиях, обеспечивающих открытый доступ к ключевой инфраструктуре на справедливых и разумных условиях³⁶, способствуя тем самым формированию здорового конкурентного рынка услуг.
- Держателям лицензий следует также разрешать совместно использовать инфраструктуру и проводить слияния, руководствуясь лишь учетом вопросов политики в области конкуренции.

2.9 Слияния и поглощения

История вопроса

Слияния и поглощения (M&A) представляют собой неотъемлемую составную часть нормально функционирующего конкурентного рынка. Способы безболезненного ухода с рынка для его действующих участников важны не в меньшей степени, чем преодоление барьеров, препятствующих выходу на него.

Регуляторные органы оспаривают операции в сфере M&A лишь в том случае, если их следствием оказывается существенное ослабление конкуренции (СОК): как правило, это может случиться, если

³⁶ См., например, тематические разделы "Сеть Red Compartida, Мексика" и "Единая интегрированная оптово-широкополосная сеть в Бразилии" *Платформы цифрового регулирования*.

поставщик, обладающий значительным влиянием на рынке, приобретает конкурирующую компанию или если две небольшие конкурирующие компании сливаются, в результате чего возникает компания-поставщик, способная оказывать значительное влияние на рынок. Вместе с тем проверка в отношении СОК дает лишь гипотетические результаты и сложна в проведении, поскольку она предусматривает оценку будущей конкурентоспособности рынка при двух возможных сценариях – с проведением слияния и без него, а затем – определение, насколько значительными являются различия.

Эффективная практика предполагает утверждение всех слияний, отвечающих определенным пороговым критериям, соответствующими компетентными органами (например, национальной комиссией по вопросам конкуренции, если таковая существует, в сотрудничестве с регуляторным органом в области ИКТ). Так, например, в Соединенном Королевстве слияние обычно становится предметом рассмотрения в Управлении по вопросам конкуренции и рынков (СМА) в том случае, если оборот компании – участника этой сделки в Соединенном Королевстве превышает 70 млн. фунтов стерлингов (примерно 86 млн. долл. США) или если совокупная доля рынка компаний – участников сделки превышает 25%. Подобные критерии установлены для того, чтобы в дальнейшем не пришлось отменять сделку, – сделать это гораздо сложнее, чем просто изначально предупредить слияние или поглощение.

Тенденции последнего времени

Слияния лицензируемых операторов сетей стали широко распространенным явлением, поскольку компании стремятся расширить масштабы деятельности, обеспечить универсальное покрытие и привлечь инвестиции в сети 4G/5G и оптоволоконные сети. В результате возникают основания для беспокойства по поводу концентрации, олигополистических рынков и совместного доминирования.

Крупнейшие цифровые платформы (такие, как Google, Facebook и Amazon) часто поглощали менее крупных конкурентов (таких, как YouTube, WhatsApp, Instagram), чтобы сохранить свое доминирующее положение на рынке³⁷. Цена приобретения нередко превышала уровень рыночной капитализации. Крупные платформы, прежде всего Amazon, осуществляют вертикальную интеграцию как вверх, так и вниз по цепочке поставок (или стоимости), чтобы иметь возможность конкурировать с поставщиками и клиентами и использовать доминирующее положение на новых рынках. Постепенно подобные действия привели к "окаменению" цифровых рынков, создавая вокруг крупных компаний "мертвую зону", в которой вновь выходящие на рынок компании не имели шансов на выживание.

Проверка в отношении СОК уже не позволяет точно определить, следует ли регуляторному органу вмешиваться в сделку М&А³⁸. Как правило, сделки М&А, которые проводят поставщики цифровых платформ, легко проходят тест на СОК (такие сделки способствуют лишь увеличению рыночной доли компании-приобретателя), но при этом они делают невозможным для любой вновь создаваемой компании увеличение до масштабов, позволяющих соперничать с компанией-приобретателем в плане сетевых эффектов. Здесь требуются новые подходы. Такие подходы, в частности, должны учитывать влияние на рынке с точки зрения не только доходов и количества абонентов, но и доступа к данным потребителей и алгоритмов, необходимых для анализа и использования таких данных, в том числе, возможно, в целях недопущения конкуренции.

Основные выводы

- Нормативно-правовая база нуждается в модернизации, которая расширила бы круг полномочий в отношении предупреждения и выдачи разрешений на М&А (как это, например, было недавно сделано в Германии³⁹).
- Для проведения новых видов анализа М&А регуляторный орган должен иметь необходимое кадровое обеспечение – с точки зрения как количества сотрудников, так и уровня их квалификации.
- Если согласие на проведение М&А может быть дано лишь на определенных условиях, такие условия должны быть выполнены до проведения слияния или поглощения.

³⁷ См. тематический раздел "Деятельность поставщиков крупнейших цифровых платформ в сфере М&А" *Платформы цифрового регулирования*.

³⁸ См. анализ недавнего примера из практики в тематическом разделе "Операционное слияние Vodafone/TPG – тест на СОК более не дает достоверных результатов" *Платформы цифрового регулирования*.

³⁹ См. тематический раздел "Германия корректирует свой подход к регулированию М&А" *Платформы цифрового регулирования*.

- Антимонопольный орган должен иметь возможность не только налагать штрафы (которые зачастую воспринимаются как часть расходов на ведение бизнеса), но и предъявлять более широкий спектр других условий (которыми нельзя просто пренебречь).
- К анализу M&A необходимо привлекать структуры, представляющие все затрагиваемые отрасли экономики, чтобы решение регуляторного органа полностью учитывало последствия M&A для рынков и потребителей.
- По умолчанию итогом антимонопольного расследования (поводом для проведения которого является достижение соответствующих пороговых показателей) должно быть решение о блокировке сделки M&A, если только не будет доказано, что она в долгосрочной перспективе отвечает интересам потребителей.

2.10 Налогообложение

История вопроса

Смысл налогообложения корпораций состоит в обеспечении того, чтобы все компании вносили справедливый вклад в оплату общественных услуг, которыми они пользуются (как это делают резиденты, уплачивая налоги на доходы и на потребление). По традиции налогом обычно облагалась прибыль корпораций.

Налоговая нагрузка компаний электросвязи, особенно операторов сетей подвижной связи, часто гораздо выше, особенно в развивающихся странах. К числу отраслевых налогов относятся акцизы, налог на добавленную стоимость (НДС) по повышенной ставке, лицензионные платежи, сборы за использование спектра и обязательства по универсальному обслуживанию. Исследование налогообложения сферы подвижной связи, которое GSMA провела в 2017 году, показало, что налоги, которые платят потребители и предприятия сферы подвижной связи, составляли 22% выручки от операций на рынке и что почти треть этих платежей составляют отраслевые налоги (GSMA 2019, 5). Полная информация о ситуации с налогообложением ИКТ представлена на рисунке 2.6.

Основанием для подобной системы налогообложения зачастую является то обстоятельство, что операторы сетей подвижной связи успешнее собирают облагаемую налогом выручку, нежели государство – прямые налоги. Для многих развивающихся стран это, по всей видимости, верно, однако непредвиденным последствием при этом становится ценовая недоступность интернета для многих пользователей по всему миру, в результате чего некоторые экономические и социальные блага цифровой экономики оказываются нереализованными. В отчете МСЭ (ITU 2015, 5) был сделан вывод, что политику в сфере налогообложения необходимо "разрабатывать исходя из учитывающих особенности каждой страны политических компромиссов между наполнением бюджета и возможными негативными последствиями для развития цифровой отрасли и для рыночной среды в отраслях электросвязи/ИКТ". Однако, как совсем недавно – в 2019 году – сообщила Комиссия по широкополосной связи в интересах устойчивого развития (Broadband Commission for Sustainable Development 2019, 63), "хотя вопросам ценовой доступности товаров и услуг ИКТ и роли налогообложения в повышении такой доступности стало уделяться больше внимания, в некоторых случаях наблюдался заметный рост отраслевых налогов, влияющий на внедрение и использование услуг подключения".

Рисунок 2.6. Виды налогов, применяемых в секторе ИКТ, общемировые показатели (проценты), 2019 год

Вид налога	Объект налогообложения										
	Услуги по передаче контента	Услуги приема межд. входящих голосовых вызовов	Межд. услуги передачи данных	Межд. мобильный роуминг	Услуги интернета	Нац. услуги передачи данных	Нац. мобильный роуминг	Нац. услуги голосовой связи	ОТТ-услуги по предоставлению контента	Услуги межд. исходящих голосовых вызовов (IDD)	Карточки для оплаты услуг подвижной связи
НДС	0–27%	0–27%	0–27%	0–27%	0–25%	0–25%	0–27%	0–27%	0–27%	0–27%	0–27%
Отраслевой налог	0,1–17%	0,1–15%	0,1–13%	0,1–49,77%	0,1–40%	0,1–40%	0,1–26%	0,1–49,77%	1,5–13%	0–40%	0,1–49,77%
Налог с продаж	3–35%	0–27%	1,5–27%	4–27%	3–35%	1,5–35%	3–27%	1,5–35%	5–25%	3–27%	3,65–35%
Импортные пошлины	5–40,55%	5–40,55%	5–40,55%	5–15%	5–40,55%	5–15%	5–15%	5–15%	7,7–15%	5–15%	5–25%

Примечание. – Межд. – международный, нац. – национальный.

Источник: МСЭ.

Тенденции последнего времени

Возможно, установление более высоких налогов на подвижную связь или интернет было оправданно тогда, когда подобные услуги были премиальными и доступными только зажиточным категориям населения. Собираемые таким образом налоги можно было рассматривать как подлежащие перераспределению. Однако сегодня, когда особое внимание уделяется обеспечению универсального и приемлемого по цене доступа, все это теряет смысл.

В ситуации, когда основная часть трафика и доходов приходится на поставщиков услуг ОТТ и приложения, предоставляемые через цифровые платформы, налогообложение традиционных услуг, прежде всего подвижной связи, деформирует рынок, а налоги и сборы с ИКТ в целом снижают ценовую доступность интернета и усиливают цифровое неравенство. Дополнительные сборы с конечных пользователей за услуги ОТТ, введенные, например, в некоторых странах Африки, не достигают поставленных целей, поскольку налогообложение пользователей, как правило, ведет к снижению ценовой доступности интернета и падению спроса, что в результате сокращает ВВП и налоговые поступления в целом.

Транснациональные цифровые платформы зачастую платят гораздо меньшие налоги, нежели национальные компании, — они пользуются методами размывания налоговой базы и вывода доходов из-под налогообложения (BEPS), позволяющими платить налоги там, где они ниже, а не там, где в действительности ведется экономическая деятельность. Многосторонние усилия, прилагаемые, в частности, Организацией экономического сотрудничества и развития (ОЭСР), и односторонние действия ряда государств (в частности, Франции, Индии) направлены на установление более справедливых правил налогообложения цифровых платформ, с тем чтобы за его основу принимались доходы, полученные в стране, или прибыль, пропорциональная доходам, полученным платформой в каждой из стран⁴⁰. Другими важными отличительными чертами здесь являются простота и предсказуемость.

Как отмечается в отчете *Глобальные регуляторные перспективы в области ИКТ* (ITU 2018b), налогообложение цифровой экономики является проблемой для всего мира, и для ее решения применяются разные подходы. Правительствам необходимо укреплять сотрудничество на региональном и международном уровнях в вопросах налогообложения цифровых услуг и не следует в погоне за сиюминутной прибылью ставить под угрозу экономическую выгоду в долгосрочной перспективе. Кроме того, поскольку решения по вопросам налогообложения чаще принимают министерства финансов и налоговые органы, нежели руководящие органы в сфере ИКТ, целесообразно создавать эффективные механизмы совместного регулирования, позволяющие, например, выслушать мнения всех сторон, прежде чем принимать решения.

⁴⁰ Подробнее об этих тенденциях см. тематический раздел "Односторонние и двусторонние подходы к решению проблемы BEPS" *Платформы цифрового регулирования*.

Основные выводы

- Налогообложение цифровых платформ и услуг исходя из их выручки (а не прибыли) экономически целесообразно в силу значительного воздействия внешних сетевых факторов и поскольку выручка не подпадает под действие политики внутреннего трансфертного ценообразования.
- Уровень налогообложения не должен препятствовать универсальному доступу к приемлемым в ценовом отношении цифровым услугам: налоги на основе выручки следует снижать, например, в тех случаях, когда поставщик услуг осуществляет инвестиции в стране (например, путем развертывания инфраструктуры, обеспечения охвата сельских и отдаленных районов и создания новых рабочих мест).
- На национальном уровне правительствам следует проводить политику, которая (ITU 2018b):
 - способствовала бы созданию сбалансированной системы налогообложения и гармонизации налогов;
 - не была бы чрезмерно обременительной для всех заинтересованных сторон;
 - поощряла бы инновации и реальную конкуренцию всех участников цифровой экосистемы; и
 - ставила бы во главу угла обеспечение ценовой доступности.

Справочные материалы

- A4AI (Alliance for Affordable Internet). 2018. *2018 Affordability Report*. Washington, DC: A4AI. https://a4ai.org/affordability-report/report/2018/#executive_summary
- BEREC (Body of European Regulators for Electronic Communications). 2016. *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*. Brussels: BEREC. 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
- Blackman, Colin and Lara Srivastava, eds. 2011. *Telecommunications Regulation Handbook: Tenth Anniversary Edition*. Washington, DC: World Bank and Geneva: International Telecommunication Union. <https://www.itu.int/pub/D-PREF-TRH.1-2011>
- Broadband Commission for Sustainable Development. 2019. *State of Broadband Report 2019*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf
- Bruce, Robert R., Rory Macmillan, Timothy St. J. Ellam, Hank Intven, and Theresa Miedema. 2004. *Dispute Resolution in the Telecommunications Sector*. Discussion Paper. Geneva: International Telecommunication Union and Washington, DC: World Bank. https://www.itu.int/ITU-D/treg/publications/ITU_WB_Dispute_Res-E.pdf
- Cave, Martin. 2006. "Encouraging Infrastructure Competition via the Ladder of Investment". *Telecommunications Policy* 30 (3-4). <https://doi.org/10.1016/j.telpol.2005.09.001>
- Digicel. 2019. "OTTs and Network Infrastructure". A contribution to ITU-D Study Groups, Question 3/1 and Question 4/1 joint session on the Economic Impact of OTTs on National Telecommunication/ICT Markets, October 2019. https://www.itu.int/dms_pub/itu-d/oth/07/1a/D071A0000030001PDFE.pdf
- EU (European Union). 2015. Regulation 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access, 25 November 2015. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=en>
- FCC (Federal Communications Commission). 2015. Open Internet Order 15-24. <https://www.fcc.gov/document/fcc-releases-open-internet-order>
- FCC (Federal Communications Commission). 2018. Restoring Internet Freedom Order. <https://www.fcc.gov/restoring-internet-freedom>
- GSMA. 2016. *A New Regulatory Framework for the Digital Ecosystem*. London: GSMA. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/NERA_Full_Report.pdf
- ITU (International Telecommunication Union). 2015. *The Impact of Taxation on the Digital Economy*. GSR15 Discussion Paper. Geneva: ITU. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR16_Discussion-Paper_Taxation_Latest_web.pdf
- МСЭ (Международный союз электросвязи). 2016. *Принципы определения рынков и выявления операторов, обладающих значительным влиянием на рынке*. Рекомендация МСЭ-T D.261, октябрь. <https://www.itu.int/rec/T-REC-D.261-201610-I/en>
- ITU (International Telecommunication Union). 2018a. "Competition Analysis in Digital Application Environment", Session 11, Regulating Two-sided Markets". ITU Asia-Pacific Centre of Excellence, September 2018.
- ITU (International Telecommunication Union). 2018b. *Global ICT Regulatory Outlook 2018*. Geneva: ITU. <https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Outlook/2018.aspx>
- МСЭ (Международный союз электросвязи). 2018с. *Руководящие указания ГСР-18 на основе примеров передового опыта, касающиеся новых границ регулирования для обеспечения цифровой трансформации*. Женева: МСЭ. https://www.itu.int/net4/ITU-D/CDS/GSR/2018/documents/Guidelines/GSR-18_BPG_Final-R.PDF

- ITU (International Telecommunication Union). 2019a. ICT Infrastructure Business Planning Toolkit. Geneva: ITU. <http://handle.itu.int/11.1002/pub/813e6d7f-en>
- ITU (International Telecommunication Union). 2019b. "Costing and Pricing Methodologies in the Digital Economy". ITU, Regional Economic Dialogue on Information and Communications Technologies in Europe and CIS, Odessa, October 2019. ITU, 2020a. Economic Impact of OTTs on National Telecommunication/ ICT Markets. ITU-D Study Group 1 report, February. Geneva: ITU.
- ITU (International Telecommunication Union). 2020b. Global ICT Regulatory Outlook 2020: Pointing the Way Forward to Collaborative Regulation. Geneva: ITU. https://www.itu.int/pub/D-PREF-BB.REG_OUT01
- QMUL (Queen Mary University of London). 2016. *Pre-empting and Resolving Technology, Media and Telecoms Disputes. International Dispute Resolution Survey*. London: Queen Mary University of London. http://www.arbitration.qmul.ac.uk/media/arbitration/docs/Fixing_Tech_report_online_singles.pdf
- Rogerson, David, Pedro Seixas and Jim Holmes, *Net Neutrality*, Australian Journal of Telecommunications and the Digital Economy, November 2016. <https://telsoc.org/journal/ajtde-v4-n4/a79>
- WTO (World Trade Organisation). 1996. *Telecommunications Services: Reference Paper*. Negotiating Group on Basic Telecommunications, World Trade Organization, April 24, 1996, https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

Глава 3. Доступ для всех



3.1 Введение

Цифровые технологии занимают все более важное место в жизни людей, изменяя наш образ жизни, работы и развлечений и создавая новые возможности для социально-экономического развития. Компании, в свою очередь, используют информационно-коммуникационные технологии (ИКТ) для коренного преобразования своих процессов, повышения эффективности, разработки новых изделий и повышения качества обслуживания клиентов. Однако переход к цифровой экономике может еще больше увеличить цифровой разрыв между теми, кто имеет возможность получать пользу от цифровой трансформации, и теми, кому она недоступна, поскольку они либо относятся к социально и экономически незащищенным группам населения, либо проживают в районах, где отсутствует доступ к цифровым технологиям, услугам и возможностям.

Одним из ключевых условий для того, чтобы каждый человек, где бы он ни находился, мог пользоваться всеми преимуществами цифровой трансформации, является универсальный доступ (UA) к ИКТ, в том числе доступ к широкополосным сетям, устройствам и цифровым услугам. Это еще и жизненно важное средство связи в чрезвычайных ситуациях, таких как пандемия COVID-19, обеспечивающее доступ к основным коммерческим и государственным услугам, а также возможность общения с друзьями и родственниками, удаленной работы, получения медицинской помощи и образования. Следовательно, в соответствии с целью 9с Целей Организации Объединенных Наций в области устойчивого развития и целевыми показателями Комиссии по широкополосной связи в интересах устойчивого развития (см. вставку 3.1) эффективная политика в области универсального доступа должна обеспечивать доступ к недорогим и качественным услугам широкополосной связи и способствовать всеобщему охвату цифровыми технологиями, включая развитие цифровых навыков, доступ для женщин и лиц с ограниченными возможностями, а также наличие соответствующего контента и приложений (United Nations 2015, 9с).

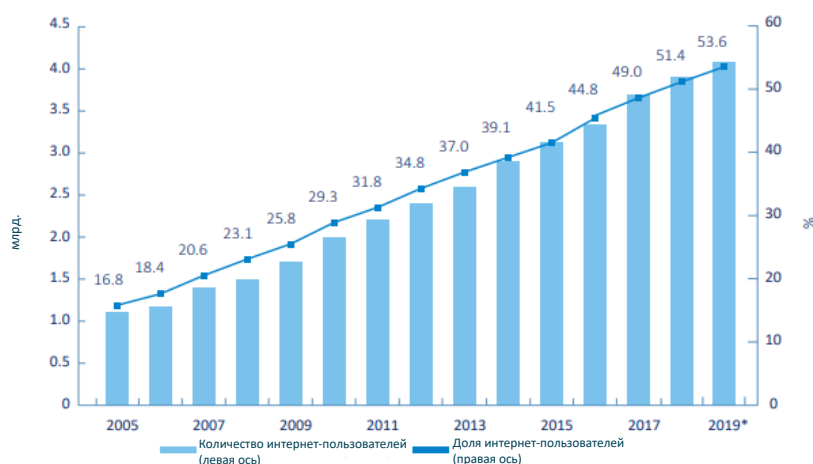
Вставка 3.1. Целевые показатели Комиссии по широкополосной связи в интересах устойчивого развития на период до 2025 года

К 2025 году

1. Все страны должны разработать общегосударственный план или общегосударственную стратегию по обеспечению широкополосной связи либо включить понятие широкополосной связи в свои определения универсального доступа и обслуживания (УДО).
2. Базовые услуги широкополосной связи в развивающихся странах должны стать приемлемыми в ценовом отношении, то есть стоимость таких услуг должна составлять менее 2% от ежемесячного валового национального дохода (ВНД) на душу населения.
3. Уровень проникновения пользователей широкополосного доступа в интернет должен достичь а) 75% во всем мире, б) 65% в развивающихся странах и с) 35% в наименее развитых странах.
4. 60% молодежи и взрослых должны иметь по меньшей мере минимальный уровень владения устойчивыми цифровыми навыками.
5. 40% населения мира должны пользоваться цифровыми финансовыми услугами.
6. В каждом секторе экономики сократить на 50% число микро-, малых и средних предприятий (ММСП), не имеющих интернет-соединения.
7. Должно быть достигнуто гендерное равенство по всем целевым показателям.

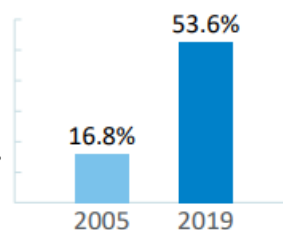
Организация Объединенных Наций отмечает, что несмотря на постоянный прогресс в достижении этих целей около 90% населения мира проживают в пределах зоны действия сетей подвижной связи 3G (ITU 2019, 8), а по оценке Международного союза электросвязи (МСЭ) количество интернет-пользователей в период с 2005 по 2019 год росло в среднем на 10% в год (ITU 2019) и свыше 3,6 млрд. человек, или около 46% населения мира, все еще не пользуются интернетом. Однако что еще более тревожно, в последние годы темпы роста использования интернета ввиду насыщения рынка замедлились (см. рисунок 3.1) (ITU 2019).

Рисунок 3.1. Количество физических лиц, пользующихся интернетом, и темпы роста этого показателя





По оценкам, в 2019 году интернетом пользовались 4,1 млрд. человек, что на 5,3% больше, чем в 2018 году.



Среднемировой уровень проникновения вырос с примерно 17% в 2005 году до более чем 53% в 2019 году.



В период с 2005 по 2019 год количество интернет-пользователей росло в среднем на 10% в год.



Однако в последние годы среднемировые темпы роста не так высоки, как 10 лет назад, потому что в некоторых частях мира достигается уровень насыщения.

Источник: ITU 2019.

При изучении различий в использовании интернета между странами, сгруппированными по уровню доходов, очевиден сохраняющийся, хотя и сокращающийся цифровой разрыв. В 2009 году соотношение между количеством интернет-пользователей в развитых и развивающихся странах составляло 3,6 : 1, а в 2019 году этот показатель сократился до 1,8 : 1. Однако темпы роста в развивающихся странах за последние годы значительно снизились. При нынешних темпах замедления роста развивающимся странам вряд ли удастся достичь к 2025 году установленного Комиссией по широкополосной связи в интересах устойчивого развития целевого показателя проникновения пользователей широкополосного доступа в 65%. Это подтверждает необходимость переоценки политики и подходов, применяемых в настоящее время для достижения целей по универсальному доступу и указанных целевых показателей.

В настоящей главе обсуждаются ключевые проблемы и политика в отношении достижения целей по универсальному доступу в контексте цифровой трансформации. Обсуждение сосредоточено на трех темах:

- обеспечение возможности установления соединений, то есть решение проблем, связанных с финансированием расширения инфраструктуры широкополосной связи;
- ценообразование, направленное на устранение барьеров для приемлемости в ценовом отношении цифровых услуг и устройств для конечных пользователей; а также
- охват цифровыми технологиями, который включает политику по развитию цифровых навыков, меры по устранению гендерного неравенства и обеспечению доступности услуг для лиц с ограниченными возможностями и способствует созданию местного цифрового контента.

Кроме того, в данной главе обсуждается необходимость введения контроля и оценки политики в области универсального доступа для обеспечения принятия решений на основе фактических данных и оперативного выявления и исправления ошибок регулирования¹.

3.2 Препятствия на пути к достижению универсального доступа к услугам широкополосной связи и цифровым услугам

Важнейшую роль в расширении доступа к услугам широкополосной связи и цифровым услугам в развивающихся странах, особенно с использованием технологий подвижной связи и других инновационных беспроводных технологий, играют частные инвестиции. Ответственность за реализацию политики,

¹ Более подробное рассмотрение тем, затронутых в данной главе, см. в соответствующих тематических разделах *Платформы цифрового регулирования*.

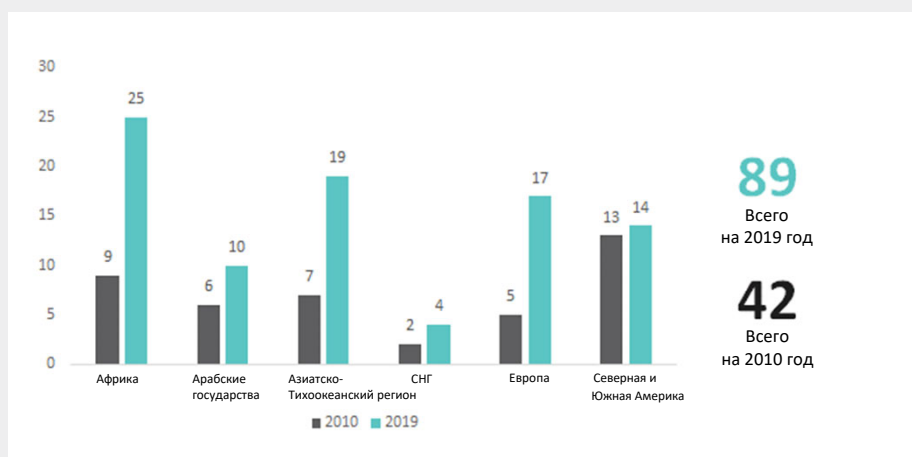
стимулирующей инвестиции и использование новых технологий и бизнес-моделей, несут директивные и регуляторные органы (см. вставку 3.2).

Однако для распространения услуг широкополосной связи и цифровых услуг на некоторые районы (например, удаленные сельские районы) или группы населения (например, группы с низким уровнем доходов) одних коммерческих усилий участников рынка недостаточно. Для решения этой проблемы требуются узкоспециализированная и целенаправленная политика в области универсального доступа. В данном разделе кратко излагаются основные проблемы, с которыми сталкиваются директивные органы в деле обеспечения универсального доступа. В развивающихся странах, где имеются серьезные ограничительные факторы в финансовой, социально-экономической сфере и сфере образования, в национальных цифровых стратегиях упор должен быть сделан на использовании многосекторального коллективного подхода к решению проблем универсального доступа, таких как доступность, приемлемость в ценовом отношении, наличие навыков и распространение услуг.

Вставка 3.2. Эволюция политики в области универсального доступа и обслуживания

Политика в области универсального доступа и обслуживания (УДО) традиционно была ориентирована на базовые услуги голосовой связи, особенно на более развитых рынках. Но за последнее десятилетие политика и стратегии расширились и стали охватывать доступ в интернет, в частности широкополосный доступ. В период с 2010 по 2019 год количество стран, включивших широкополосный доступ в политику в области УДО, увеличилось более чем вдвое – с 42 до 89 стран. В 2019 году их доля составила около 60% всех стран, сообщивших о принятии политики в области УДО. В некоторых развивающихся регионах эта тенденция выражена сильнее – в настоящее время около 70% стран Африки и Азиатско-Тихоокеанского региона включают в определение УДО услуги широкополосного доступа. Кроме того, несколько стран, а также Организация Объединенных Наций объявили доступ в интернет всеобщим правом (United Nations 2016).

Рисунок 3.2. Количество стран, в которых в определение УДО включен широкополосный доступ



Источник: ITU 2020.

Для преодоления цифрового разрыва, определяемого как "разрыв между отдельными лицами, домашними хозяйствами, коммерческими предприятиями и географическими районами на различных социально-экономических уровнях в плане их возможностей доступа к информационно-коммуникационным технологиям (ИКТ) и использования ими интернета для самых различных видов деятельности" (United Nations 2018, 2), требуется специальная политика и стратегии, способные решить проблемы, перечисленные в таблице 3.1.

Таблица 3.1. Ключевые проблемы универсального доступа, с которыми сталкиваются развивающиеся страны

	Проблема	Описание	Ключевая политика/деятельность
Возможность установления соединений	Наличие	Ограниченные источники финансирования для развертывания инфраструктуры широкополосного доступа Ограниченное наличие инфраструктуры во всей цепочке создания стоимости широкополосного доступа	Модернизация или создание эффективных фондов универсального доступа и обслуживания (ФУДО) для направления средств в нерентабельные области и программы Использование государственного финансирования, помощи на цели развития или государственных инициатив и нормативных стимулов для охвата недорогими услугами широкополосной связи недостаточно обслуживаемых районов и групп населения (например, обязательства по подключению в рамках лицензий на использование спектра; доступ к спектру в обмен на развертывание инфраструктуры или совместное использование инфраструктуры) Заключение контрактных соглашений (например, создание государственно-частных партнерств (PPP)) или применение таких механизмов, как "плати или играй", для совместного финансирования развертывания цифровой инфраструктуры Обеспечение возможности использования инновационных бизнес-моделей, альтернативных технологий (например, спутников, БПЛА/аэростатов, Wi-Fi) Содействие межотраслевому развертыванию инфраструктуры (например, транспортной, нефтегазовой, электроэнергетической отраслей) и совместному использованию инфраструктуры (пассивному и активному) Обеспечение разумных сборов и налогов с поставщиков услуг ИКТ (включая плату за использование спектра) и адекватного баланса между сбором государственных доходов и возможностью развития цифровых услуг
	Приемлемость в ценовом отношении	Низкая покупательная способность в сочетании с высокими ценами на услуги и устройства для конечных пользователей	Целенаправленная политика, субсидии, рассрочка платежей и спонсируемый доступ к данным для повышения ценовой доступности цифровых услуг и устройств для конечных пользователей среди уязвимых групп населения Развитие бесплатных пунктов общего доступа в интернет, таких как центры цифрового доступа в школах, библиотеках, почтовых отделениях и общедоступные сети Wi-Fi Снижение импортных пошлин и других налогов, применяемых к устройствам для конечных пользователей

Таблица 3.1. Ключевые проблемы универсального доступа, с которыми сталкиваются развивающиеся страны (продолжение)

	Проблема	Описание	Ключевая политика/деятельность
Интеграция	Доступность	Возможность использования цифровых услуг и технологий независимо от уровня образования, ограниченных возможностей, возраста, пола и других факторов	Разработка планов стимулирования спроса, ориентированных на женщин и девушек, а также на лиц с ограниченными возможностями
	Навыки и умения	Отсутствие необходимых цифровых навыков и цифровой грамотности	Реализация инициатив по обучению цифровым навыкам и программ непрерывного обучения
	Релевантность	Ограниченная осведомленность о возможностях и преимуществах ИКТ Ограниченная доступность соответствующего контента и услуг на местных языках	Содействие внедрению ИКТ на государственном уровне и развертыванию услуг и приложений электронного правительства (включая электронное здравоохранение и электронное образование) Разработка политики содействия развитию местной индустрии цифрового контента и созданию цифрового контента

3.3 Политика содействия обеспечению универсального доступа к услугам широкополосной связи и цифровым услугам

Политика в области универсального доступа включает не только возможность установления соединений, но и меры по обеспечению приемлемости в ценовом отношении и охвата цифровыми технологиями. Средства, с помощью которых государство, частный сектор, неправительственные организации и международные органы могут эффективно на основе сотрудничества достичь этих целей, напрямую связаны с такими параметрами, как плотность населения, уровень дохода, географические особенности, политические и экономические характеристики, доступные ресурсы и др. В зависимости от этих параметров страны применяют разные подходы к устранению разрыва в доступе. Кроме того, в некоторых случаях, например в Кении, универсальный доступ включен в стратегию цифрового развития страны (Republic of Kenya 2019). В данном разделе рассматриваются политика в области универсального доступа и соответствующие подходы, принятые в разных странах.

Политика финансирования универсального доступа: решение проблем доступности

Механизмы финансирования для достижения целей универсального доступа – это ключевой вопрос обеспечения услуг широкополосной связи и цифровых услуг. Традиционно для достижения целей универсального доступа государство во многих случаях использует в качестве механизма финансирования последней инстанции фонды универсального доступа и обслуживания (ФУДО). Однако в последние несколько лет вследствие финансовых, операционных и других проблем появились альтернативные источники и стратегии финансирования. Эти подходы, вместе взятые, могут использоваться для гарантирования того, что политика в области универсального доступа лучше подходит для обеспечения возможности установления соединений, надлежащей инфраструктуры, приемлемости в ценовом отношении, развития цифровых навыков и охвата традиционно маргинализированных групп населения.

Ниже рассмотрены основные варианты финансирования:

- фонды универсального доступа и обслуживания;
- стратегии дополнительного финансирования;
- дополнительное прямое государственное финансирование или совместное государственное и частное финансирование;

- эффективные меры регулирования;
- политика "плати или играй".

Фонды универсального доступа и обслуживания

ФУДО – это механизмы финансирования, создаваемые государством для содействия универсальному доступу к услугам электросвязи. Они обеспечивают финансовую заинтересованность операторов услуг электросвязи в предоставлении услуг в тех местах, где в противном случае они были бы коммерчески нецелесообразны (UN ESCAP 2017, 10). Традиционно государство выделяло субсидии на конкретные услуги (например, услуги таксофонов фиксированной телефонной связи). Однако в последнее время произошел сдвиг в сторону конкуренции за субсидии ФУДО независимо от вида услуг (например, услуг фиксированной или подвижной связи), равно как и от вида технологий. Кроме того, по мнению Экономической комиссии для Латинской Америки и Карибского бассейна (ЭКЛАК), ФУДО является ценным ресурсом, который можно использовать для финансирования программ помощи лицам с ограниченными возможностями в странах Карибского бассейна (Bleeker 2019), что в равной степени справедливо и для других уязвимых групп населения и в других регионах. Точно так же в чрезвычайных ситуациях, таких как пандемия COVID-19, ФУДО считается средством краткосрочного финансирования сетей при временном сокращении их пропускной способности, а также поддержания сетей в рабочем состоянии (Broadband Commission for Sustainable Development 2020²).

Решающее значение для стран имеет смещение акцента с услуг голосовой связи в сторону широкополосных соединений, обеспечения приемлемости в ценовом отношении и охвата цифровыми технологиями. Но для обеспечения гибкости ФУДО в целях поддержки инициатив и программ по реализации стратегий широкополосной связи требуется внесение изменений в нормативно-правовые акты (Alliance for Affordable Internet 2015, 17).

Анализ успешных ФУДО показывает, что для достижения целей универсального доступа необходимо удовлетворение определенных требований к возможностям фондов. ФУДО выполняет многие из функций финансового учреждения. Он управляет крупными капитальными активами, оценивает и определяет проекты с точки зрения инвестиционных возможностей, а также предоставляет финансирование подрядчикам-исполнителям, чью работу необходимо контролировать и оценивать, чтобы гарантировать рациональное использование ресурсов ФУДО. В число необходимых требований входят:

- политика и параметры, в которые можно быстро и эффективно вносить изменения с учетом потребностей новой концепции ФУДО и в ответ на быстро меняющиеся и развивающиеся приоритеты;
- четко сформулированные политика и концепция;
- прозрачность, наглядность и подотчетность;
- подробные правила в отношении процесса выделения средств и прав на их получение;
- наращивание потенциала, устойчивость и дополнительные услуги;
- наличие ресурсов и знаний;
- регуляторные органы как партнеры в области развития и социальной интеграции;
- автономные ФУДО в плане административного бюджетирования и распределения ресурсов.

Тем не менее ФУДО сталкиваются с четко документированными проблемами. К ним относятся, в частности, недостаточная прозрачность процессов распределения ресурсов, недостаточный объем или невыплата собранных средств, нередко отсутствие связи между сбором средств и фактическими потребностями в финансировании/субсидировании услуг, политическое вмешательство и отсутствие должным образом подготовленного персонала (GSMA 2013, 261–262). В будущем для эффективного функционирования ФУДО потребуются выявление и решение таких проблем, если они возникнут (см. вставку 3.3).

² Кризис COVID-19. Программа действий Комиссии по широкополосной связи – более оперативное и более эффективное восстановление. <https://www.broadbandcommission.org/COVID19/Pages/default.aspx>

Вставка 3.3. Примеры эффективных ФУДО

Недавними примерами успешных ФУДО могут служить фонды Коста-Рики, Нигерии и Пакистана. Эти страны обрели надлежащую возможность управления фондами, эффективно используют инвестиции ФУДО и достигли целевых показателей доступа к ИКТ (Alliance for Affordable Internet 2015, 9).

- В 2015 году Коста-Рика приступила к осуществлению программы CR Digital. Эта национальная программа была рассчитана на то, чтобы в течение двух лет обеспечить подключение к интернету всей страны. Хотя в указанный период эта цель не была достигнута, к 2018 году доступ в интернет получили еще 40 тыс. семей и 400 сельских школ. Кроме того, 95% домохозяйств, охваченных на сегодняшний день, возглавляют женщины (Alliance for Affordable Internet 2020).
- Фонд универсального обслуживания (USPF) Нигерии профинансировал сотни новых базовых станций, школ – центров знаний и общинных информационных центров, волоконно-оптическую магистральную сеть, межуниверситетскую линию связи и программы электронного здравоохранения и электронной доступности (Alliance for Affordable Internet 2015, 15^a).
- В 2007 году в Пакистане был учрежден автономный Фонд универсального обслуживания, которым управляет независимая государственная компания (Alliance for Affordable Internet 2015, 9^b). Этот фонд ориентирован на базовые услуги электросвязи и передовые услуги, включая широкополосный доступ. К 2013 году фонд профинансировал обеспечение доступа в интернет почти в 300 ранее не обслуживаемых городах и 1100 средних школах, колледжах и библиотеках.

Примечание. – а. См. Universal Service Provision Fund, <http://www.uspf.gov.ng/>; b. См. Universal Service Fund, <http://www.usf.org.pk/>.

Альтернативные подходы к финансированию инфраструктуры широкополосной связи

По всему миру также реализуются стратегии дополнительного финансирования для достижения целей универсального доступа. Эти стратегии имеют целью улучшение экономических показателей или снижение стоимости проектов, направленных на развертывание инфраструктуры для достижения целей универсального доступа, которые в противном случае могут оказаться нерентабельными. Например, они могут включать фискальные меры, такие как стимулирующая политика регулирования налогообложения, тарифов, импорта и бизнеса, направленная на снижение рисков и финансового бремени и обеспечение стимулов для инвесторов и финансирующих организаций в секторе ИКТ.

Дополнительное прямое государственное или совместное частное и государственное финансирование также направлено на содействие инвестициям в инфраструктуру широкополосной связи и цифровые экосистемы. В Европейском союзе за последние несколько лет внедрен ряд механизмов финансирования и предоставления грантов для расширения развертывания широкополосных сетей. Например, недавно принятая программа Digital фонда Connecting Europe Facility (CEF2) предназначена для поддержки и ускорения роста инвестиций в представляющие общий интерес инфраструктуры цифровой связи в период 2021–2027 годов. Программа Digital CEF2 нацелена на поддержку проектов, направленных на устранение сбоев рыночных механизмов, и не приводит к вытеснению или замещению других эквивалентных инвестиций в целевой сектор. Будучи инструментом государственного софинансирования на уровне ЕС, программа Digital CEF2 может привлекать и частное софинансирование для устранения сбоев рыночных механизмов при условии, что создаваемая инфраструктура предназначена для районов, где отсутствует (и не планируется на ближайшие 24 месяца) эквивалентная с точки зрения емкости и/или функциональных возможностей сеть (European Commission 2019, 5).

Эффективные меры регулирования также могут способствовать снижению затрат на развертывание сети. Такая политика включает политику содействия доступу к существующей физической инфраструктуре, в том числе межотраслевую политику доступа к кабелепроводам, опорам и прочей пассивной инфраструктуре, принадлежащей энергетическим и другим коммунальным предприятиям. Для снижения затрат на

строительство сети также применяется политика "копай один раз", направленная на координацию строительных работ между различными коммунальными предприятиями. Оптимизация требований к выдаче разрешений, таких как право прохода, тоже помогает сократить время и затраты на развертывание инфраструктуры.

В качестве альтернативы для финансирования целей универсального доступа применяется и политика "плати или играй". В соответствии с ней поставщики услуг в таких странах, как Вануату, могут предпочесть "играть", то есть участвовать в проекте, покрывая затраты на развертывание инфраструктуры в необслуживаемых или недостаточно обслуживаемых районах или группах населения, а неучаствующие поставщики должны платить сбор ФУДО, установленный регуляторным органом. Соответственно если поставщик услуг решает "играть" в рамках проекта универсального доступа, регуляторный орган не взимает с него сбор за соответствующий год при условии, что он выполняет свои обязательства. На случай если чистые затраты превышают пороговый уровень сбора на универсальный доступ, имеются фонды помощи. В период с 2015 по 2018 год эта схема "плати или играй" успешно применялась в Вануату для модернизации сетей подвижной связи, чтобы обеспечить предоставление услуг передачи данных и охват более 98% (TRBR 2019, 7–8).

Политика повышения ценовой доступности услуг широкополосной связи и цифровых услуг

Согласно целевому показателю 2 Комиссии по широкополосной связи в интересах устойчивого развития к 2025 году базовые услуги широкополосной связи должны стать приемлемыми в ценовом отношении, то есть иметь стоимость на уровне менее 2% от ежемесячного валового национального дохода (ВНД) на душу населения (Broadband Commission for Sustainable Development 2019b, 32). Несмотря на значительные успехи в области повышения рыночной конкуренции, достигнутые за последнее десятилетие, во многих странах цены остаются выше установленного Комиссией по широкополосной связи порогового значения целевого показателя приемлемости в ценовом отношении "1 за 2" (то есть передача 1 ГБ данных по сети подвижной связи по цене не более 2% от ежемесячного ВНД на душу населения) (Broadband Commission for Sustainable Development 2019a, 34). В некоторых странах из-за низкого уровня дохода на душу населения в сочетании с низкой плотностью населения может потребоваться поддержка со стороны государственного сектора или совместная поддержка со стороны государственного и частного секторов для обеспечения высокой интенсивности развертывания сетей и для того, чтобы стоимость устройств не приводила к сохранению неприемлемости в ценовом отношении услуг доступа в интернет.

Среднемировая цена корзины услуг подвижной передачи данных объемом не менее 1,5 ГБ понизилась с 20,4 долл. США в 2013 году до 13,2 долл. США в 2019 году, что эквивалентно совокупному годовому темпу роста (CAGR) –7%, определяемому главным образом периодом с 2013 по 2015 год, за которым на протяжении последних четырех лет наблюдался период относительной стабильности. За последние шесть лет произошел резкий рост числа активных абонентов услуг подвижной передачи данных, которое увеличилось с 27,4 до 83 на 100 жителей, так что совокупный годовой темп роста составил 20,3% (ITU 2019).

В 2019 году в развитых странах цена корзины услуг подвижной передачи данных объемом 1,5 ГБ составила 17 долл. США, что выше среднемирового показателя в 14 долл. США. Однако поскольку большинство людей в развитых странах пользуются пакетом услуг передачи данных и голоса, тарифный план только на передачу данных не очень распространен. В развивающихся странах номинальная цена оставалась чуть ниже среднемировой, составляя 13 долл. США, тогда как в наименее развитых странах стоимость такого тарифного плана составила всего 8 долл. США. В долларовом выражении наиболее низкая цена корзины услуг подвижной передачи данных зафиксирована в регионе Содружества Независимых Государств (СНГ) (7 долл. США), за ним следуют Африка (10 долл. США), Азиатско-Тихоокеанский регион (11 долл. США) и арабские государства (14 долл. США). Двумя самыми дорогими регионами оказались Европа (16 долл. США) и Северная и Южная Америка (18 долл. США) (ITU 2019).

В целях повышения ценовой доступности цифровых услуг и устройств для конечных пользователей среди уязвимых групп населения часто используются целенаправленная политика, субсидии и рассрочки платежей. Например, государственная политика может использоваться для стимулирования местных инноваций, исследований и разработок в области устройств с возможностью доступа в интернет, таких как мобильные телефоны, а также для определения приоритетности поддержки через государственные инвестиционные органы предприятий, намеренных поставлять на рынок недорогие устройства (между местными и иностранными фирмами или смешанными государственно-частными предприятиями) (Broadband Commission for Sustainable Development 2019a, 19). Аналогичным образом операторы подвижной связи разрабатывают программы рассрочки платежей, чтобы облегчить приобретение "умных"

устройств потребителями с низким уровнем доходов. В Кении кампания, организованная Maisha Ni Digital, подразделением Safaricom в партнерстве с Google, направлена на обеспечение доступа к смартфонам базового уровня (устройствам Neon) и устранение гендерного разрыва – кенийские женщины пользуются мобильным интернетом на 34% реже мужчин. Такие устройства продаются по субсидированным ценам от 32 до 55 долл. США, и в 2019 году Safaricom продала более 600 тыс. смартфонов Neon, что сделало их самыми популярными и приемлемыми в ценовом отношении смартфонами в ее розничных магазинах по всей стране (Safaricom 2019a; Safaricom 2019b; GSMA 2020).

Вставка 3.4. Различные подходы к развертыванию общедоступной сети Wi-Fi

Общедоступная сеть Wi-Fi позволяет людям в общественных местах использовать гораздо больше данных за небольшую дополнительную плату или без дополнительной платы и без значительной потери доходов поставщиками розничных услуг. Это достигается с помощью различных организационных подходов и способов финансирования государственными органами и кооперативными платформами во всем мире (Alliance for Affordable Internet 2019a, 26).

Общее бюджетное финансирование. Развертывание бесплатных общедоступных сетей Wi-Fi поддерживается государственными органами – от национальных до местных – во всем мире. В ЕС в рамках программы WiFi4EU 6000 муниципалитетам выделены субсидии в размере 15 000 евро для покрытия капитальных затрат на предоставление бесплатных услуг общедоступной сети Wi-Fi^a. Правительство Филиппин запустило программу по предоставлению бесплатных услуг общедоступной сети Wi-Fi всем гражданам во всех общественных местах, включая парки, площади, библиотеки, сельские административные центры, национальные и местные государственные учреждения, государственные школы, государственные университеты и колледжи, государственные больницы, центры общественного здравоохранения и сельские медпункты, аэропорты, морские порты и вокзалы. Законодательство, принятое в 2017 году (Республиканский закон № 10929), возложило ответственность за реализацию программы на Министерство ИКТ (DICT), и по состоянию на апрель 2020 года в рамках программы "Бесплатный общедоступный Wi-Fi" работало 3735 точек доступа.

Финансирование ФУДО. В некоторых странах ФУДО предназначены для развертывания общедоступных сетей Wi-Fi. В Тринидаде и Тобаго через ФУДО предоставляются государственные средства для субсидирования процесса развертывания общедоступных сетей Wi-Fi и оплаты услуг (TATT 2016, 12). Эта инициатива не достигла большого успеха из-за проблем координации и ограниченного участия предприятий. В 2020 году правительство возобновило инициативу для решения этих проблем.

Программы спонсируемого доступа к данным. Для поддержки развертывания общедоступных сетей Wi-Fi также внедряются инновационные бизнес-модели, нацеленные на решение проблем приемлемости в ценовом отношении. В Кении и Руанде кенийский стартап BRCK успешно запустил проект Moja WiFi, в рамках которого конечным пользователям предлагаются бесплатные услуги и который финансируется за счет спонсорства и рекламы. Пользователи "оплачивают" услуги не деньгами, а своим временем, вниманием или вовлеченностью. Moja WiFi развернул 1300 точек доступа в сельских и городских районах и предоставляет бесплатные услуги доступа в интернет примерно 2 млн. пользователей (Loyce Chloe 2020).

Примечание. – WiFi4EU – бесплатный Wi-Fi для европейцев. <https://ec.europa.eu/digital-single-market/en/wifi4eu-free-wi-fi-europeans>

Проводимая во многих странах политика поощрения пунктов общего доступа в интернет, где услуги доступа в интернет предоставляются бесплатно или по низкой цене, также направлена на обеспечение некоторых из наиболее уязвимых лиц или групп. К таким пунктам относятся центры цифрового доступа в школах, библиотеках, почтовых отделениях и общедоступные сети Wi-Fi, гарантирующие конфиденциальность и безопасность. Разработка политики, направленной на создание устойчивых коллективных центров электросвязи, предлагающих бесплатные или недорогие услуги по использованию компьютеров, широкополосные соединения, электронные услуги и обучение цифровым навыкам, расширяет охват населения услугами широкополосного доступа и решает проблемы приемлемости в ценовом отношении (см. вставку 3.4).

Еще одним важным политическим рычагом, стимулирующим доступ пользователей к широкополосным и цифровым услугам и устройствам, является снижение налогов и сборов для конкретных секторов. Органы государственного управления должны найти баланс между необходимостью повышения доходов и негативными последствиями повышенных сборов и налогов, то есть сокращением внедрения и использования широкополосной связи, для экономики в целом и для процесса цифровой трансформации. Например, в 2017 году Колумбия решила отменить налог на добавленную стоимость (НДС) для недорогих мобильных телефонов и ноутбуков и освободить недорогие тарифные планы и потребителей с низкими доходами от повышения НДС. В результате этой целенаправленной политики объем продаж мобильных телефонов в 2017 году повысился даже среди тех устройств, стоимость которых превышала порог освобождения от НДС для недорогих устройств. Некоторые производители переоценили свои устройства, установив цену чуть ниже порога освобождения от НДС, что обеспечило колумбийцам более широкий спектр устройств по более приемлемым ценам (Alliance for Affordable Internet 2020b).

Политика содействия охвату цифровыми технологиями

Межотраслевая политика: цифровые навыки и грамотность

Политика в области универсального доступа эволюционировала и вышла за пределы собственно сектора ИКТ, вобрав в себя межотраслевые подходы, которые позволяют использовать преимущества ИКТ во многих отраслях экономики. Комиссия по широкополосной связи в интересах устойчивого развития выдвинула на первый план концепцию "реальной и универсальной возможности установления соединений", охватывающую внедрение услуг широкополосной связи, "не только готовых к использованию, доступных, уместных и приемлемых в ценовом отношении, но и безопасных, надежных, расширяющих возможности пользователей и оказывающих положительное воздействие" (Broadband Commission for Sustainable Development 2019a, ix). Концепции расширения возможностей пользователей, приводящего к положительному эффекту, считаются конечной целью межотраслевой политики, направленной на улучшение и расширение использования ИКТ для достижения более широкого воздействия.

Вероятно, наиболее ярким примером такого межотраслевого мышления служит включение в политику и планы универсального доступа цифровых навыков. МСЭ определил преимущества формирования цифровых навыков и их применения как в работе, так и в личных аспектах жизни людей (ITU 2018, 5):

- работа – квалификация для работы в традиционных отраслях; возможность участия в новых секторах; использование достижений цифровых технологий, платформ и устройств; важно для изменяющегося характера рабочей среды;
- доступ к информации – безопасный доступ к новостям и информации; общение с друзьями и родственниками; доступ к ключевым услугам (электронное здравоохранение, электронное правительство, цифровые финансовые услуги, сельскохозяйственные технологии и транспорт).

Основываясь на мнении Комиссии по широкополосной связи для устойчивого развития о существовании целого спектра цифровых навыков, МСЭ определил базовые, средние и продвинутые навыки (Broadband Commission for Sustainable Development 2017a, 4; ITU 2018, 5–7). Эти определения полезны как ориентиры для директивных органов, оценивающих цифровые навыки и межотраслевые компоненты планов универсального доступа. Кратко их можно описать следующим образом.

- **Базовые навыки** – это основополагающие навыки, необходимые для решения простых задач, подобные обычной грамотности и счету, которые включают в себя умение использовать оборудование и программное обеспечение и выполнять простые онлайн-операции, такие как работа с электронной почтой или заполнение форм.
- **Средние навыки** позволяют критически оценивать технологии и контент и в настоящее время могут включать в себя такие функции, как работа с настольными издательскими системами, цифровой графический дизайн и цифровой маркетинг, хотя ввиду продолжающегося технического прогресса потребуется изменение набора навыков, которые считаются средними.
- **Продвинутые навыки** – это навыки, необходимые специалистам-профессионалам в области ИКТ, такие как программирование и управление сетями, а также более широкие способности, такие как цифровое предпринимательство.

Использование межотраслевого компонента, такого как развитие цифровых навыков, создает благоприятные волновые эффекты во всей экономике, расширяя экономические возможности и

укрепляя коммуникации независимо от отрасли, географического положения или группы населения. Преимущества развития цифровых навыков для экономики в целом оправдывают акцент на их внедрении в образовательный процесс. Эти усилия, которые иногда предпринимаются в рамках общей политики в области образования или совместной инициативы отраслей образования и связи, имеют решающее значение для обучения учащихся в раннем возрасте способам использования возможностей широкополосной связи и информационных технологий. Европейская комиссия приняла План действий в области цифрового образования, в котором подключение школ к интернету – лишь первый из 11 содержащихся в нем пунктов (European Commission 2018). Эти пункты сгруппированы в соответствии с тремя приоритетами, среди которых "более эффективное использование технологий для преподавания и обучения" и "развитие надлежащих цифровых компетенций и навыков для цифровой трансформации". К приоритетному направлению, ориентированному на цифровые навыки, отнесены пункты, касающиеся включения кодирования во все европейские школьные программы, а также повышения осведомленности о безопасности в онлайн-среде, кибербезопасности и медийной грамотности на всех уровнях (родителей, преподавателей, учащихся).

Такое образование и обучение не ограничивается курсами начальной или средней школы. Вышеупомянутые средние и продвинутые навыки предполагают прохождение более специализированных курсов профессиональной подготовки и повышения квалификации. В Нидерландах в Пакте о цифровых технологиях провозглашен принцип широкого внедрения технологического образования, включая не только начальное и среднее, но и профессиональное и высшее образование, а также повышение квалификации (National Technology Pact 2016). В этом пакте делается упор на сотрудничество между учебными заведениями и производственным сектором в целях повышения технических навыков нидерландских работников. В разных странах непрерывное обучение цифровым навыкам также ведется в форме учебных лагерей и других целевых мероприятий по развитию профессиональных навыков.

Помимо доступа к ИКТ, возможность использования потенциальных выгод таких навыков в нескольких секторах усиливает их влияние и должна стать ключевым элементом современной политики или программы универсального доступа, а также может рассматриваться совместно с министерствами или государственными органами.

Содействие развитию местного контента и индустрии контента

Еще одно ключевое направление современной политики в области универсального доступа – это стимулирование спроса на подключение к сетям за счет содействия развитию соответствующего контента. Помимо предоставления пользователям соединения для доступа к контенту, дальновидная политика в области универсального доступа также должна учитывать необходимость стимулирования вновь подключенных к выходу в интернет и предложения им выгод от использования своего соединения.

Хотя в интернете размещено огромное количество общедоступного и частного контента, спрос на услуги подключения определяется наличием контента, интересующего пользователей. Это означает, что должен быть доступен контент на соответствующих языках, адаптированный к местным потребностям и интересам. Комиссия по широкополосной связи с самого начала призывала к обеспечению доступности местного контента. В принятом в октябре 2011 года документе "Широкополосный вызов" (Broadband Commission for Digital Development 2011, 2) Комиссия призвала правительства и гражданское общество к "стимулированию производства местного контента, а также развития услуг и приложений на местных языках для целей создания инклюзивного цифрового мира". При рассмотрении вопроса о формировании спроса за счет местного контента в официальном документе Intel 2011 года об использовании ресурсов ФУДО для программ широкополосной связи отмечается, что программное обеспечение и приложения на местных языках делают более доступными услуги образования и здравоохранения, финансовые услуги, электронное правительство и другие услуги (Intel 2011, 2).

Роль политики в области универсального доступа в этом контексте заключается в поддержке усилий, направленных на создание местного контента. Одним из недавних примеров такого подхода может служить нигерийский Национальный план широкополосной связи на 2020–2025 годы, который включает меры по привлечению в интернет большего числа нигерийских предприятий с помощью предоставления возможности бесплатной регистрации имен в домене .ng в течение двух лет и нескольких инициатив по повышению цифровой грамотности и осведомленности, направленных на стимулирование спроса (Government of Nigeria 2020, 61). Меры обоих типов способствуют обеспечению доступности местного контента. Инициатива по бесплатной регистрации доменных имен направлена на содействие развитию местного контента, а также созданию рабочих мест и расширению возможностей по ведению бизнеса

в интернете для нигерийских компаний за счет снижения затрат на создание нового онлайн-предприятия или онлайн-присутствия. Примечательно, что эта политика не подразумевает выделение средств конкретным предприятиям или отраслям, а скорее направлена на обеспечение общих выгод для всех нигерийских предприятий, желающих зарегистрировать доменное имя, позволяя им направлять свои ресурсы на другие аспекты развития бизнеса. Ответственность за реализацию таких инициатив распределяется между различными государственными учреждениями, при этом во всех мероприятиях по повышению цифровой грамотности принимает участие Министерство связи и цифровой экономики, а осуществление программы регистрации доменных имен возложено на Нигерийскую ассоциацию интернет-регистраторов, Национальное агентство по развитию информационных технологий (NITDA) и Комиссию по делам корпораций. Как видно из этого примера, подходы к повышению уровня цифровой грамотности и созданию контента затрагивают широкий круг заинтересованных сторон.

Филиппины включили аналогичный компонент в свой Национальный план широкополосной связи, заявив, что государство будет поддерживать развитие местного контента и приложений для стимулирования спроса на услуги широкополосной связи (Department of Information and Communications Technology 2017, 44). В частности, этот план предусматривает следующие мероприятия:

- предоставление стимулов разработчикам местного контента, начиная с создания, развития и маркетинга контента или приложений;
- государственную политику и регуляторные меры по созданию благоприятных условий для разработки контента и приложений;
- рассмотрение возможности разработки "богатого и полезного" контента и приложений для поддержки возможности предоставления государственных услуг и создания платформ взаимодействия с гражданами в целях стимулирования спроса; такие ресурсы также должны поддерживаться интерфейсами прикладного программирования, позволяющими отображать веб-сайты на нескольких языках в зависимости от потребностей или предпочтений пользователей.

Аналогичным образом, запланированные Нигерией мероприятия, связанные с повышением цифровой грамотности, также предполагают разработку образовательного, профессионального и делового контента на местных языках. В дополнение к этому нигерийский план предусматривает разработку и внедрение расширенной национальной цифровой виртуальной электронной библиотеки, которая предоставит ряд цифровых ресурсов и обеспечит перевод материалов с иностранных языков на местные.

Дополнительные подходы к развитию местного контента могут включать мероприятия по повышению доступности государственных услуг и информации в онлайн-режиме. Национальные, региональные и местные органы власти, будучи основными производителями информации, актуальной для местных пользователей и представленной на местном языке, идеально подходят для участия в реализации политики в области универсального доступа, в рамках которой создаются новые или расширяются существующие онлайн-ресурсы с полезной информацией для граждан.

В целом политика в области универсального доступа должна учитывать потенциальную выгоду от повышения доступности местного контента с точки зрения расширения использования интернета. При разработке целей или мероприятий, направленных на повышение доступности местного контента, директивные органы, чтобы добиться максимальной отдачи от этих усилий, должны учитывать роль как частного, так и государственного секторов.

Политика в области гендерного охвата и доступности

Признавая, что возможности доступа в интернет или его использования неодинаковы для разных групп населения, директивные органы должны подумать о том, как использовать политику в области универсального доступа и ФУДО для оказания особой помощи группам населения со сравнительно низким уровнем доступа и использования. В частности исследование выявило необходимость расширения возможностей подключения и доступа к цифровым услугам для женщин и лиц с ограниченными возможностями.

По оценкам МСЭ за 2019 год, разница в уровнях проникновения интернета среди мужчин и женщин во всем мире составила 17%, хотя эта цифра варьируется в зависимости от региона и уровня доходов (ITU 2019, 3). Примечательно, что в развивающихся странах эта разница составляет 22,8%, в то время как в НРС гендерный разрыв достигает почти 43%. Возможно, наибольшее беспокойство вызывает тот факт, что за последние несколько лет гендерный разрыв увеличился. Как свидетельствуют данные МСЭ, этот

показатель возрос в период с 2013 по 2019 год в Азиатско-Тихоокеанском регионе, регионе арабских государств и в Африке, а также в группах развивающихся стран и НРС.

ОЭСР отмечает, что гендерный разрыв, иногда называемый цифровым гендерным разрывом, имеет несколько коренных причин, включая наличие барьеров для доступа, приемлемости в ценовом отношении и образования, а также недостаточную технологическую грамотность (OECD 2018, 22). Хотя эти аспекты оказывают влияние на цифровой разрыв между группами, ОЭСР также отмечает актуальность гендерных предрассудков и социокультурных норм, приводящих к цифровой изоляции по признаку пола. Сюда можно отнести сравнительно большую занятость выполнением обязанностей по ведению домашнего хозяйства и уходу за детьми, а также негативное социальное восприятие использования интернета женщинами и девушками.

Организации, включая Комиссию по широкополосной связи в интересах устойчивого развития и Фонд World Wide Web, предложили политические подходы к устранению гендерного разрыва. Среди четырех рекомендаций, представленных Рабочей группой по цифровому гендерному разрыву Комиссии по широкополосной связи, предложение о включении гендерного аспекта в стратегии, политику, планы и бюджеты (Broadband Commission for Sustainable Development 2017b). Данная рекомендация основана на признании того факта, что политика, стратегии и планы действий, связанные с гендерной проблематикой, часто не учитывают важность ИКТ и широкополосной связи в качестве полезных инструментов, а стратегии, политика и планы в области широкополосной связи часто не включают гендерный аспект. В связи с этим Рабочая группа предложила три основные меры для решения данной проблемы:

- установление целевых показателей гендерного равенства в отношении доступа к интернету и широкополосной связи и их использования;
- оценку стратегий, политики, планов и бюджетов с точки зрения гендерного равенства; и
- проведение консультаций и вовлечение женщин, а также соответствующих местных сообществ и специалистов.

Такие подходы особенно важны для разработки или пересмотра политики в области универсального доступа и повышают вероятность устранения гендерного разрыва наряду с улучшением общей ситуации с подключением и доступом.

Фонд World Wide Web также определил ФУДО как "незадействованный ресурс" для решения проблемы гендерного цифрового разрыва (Thakur and Potter 2018). В связи с этим данная организация предложила четыре основные рекомендации по повышению эффективности и действенности ФУДО специально для устранения гендерного разрыва:

- 1) инвестировать не менее 50% средств в проекты, направленные на обеспечение доступа женщин в интернет и его использование ими;
- 2) обеспечить больший учет гендерных факторов при разработке и осуществлении проектов;
- 3) повысить прозрачность финансирования, выплат и операций фонда;
- 4) повысить разнообразие в руководстве ФУДО и степень осведомленности о гендерных проблемах в ФУДО.

Недавним примером такого подхода может служить План развития ИКТ Колумбии на 2018–2022 годы, который включает раздел об использовании ИКТ в качестве инструмента для сокращения гендерного разрыва (MinTIC 2018, 72). В этом плане подчеркивается важность расширения возможностей доступа к ИКТ для женщин и использования ими таких технологий, а также отмечается необходимость преодоления социокультурных норм и убеждений, препятствующих использованию женщинами ИКТ или их устройству на работу, связанную с ИКТ. В колумбийском плане также выделены две программы, направленные на расширение использования женщинами ИКТ и связанных с ними инструментов.

Помимо гендерного разрыва существует также неравенство в доступе, от которого страдают лица с ограниченными возможностями. Хотя ИКТ могут играть важную роль в преодолении барьеров, с которыми сталкиваются люди с ограниченными возможностями в плане активного участия в жизни общества, технический прогресс не гарантирует равного доступа к новым и усовершенствованным технологиям.

Среди различных мер по улучшению работы ФУДО в более широком плане ЭКЛАК предлагает ряд мер, направленных на устранение разрыва в доступе для людей с ограниченными возможностями. В их числе:

- позволить финансирование организаций гражданского общества и неправительственных организаций, работающих с лицами с ограниченными возможностями и другими маргинализированными группами;
- включить более строгие требования к фондам в отношении лиц с ограниченными возможностями, в том числе обязанность определять годовые целевые показатели достижения своих целей;
- расширить взаимодействие с лицами с ограниченными возможностями на каждом этапе жизненного цикла проекта, включая процессы идентификации, оценки и распределения;
- увеличить представительство лиц с ограниченными возможностями в ФУДО; и
- инвестировать фиксированную долю средств в проекты по расширению доступа к технологиям для лиц с ограниченными возможностями.

Вероятно, стоит отметить, что рекомендации Фонда World Wide Web по устранению гендерного разрыва во многом совпадают с рекомендациями ЭКЛАК по расширению доступа для лиц с ограниченными возможностями. Это может указывать на общие подходы к устранению разрыва в доступе среди других маргинализированных групп населения.

3.4 Контроль и оценка воздействия политики в области универсального доступа

Помимо эволюции политики в области универсального доступа и ключевых направлений деятельности для современных планов важно также иметь возможность оценки того, достигла ли эта политика или отдельный проект намеченных целей. Такой анализ отчетности должен быть основополагающим компонентом подходов к обеспечению универсального доступа и опираться как на четкие, измеримые цели, так и на возможность измерения прогресса в их достижении. В некотором смысле это уравнивает политику и планы обеспечения универсального доступа со многими другими направлениями государственной политики и программами, для которых директивным органам необходимо разработать и внедрить механизмы контроля воздействия. Помимо прозрачного распределения средств в поддержку целевых проектов ФУДО также очень важно оценивать, насколько эффективно и экономно используются собранные средства.

В связи с этим следует рассмотреть следующие два подхода к контролю и оценке воздействия политики в области универсального доступа: i) оценку общей политики и ii) оценку отдельных проектов, поддерживаемых ФУДО. В обоих случаях установление четких целей и/или основных этапов составляет основу для последующей оценки воздействия.

В отношении политики в области универсального доступа органы власти должны установить конкретные достижимые цели по ее ключевым аспектам. В число таких целей могут входить, например, обеспечение подключения к интернету в минимальном количестве пунктов или для минимального процента населения, обеспечение доступа к соединениям определенного уровня без превышения заданной доли национального дохода на душу населения и обеспечение минимального уровня качества обслуживания. Установление конкретных целей или этапов позволяет проанализировать усилия, предпринятые в результате осуществления политики. Например, если политика в области универсального доступа включает такую цель, как повышение доли населения, имеющего доступ к интернет-соединению со скоростью 10 Мбит/с, по крайней мере до 98% в течение пяти лет, то последующий анализ должен показать, достигнута ли эта цель. Если позволяют ресурсы, то особенно полезным инструментом будет служить промежуточная или среднесрочная оценка воздействия политики, которая дает возможность скорректировать курс до установленного срока.

Точно так же при разработке проектов, финансируемых ФУДО, должны устанавливаться конкретные основные этапы реализации и цели, которые должны быть достигнуты с указанием четких критериев измерения успеха. Традиционные проекты в области услуг голосовой связи, поддерживаемые ФУДО, часто структурированы таким образом, что выплаты осуществляются после успешного и своевременного завершения основных этапов проекта, что дает получателям стимул для соблюдения установленных сроков реализации и поставленных целей. Этот подход в равной мере применим и в более широком плане к поддерживаемым ФУДО проектам по расширению доступа в интернет и к цифровым услугам. Получатели финансирования должны суметь подтвердить, что они достигли поставленных целей, к которым могут

относиться не только подключение, но и степень освоения, уровень цен, разнообразие доступных услуг или услуги, доступные для малоимущих слоев населения.

В соответствии с конкретными этапами и сроками проекты, финансируемые ФУДО, должны включать в себя требования к отчетности, в которые могут входить оценка хода осуществления проекта, анализ любых неожиданных обстоятельств, финансовая отчетность и любой другой соответствующий анализ, особенно в случаях отклонения от первоначальных планов проекта. Как отмечалось выше, такие требования могут не сильно отличаться от требований к отчетности по проектам, ориентированным на телефонию, но должны быть адаптированы к конкретному проекту и его целям. Так, дополнительные требования к отчетности могут включать среднюю скорость широкополосного доступа, доступ к определенным цифровым услугам или меры по обеспечению доступа для лиц с ограниченными возможностями. Цели требований к отчетности должны состоять в том, чтобы дать возможность всем заинтересованным сторонам оценить ход осуществления или успех проекта, а также служить мотивацией для получателя финансирования к выделению соответствующих ресурсов для достижения целей проекта.

Контроль политики в области универсального доступа и соответствующих проектов – это ключевой элемент, повышающий вероятность успеха. Хотя данная концепция восходит к самым ранним политическим подходам в этой области, ее можно и нужно адаптировать к современным потребностям в отношении универсального доступа и цифровых услуг.

3.5 Основные выводы

С учетом вопросов, рассмотренных в предыдущих разделах, можно сделать следующие основные выводы, полезные для директивных органов и других заинтересованных сторон.

Акцент на надежные и приемлемые в ценовом отношении услуги широкополосного доступа и устройства. По мере того как директивные органы разрабатывают или пересматривают политику в области универсального доступа, все более важное значение приобретает наличие надежных и приемлемых в ценовом отношении услуг широкополосного доступа. Для этих услуг используются международные интернет-соединения и соединения магистральных сетей, транзитные соединения и соединения последней мили. Эта инфраструктура обеспечивает возможность установления соединений, что в свою очередь способствует более широкому социально-экономическому развитию. Ключевой вопрос, требующий новаторских подходов и бизнес-моделей, особенно для доступа к устройствам, – это приемлемость в ценовом отношении.

Повышение эффективности ФУДО. Прошлые и текущие проблемы, с которыми сталкивались и сталкиваются ФУДО и группы населения, которые должны получать выгоду от осуществления проектов этих фондов, указывают на необходимость пересмотра и, если требуется, реформирования сферы деятельности, процессов и эффективности таких фондов. Эти проблемы необходимо решить, чтобы сделать ФУДО более эффективными и лучше подготовленными для обеспечения универсальной возможности установления соединений.

Диверсифицированные источники финансирования и альтернативные подходы. Директивные органы и заинтересованные стороны в настоящее время рассматривают широкий спектр традиционных и альтернативных подходов к финансированию проектов для более эффективного достижения целей универсального доступа. Как уже говорилось, к ним могут относиться фискальные меры и нормативные акты, направленные на снижение риска, ФУДО и новые подходы к финансированию с использованием частного финансирования или опыта или же сочетание государственных и частных источников, а также оптимизация регулирования.

Развитие навыков делает возможным и стимулирует внедрение широкополосной связи. Для стимулирования более широкого внедрения широкополосной связи одной лишь возможности установления соединений недостаточно. Планы универсального доступа расширяются, охватывая также компоненты, направленные на развитие цифровых навыков, которые позволят людям использовать преимущества этих соединений и эффективно работать в условиях экономики, которая все больше становится цифровой.

В планы универсального доступа все чаще включаются вопросы обеспечения охвата и доступности.

Помимо возможности установления соединений и широких социально-экономических целей в планы универсального доступа все чаще включаются меры по охвату групп населения, традиционно не имеющих этой возможности и не пользующихся ее преимуществами, таких как женщины и лица с ограниченными возможностями.

Контроль и оценка продолжают играть важную роль. Воздействие политики в области универсального доступа зависит от эффективной и действенной реализации. Поэтому для такой политики по-прежнему требуются структурированные механизмы контроля и оценки, призванные обеспечить достижение целей этой политики, программы и инвестиций.

Рассмотрение этих основных выводов поможет директивным органам и другим заинтересованным сторонам учесть вопросы и проблемы, важные для оценки и разработки политики в области универсального доступа.

Справочные материалы

- Alliance for Affordable Internet. 2015. *Universal Access and Service Funds in the Broadband Era: The Collective Investment Imperative*. Washington, DC: A4AI. http://a4ai.org/wp-content/uploads/2015/03/A4AI-USAFs-2015_Final-v.2.pdf
- Alliance for Affordable Internet. 2019. *2019 Affordability Report*. Washington, DC: A4AI. https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/A4AI_2019_AR_Screen_AW.pdf
- Alliance for Affordable Internet. 2020. *Good Practices Database*. Washington, DC: A4AI. <https://a4ai.org/good-practices-database/>
- Article 19. 2020. *Coronavirus: Access to the Internet Can Be a Matter of Life and Death During a Pandemic*, London. <https://www.article19.org/resources/access-to-the-internet-can-be-a-matter-of-life-and-death-during-the-coronavirus-pandemic/>
- Broadband Commission for Digital Development. 2011. *The Broadband Challenge*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.broadbandcommission.org/Documents/publications/Broadband_Challenge.pdf
- Broadband Commission for Sustainable Development. 2015. *2025 Targets: "Connecting the Other Half"*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. <https://www.broadbandcommission.org/Documents/publications/wef2018.pdf>
- Broadband Commission for Sustainable Development. 2017a. *Working Group on Education: Digital skills for Life and Work*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. <https://broadbandcommission.org/Documents/publications/WG-Education-Report2017.pdf>
- Broadband Commission for Sustainable Development. 2017b. *Working Group on the Digital Gender Divide: Recommendations for Action: Bridging the Gender Gap in Internet and Broadband Access and Use*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. <https://www.broadbandcommission.org/Documents/publications/WG-Gender-Digital-Divide-Report2017.pdf>
- Broadband Commission for Sustainable Development. 2019a. *Connecting Africa Through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf
- Broadband Commission for Sustainable Development. 2019b. *The State of Broadband 2019*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf
- Bleeker, Amelia. 2019. "Using Universal Service Funds to Increase Access to Technology for Persons with Disabilities in the Caribbean", Studies and Perspectives series-ECLAC Subregional Headquarters for the Caribbean, No. 79(LC/TS.2019/59-LC/CAR/TS.2019/2). Santiago: Economic Commission for Latin America and the Caribbean. https://www.cepal.org/sites/default/files/events/files/series_79_lcarts2019_2.pdf
- Department of Information and Communication Technology. 2017. *National Broadband Plan*. Quezon City: Department of Information and Communications Technology (DICT). <https://dict.gov.ph/wp-content/uploads/2017/09/2017.08.09-National-Broadband-Plan.pdf>
- ECTEL. 2008. *Telecommunications Universal Service Guidelines*. Saint Lucia: Eastern Caribbean Telecommunications Authority (ECTEL). <https://www.ectel.int/wp-content/uploads/2015/12/ECTEL-universal-service-guidelines.pdf>
- European Commission. 2018. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan*. Brussels: European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:22:FIN>

- European Commission. 2019. *Draft Orientations Towards an Implementation Roadmap: Connecting Europe Facility (CEF2) Digital*. Brussels: European Commission. <https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital>
- Government of Nigeria. 2020. *Nigerian National Broadband Plan 2020-2025*. Abuja: Federal Ministry of Communications and Digital Economy. <https://www.ncc.gov.ng/docman-main/legal-regulatory/legal-other/880-nigerian-national-broadband-plan-2020-2025/file>
- GSMA. 2013. *Universal Service Fund Study*. London: GSMA. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_Report_SurveyOfUniversalServiceFunds.pdf
- GSMA. 2016. *Are Universal Service Funds an Effective Way to Achieve Universal Access?* London: GSMA. <https://www.gsma.com/mobilefordevelopment/country/global/universal-service-funds-effective-way-achieve-universal-access/>
- GSMA. 2020. *Safaricom Maisha Ni Digital: Driving Digital Inclusion for Women*. London: GSMA. <https://www.gsma.com/mobilefordevelopment/resources/safaricom-maisha-ni-digital/>
- IEEE. 2017. *Options and Challenges in Providing Universal Access*. New Jersey: Institute of Electrical and Electronics Engineers (IEEE). https://internetinitiative.ieee.org/images/files/resources/white_papers/universal_access_feb2017.pdf
- Intel. 2011. *The Benefits of Applying Universal Service Funds to Support ICT/Broadband Programs*. Santa Clara: Intel Corporation. <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/usf-support-ict-broadband-programs-paper.pdf>
- ITU. 2017. *Connecting the Unconnected: Working Together to Achieve Connect 2020 Agenda Targets*. Geneva: International Telecommunication Union. https://broadbandcommission.org/Documents/ITU_discussion-paper_Davos2017.pdf
- ITU. 2018. *Digital Skills Toolkit*. Geneva: International Telecommunication Union. <https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf>
- ITU. 2019. *Measuring Digital Development: Facts and Figures 2019*. Geneva: International Telecommunication Union. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>
- ITU. 2020. *2019 Statistics*. Geneva: International Telecommunication Union. <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>
- Loyce Chloe. 2020. "The Affordability Barrier: Moja in Numbers". *BRCK Blog*, April 3, 2020. <https://www.brck.com/2020/04/the-affordability-barrier-moja-in-numbers/>
- MinTIC. 2018. *Plan TIC 2018-2022*. Bogota: Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/604/articles-101922_Plan_TIC.pdf
- National Technology Pact. *National Technology Pact 2020: Targets for 2016-2020*. <https://www.technikpact.nl/cdi/files/e3bd421f98a0f362b6a13091de60d08978df34e9.pdf>
- OECD. 2018. *Bridging the Digital Gender Divide: Include, Upskill, Innovate*. Paris: Organisation for Economic Co-operation and Development. <http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf>
- OECD. 2019a. *Going Digital: Shaping Policies, Improving Lives*. Paris: Organisation for Economic Co-operation and Development. <https://www.oecd-ilibrary.org/docserver/9789264312012-en.pdf?expires=1588087194&id=id&accname=guest&checksum=01C4C2080AC6C52A3024A2989151250D>
- OECD. 2019b. "OECD Urges More Action on Bridging Digital Divides, Boosting Skills and Enhancing Access to Data at Going Digital Summit". Press Release, March 12, 2019. <https://www.oecd.org/newsroom/oecd-urges-more-action-on-bridging-digital-divides-boosting-skills-and-enhancing-access-to-data-at-going-digital-summit.htm>
- Republic of Kenya. 2019. *Digital Economy Blueprint: Powering Kenya's Transformation*. <https://ca.go.ke/wp-content/uploads/2019/05/Kenyas-Digital-Economy-Blueprint.pdf>
- Safaricom. 2019a. "Safaricom Launches Third Edition of Maisha Ni Digital Campaign". Press Release, April 18, 2019. <https://www.safaricom.co.ke/about/media-center/publications/press-releases/release/546>

- Safaricom. 2019b. "Safaricom Sells More Than 0.6 Million Neon Smartphones". Press Release. September 24, 2019. <https://www.safaricom.co.ke/about/media-center/publications/press-releases/release/801>
- TATT. 2016. *Framework for the Implementation of Free Public WiFi Hotspots Throughout Trinidad and Tobago*. Port of Spain: TATT. <https://tatt.org.tt/UniversalService/UniversalServiceFundInitiatives.aspx>
- Thakur, D., and Potter, L. 2018. *Universal Service and Access Funds: An Untapped Resource to Close the Gender Digital Divide*. Washington DC: Web Foundation. <http://webfoundation.org/docs/2018/03/Using-USAFs-to-Close-the-Gender-Digital-Divide-in-Africa.pdf>
- TRBR (Office of the Telecommunications, Radiocommunications and Broadcasting Regulator). 2019. *Universal Access Policy (UAP) Stakeholders Tenth and Final Report on the Status of Implementation of the Government's Universal Access Policy*. Port Vila, Vanuatu: TRBR. https://www.trbr.vu/attachments/article/756/uap_stakeholder_10th_and_final_report.pdf
- Организация Объединенных Наций, 2015. *Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года*. A/RES/70/1. Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E
- Организация Объединенных Наций, 2016. *Поощрение, защита и осуществление прав человека в Интернете*. A/HRC/32/L.20. Резолюция, принятая Генеральной Ассамблеей 27 июня 2016 года. <https://digitallibrary.un.org/record/845728?ln=en>
- United Nations. 2017. *Promotion, Protection and Enjoyment of Human Rights on the Internet: Ways to Bridge the Gender Digital Divide from a Human Rights Perspective*. Report of the United Nations High Commissioner for Human Rights. New York: United Nations. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/111/81/PDF/G1711181.pdf?OpenElement>
- United Nations. 2018. *Progress Made in the Implementation of and Follow-Up to the Outcomes of the World Summit on the Information Society at the Regional and International levels*. Report of the Secretary-General. New York: United Nations. https://unctad.org/en/PublicationsLibrary/a73d66_en.pdf
- United Nations. 2019. *Report of the Secretary-General on SDG Progress 2019: Special Edition*. E/2019/68. New York: United Nations. https://sustainabledevelopment.un.org/content/documents/24978Report_of_the_SG_on_SDG_Progress_2019.pdf
- UN ESCAP (United Nations Economic and Social Commission for Asia and the Pacific). 2017. *The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific*. Thailand: UN ESCAP. <https://www.unescap.org/sites/default/files/Universal%20Access%20and%20Service%20Funds%20final.pdf>

Глава 4. Вопросы, касающиеся потребителей



4.1 Введение в права потребителей цифровых услуг

Почему нужно заботиться о правах потребителей?

Цифровая трансформация экономики охватывает множество аспектов, в том числе перевод в цифровой формат самих продуктов, производственных процессов, способов рекламирования и распространения продуктов, методов их приобретения и, разумеется, связи.

У потребителей есть важные интересы, касающиеся всех этих аспектов, в первую очередь, возможно, связи, а также контента и других возможностей, доступ к которым предоставляют сети и средства связи. Предметом рассмотрения в настоящей главе являются вопросы регулирования, касающиеся интересов потребителей в плане возможности установления соединений; в ней также описаны проблемы в сфере цифровых финансовых операций, контента, рекламы и распределения, с которыми сталкиваются потребители.

Расширение прав и возможностей потребителей и их защита становятся более важной составной частью деятельности регуляторных органов по ряду причин, включая следующие.

- Широкое распространение цифровой связи означает, что люди полагаются на нее как на жизненно важную услугу, и регуляторные органы ИКТ обычно несут ответственность за обеспечение ее всеобщей доступности и приемлемости в ценовом отношении¹.

¹ См. главу 3 "Доступ для всех".

- Еще одна причина роста заинтересованности потребителей в регулировании цифровой сферы – это переход к регулированию на основе результатов (Hogg 2020), когда регуляторный орган не только следит за тем, как компания соблюдает правила, но и учитывает реальный опыт потребителей².
- В последние несколько десятилетий достигнут большой прогресс в области поведенческих наук, что позволило лучше понять поведение потребителей и то, как его следует учитывать при разработке политики. Реальные люди не всегда ведут себя как "рациональные потребители", на которых ориентировались экономисты-классики³.
- Огромное разнообразие цифровых услуг означает, что выбор, который делает потребитель, играет важнейшую роль для обеспечения здоровой конкуренции на многих взаимосвязанных рынках⁴.
- Широкое использование интернета и приложений создает условия для такого явления, как *просьюмеризм*, когда потребители одновременно и производят контент, и потребляют контент, созданный другими пользователями, и могут напрямую взаимодействовать друг с другом на таких платформах, как eBay или Taobao.

Все это свидетельствует о появлении новых выгод для потребителя и о том, что в цифровую эпоху потребители обладают потенциалом, способным повлиять на конфигурацию рынков. В то же время появление новых категорий услуг ведет к возникновению новых проблем и новых рисков, что, соответственно, требует расширения прав и возможностей потребителей и их защиты. Заявление Ассоциации европейских регуляторных органов электронных средств связи (BEREC), которое приводится во вставке 4.1, убедительно свидетельствует о том, что расширение прав и возможностей конечных пользователей может в ближайшее десятилетие стать приоритетной задачей для регуляторных органов по всему миру.

МСЭ обращает особое внимание на вопросы, касающиеся потребителей, и в своей концепции регулирования пятого поколения (совместного регулирования)⁵:

Концепция совместного регулирования вновь подчеркивает значение выгод для потребителей и их защиты и предусматривает привлечение ресурсов государственных учреждений и компаний отрасли для решения этой задачи путем постоянных консультаций, сотрудничества и согласований.

² Подобный упор на добросовестность наблюдается как минимум по всей Европе. См., например, документы Ofcom (2020) и BEREC (2020), в которых акцентируется внимание на расширении прав и возможностей потребителей как составной части программы деятельности.

³ См., например, Evans (2003), Dutta-Powell and others (2019), Lunn (2014), Lunn and Lyons (2018) и <https://www.esri.ie/news/experiments-show-when-consumers-are-vulnerable-to-mistakes>.

⁴ См. главу 2 "Конкуренция и экономика".

⁵ См. <https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Policy-%26-Regulatory-Frameworks.aspx>

Вставка 4.1. Заявление BEREC о стратегии расширения прав и возможностей потребителей

Проект стратегии BEREC на 2021–2025 годы предусматривает три основных стратегических приоритета: содействовать полной реализации возможности установления соединений, оказывать поддержку устойчивым и открытым цифровым рынкам и расширять права и возможности конечных пользователей. В отношении последнего BEREC заявляет:

Привлечение потребителей к участию в стремительно развивающейся цифровой экосистеме становится все более сложной задачей. Хотя инновации в цифровой сфере и конкуренция между поставщиками цифровых услуг способствовали расширению прав и возможностей потребителей, регуляторным органам по-прежнему необходимо уделять пристальное внимание обеспечению определенного уровня прозрачности для потребителей и приобретению ими некоторых цифровых навыков.

Содействие полной реализации возможности установления соединений приведет к росту спроса на высококачественные услуги со стороны части потребителей, чему будет способствовать очень высокая пропускная способность сетей, совершенствование которых становится главным условием обеспечения позитивного взаимодействия.

BEREC будет и далее содействовать увеличению возможностей выбора для конечных пользователей и расширению их прав и возможностей, уделяя при этом особое внимание укреплению доверия к ИКТ и цифровым услугам, а также предоставлению пользователям возможностей для более информированного выбора.

Подход BEREC к расширению прав и возможностей конечных пользователей имеет две основные составляющие: проведение мониторинга отрасли и обеспечение необходимого уровня прозрачности. В рамках мониторинга соблюдения норм Европейского кодекса электронных средств связи BEREC намерен также осуществлять надзор за новыми положениями, касающимися конечных пользователей, такими как требования к предоставлению информации, включая шаблон типового контракта, и будет направлять в ЕК свои предложения, касающиеся обзора прав конечных пользователей. Что касается обеспечения прозрачности, BEREC продолжит работу по более активному взаимодействию с заинтересованными сторонами, в том числе представителями потребителей, и будет публиковать материалы об этой работе в соответствии со своими нормативными требованиями.

В рамках деятельности по обеспечению прозрачности BEREC продолжит создание базы знаний по ИИ, а также будет изучать способы защиты потребителей от потенциальных рисков.

Источник: BEREC 2020.

Предметом рассмотрения в настоящей главе являются следующие темы.

- В разделе "**Система поддержки потребителей**" рассматриваются рамочные основы деятельности регуляторных органов в области ИКТ. В подразделе "**Функции регуляторных органов в области ИКТ**" дается описание ориентированных на интересы потребителей мер, которые, скорее всего, станут прерогативой регуляторных органов ИКТ.
- В разделе "**Конкретные проблемы, касающиеся потребителей**" дается описание уже возникающих основных проблем потребителей, а также характеристика изменяющихся перспектив и нужд потребителей.
- Наконец, в разделе "**Основные выводы**" обобщаются наиболее значимые выводы по материалам данной главы.

Права и обязанности потребителей в цифровом мире

В контексте регулирования ИКТ понятие "потребитель" обычно означает лицо, приобретающее услуги для себя самого или для использования в домохозяйстве. К потребителям часто относят и лиц, приобретающих услуги как для делового, так и для личного потребления, а также в учебных целях⁶.

Это означает, что большинство жителей планеты являются потребителями услуг ИКТ⁷. Осознание этого может быть полезно для регуляторных органов, которые испытывают трудности при поиске представителей потребителей для консультаций по вопросам политики или хотели бы знать, какие именно меры в наибольшей степени отвечают интересам потребителей. Хотя лучше всего искать ответы на эти вопросы путем консультаций с потребителями и проведения исследований, удачным началом может стать изучение потребительских запросов собственной семьи, друзей и знакомых, особенно если в их число входят жители сельских районов, малоимущие или другие лица, находящиеся в сложных жизненных ситуациях.

Основные права потребителей для всех отраслей были определены в 1960-е годы, и к их числу относятся доступность, возможность выбора, информирование/просвещение, безопасность, возмещение ущерба, устойчивость и представительство⁸. В 2014 году на Глобальном симпозиуме МСЭ для регуляторных органов эти принципы были включены в Руководящие указания на основе примеров передового опыта по защите прав потребителей в цифровом мире, краткое изложение которых приводится во вставке 4.2. На их основе и по результатам исследований, проведенных в 23 странах, в основном развивающихся, был разработан, в частности, более полный перечень (см. таблицу 4.1), показывающий, как представления о правах потребителей и граждан становятся все более изменчивыми и образуют то, что сегодня называют "правами в цифровой сфере", которыми обладают все люди без исключения⁹.

⁶ Подробнее об этом и других сопутствующих терминах (в том числе "(конечный) пользователь", "(коммерческий или бытовой) потребитель", "потенциальный потребитель" и "гражданин") см. тематический раздел "Защита потребителей в целом" *Платформы цифрового регулирования*.

⁷ В *Справочнике по цифровому регулированию* и на *Платформе цифрового регулирования* под термином "информационно-коммуникационные технологии" (ИКТ) обычно понимается электросвязь и относящиеся к ней оборудование и сети, а под термином "цифровой" — понятия, связанные с интернетом и онлайн-средой.

⁸ Новейший перечень основных прав потребителей см. в ЮНКТАД (2016).

⁹ Подробнее об этом см. тематический раздел "Права потребителей в цифровом контексте" *Платформы цифрового регулирования*. В отчете организации Consumers International, по данным которого составлена таблица 4.1, содержатся более подробные данные о ситуации по состоянию на 2017 год и ее возможных изменениях.

Вставка 4.2. Принципы, перечисляемые в принятых ГСР-14 Руководящих указаниях на основе примеров передового опыта по защите прав потребителей в цифровом мире

- 1. Намечать стратегическое направление** повышения роли и значимости вопросов, касающихся потребителей, в рассчитанной на перспективу общеполитической программе действий, учитывающей как национальный, так и международный контекст.
- 2. Повышать рыночную конкурентоспособность** на всех уровнях, придерживаясь равного подхода к поставщикам услуг ИКТ и поставщикам услуг ОТТ в вопросах защиты прав потребителей.
- 3. Устанавливать партнерские отношения с отраслью**, опираясь на стремление поставщиков услуг защищать потребителей от возможного ущерба.
- 4. Обеспечивать надежную основу для контрактных услуг**, гарантируя прозрачность и поддержание баланса между правами и обязанностями.
- 5. Различные каналы возмещения ущерба**, позволяющие потребителям защищать свои права быстро и бесплатно или при минимальных затратах.
- 6. Качество обслуживания и опыт потребителей:** принятие мер для обеспечения того, чтобы у потребителей, в том числе у лиц с ограниченными возможностями, был легкий и надежный доступ к услугам ИКТ и сетевому контенту.
- 7. Защита частной жизни и данных потребителей:** необходимость получать от потребителей согласие в явной форме на сбор данных в сети, обращая при этом особое внимание на защиту детей и молодежи и создавая Группы реагирования на нарушения компьютерной защиты (CERT).
- 8. Расширение прав и возможностей потребителей** путем просвещения, повышения осведомленности и привлечения к участию в диалогах по вопросам политики, с использованием как новых средств массовой информации, так и традиционных каналов, например школ.
- 9. Право потребителей на информацию:** предоставление четкой, актуальной и сопоставимой информации способами, помогающими потребителям принимать рациональные решения.
- 10. Переопределение роли регуляторных органов**, что может предусматривать защиту прав потребителей, предоставление фактических данных и технических знаний, а также расширение их правоприменительных полномочий по делам, затрагивающим интересы потребителей.

Источник: МСЭ 2014.

Естественно, в законодательстве разных стран права закреплены по-разному, и так же по-разному обстоят дела с их осуществлением. Права предполагают соответствующие обязанности. К числу обязанностей потребителей относятся:

- внесение установленной платы за услугу;
- соблюдение соответствующих законов в онлайн-среде в той же мере, что и вне интернета, включая неучастие в мошеннической или иной преступной деятельности;
- соблюдение в сети соответствующих правил и норм, например, касающихся авторских прав и ограничений на передачу персональных данных третьим лицам, использования приемлемой лексики и недопустимости преднамеренного введения других лиц в заблуждение;
- защита паролей и своевременная установка обновлений для систем безопасности приложений и программного обеспечения;
- предоставление помощи в использовании цифровых услуг детям и другим окружающим, которым, возможно, такая помощь требуется.

Таблица 4.1. Карта цифровых прав потребителей и граждан

ЦИФРОВЫЕ ПРАВА ФИЗИЧЕСКИХ ЛИЦ КАК	
ПОТРЕБИТЕЛЕЙ	ГРАЖДАН
1. Доступ и всеохватность	
• Приемлемые по цене доступ и устройства • Качественное, надежное соединение • Актуальный контент • Право на интернет без ограничений • Инфраструктура в отдаленных районах	• Свобода от онлайн-домогательства • Равноправие и всеохватность • Свобода ассоциации • Открытые сети
2. Раскрытие информации и прозрачность	
• Содержательная информация, легкодоступная и простая для понимания • Справедливые условия контрактов • Информированный выбор • Прозрачные бизнес-модели и условия использования	• Свобода печати, свобода информации • Право на связь • Свобода выражения мнений, запрет цензуры • Фильтрация/контроль контента
3. Безопасность и защищенность	
• Безопасность данных/защита от мошеннических действий/утраты • Возмещение ущерба в случае утечки данных • Право на безопасные и конфиденциальные цифровые продукты и услуги, в том числе для уязвимых категорий потребителей • Прозрачность информации об утечке данных • Люди на самом деле являются теми, за кого они себя выдают (цифровое удостоверение личности)	• Защищенные государственные услуги, особенно в случае конфиденциальных данных (например, о состоянии здоровья) • Безопасное интернет-пространство для всех – женщин, представителей меньшинств, детей; недопустимость агрессивных высказываний • Кибербезопасность
4. Защита данных и конфиденциальность в сети	
• Конфиденциальность – недопущение корпоративного наблюдения • Свобода от навязчивой рекламы • Недопущение дискриминации по ценам, качеству, услугам • Особые положения в отношении конфиденциальных данных и уязвимых категорий потребителей	• Право на забвение • Свобода от наблюдения со стороны государства • Недопущение основанной на анализе данных предвзятости при принятии решений по вопросам трудоустройства, образования, правосудия, государственной службы и т. д.
5. Конкуренция и выбор	
• Выбор поставщика и право беспрепятственно перейти к другому поставщику • Применение законодательства о конкуренции • Признание преимущественного положения держателя данных • Справедливый выбор независимо от местоположения • Справедливые, инклюзивные рынки	• Права на доступ к правосудию и беспристрастное слушание дела

Таблица 4.1. Карта цифровых прав потребителей и граждан (продолжение)

ЦИФРОВЫЕ ПРАВА ФИЗИЧЕСКИХ ЛИЦ КАК	
ПОТРЕБИТЕЛЕЙ	ГРАЖДАН
6. Добросовестное использование и четкое указание права собственности	
- Права на исправление ошибок - Право на ответ/должное разбирательство в случае автоматического наложения санкций - Разумный срок действия и поддержка	- Справедливые нормы в отношении авторских прав - Управление цифровыми правами - Добросовестное использование - Доступ к знаниям
7. Возмещение ущерба и рассмотрение претензий	
Право на беспрепятственный, простой и экономичный доступ к механизмам возмещения ущерба	Права на доступ к правосудию и на получение возмещения ущерба
8. Цифровое образование и повышение осведомленности о цифровых технологиях	
- Право потребителей на обучение - Простые в использовании системы и продукты - Доступ к контенту - Надежные и проверяемые источники	- Право на обучение методам управления рисками и расширения возможностей в сети - Право на цифровую грамотность - Предоставление контента на местном языке
9. Система регулирования	
- Право быть услышанным при разработке политики в цифровой сфере - Наличие у компаний процедуры ответов на запросы потребителей - Прозрачные процедуры	- Учет разных мнений в процессе управления использованием интернета - Электронное голосование - Участие в гражданской и политической жизни, онлайн-акции протеста - Свобода информации
10. Ответственные методы ведения бизнеса	
- Недопущение дискриминации по ценам, качеству, услугам - Достоверная информация/контент - Недопустимость занижения стандартов для стран с более низким уровнем дохода - Выполнение компаниями обязательств в области прав человека	- Цепочки поставок информации, отвечающие этическим стандартам - Обязанность соблюдать интересы - Условия труда работников: справедливое обращение, недопустимость надзора

Источник: на основании Consumers International 2017a.

Общее и специальное законодательство о защите прав потребителей

Общее законодательство о защите прав потребителей имеет давнюю историю¹⁰, и со временем на базе его основополагающих принципов были разработаны законы, обеспечивающие баланс между правами потребителей и правами производителей. По мере изменения в расстановке соответствующих сил возникает необходимость в корректировке этих законов: как правило, рост относительного влияния производителей приводит (с некоторым запозданием) к усилению правовой защиты потребителей.

¹⁰ Руководящие принципы ООН для защиты интересов потребителей, в основу которых были положены принципы, впервые сформулированные президентом США Кеннеди в начале 1960-х годов, были впервые утверждены резолюцией 39/248 Генеральной Ассамблеи, принятой 16 апреля 1985 года; затем они были расширены решением E/1999/INF/2/Add.2 Экономического и Социального Совета от 26 июля 1999 года и пересмотрены резолюцией 70/186 Генеральной Ассамблеи от 22 декабря 2015 года.

В силу того что электронная связь прежде являлась монополией, а также поскольку она представляет собой жизненно важную услугу и *благо скрытой полезности* (продукт, качество и характеристики которого можно выявить только в процессе употребления), в разных странах были приняты различные специальные нормы, регулирующие защиту прав потребителей в этой сфере¹¹. Так, например, поставщиков могут обязать обеспечить доступ лиц с ограниченными возможностями как к сетевым услугам, так и к абонентским службам; кроме того, может быть определена максимальная продолжительность действия договора¹².

Аналогичным образом, особых мер защиты нередко требуют финансовые операции в рамках электронной торговли. Это оправданно, поскольку потребители, как правило, не могут проверить свое потенциальное приобретение до его покупки и могут подпасть под воздействие приемов навязывания со стороны продавцов, таких как предложения "только один раз" и бонусы за регистрацию. Как правило, ответственность за осуществление общих мер по защите потребителей чаще несут органы защиты прав потребителей, а не регуляторные органы ИКТ, но регуляторные органы ИКТ должны быть в курсе существования таких мер. Более широкое регулирование таких платформ, как Google, Amazon и Facebook, является сегодня предметом обсуждения, что связано с транснациональным характером этих платформ, зачастую в сочетании с их доминированием на рынке.

В таблице 4.2 показаны имеющиеся в мире варианты сводов законов, считающихся необходимыми для того, чтобы развитие цифровой экономики было безопасным для потребителей, а также указано, кто несет ответственность за защиту прав потребителей услуг электросвязи/ИКТ. При этом особо необходимо отметить следующее.

- В основном законодательстве по-прежнему остаются серьезные пробелы, прежде всего в части общих законов о защите прав потребителей и законов о защите данных¹³ в странах Африки, Арабского региона, Азиатско-Тихоокеанского региона, а также Содружества Независимых Государств (СНГ).
- Во всех регионах, кроме Северной и Южной Америки, значительно больше стран имеют особые законы/нормы регулирования, защищающие права потребителей услуг электросвязи, нежели законодательство общего характера. Иными словами, регуляторные органы ИКТ находятся в этом вопросе на лидирующих позициях.
- Во всех регионах подавляющее большинство регуляторных органов ИКТ несут ответственность за рассмотрение претензий со стороны потребителей. Там, где существует отдельный орган по защите прав потребителей, он нередко не имеет полномочий самостоятельно рассматривать вопросы защиты потребителей применительно к услугам сектора электросвязи/ИКТ – чаще такими полномочиями либо наделяется исключительно регуляторный орган ИКТ, либо (в большинстве случаев) они делятся между двумя этими органами. Иными словами, регуляторные органы ИКТ, как правило, сотрудничают с органами по защите прав потребителей.

На рисунке 4.1 представлена доля регуляторных органов (в процентах), сообщивших в ходе обследований, которые МСЭ проводил в 2007 и 2019 годах, об участии в той или иной деятельности, касающейся вопросов защиты прав потребителей. В период между первым и вторым обследованиями наблюдалась активизация всех видов такой деятельности. В целом представляется, что большинство регуляторных органов ИКТ уже активно занимаются вопросами защиты прав потребителей, а те, кто пока этого не делает, имеют много примеров для подражания.

Более подробно эти и другие связанные с этим тенденции рассматриваются в отчете МСЭ о сотрудничестве в сфере регулирования за 2018 год (ITU 2018a¹⁴).

¹¹ В настоящей главе понятие "нормы регулирования" включает условия соответствующих лицензий.

¹² Эти вопросы рассматриваются в тематическом разделе "Права потребителей в цифровой среде" *Платформы цифрового регулирования*.

¹³ Юридическая компания DLA Piper разработала полезный инструмент для сопоставления законов о защите прав потребителей в разных странах мира (см. <https://www.dlapiperdataprotection.com/#handbook/world-map-section>).

¹⁴ См., в частности, главы 4 и 5: в главе 4 – раздел "Developments in the field of consumer protection" (Процессы в сфере защиты прав потребителей) (pp. 53–55), а в главе 5 – раздел 5.3 "Power coupling: the ICT regulator and the consumer protection authority" (Объединение сил: регуляторный орган ИКТ и орган по защите прав потребителей) (pp. 133–134).

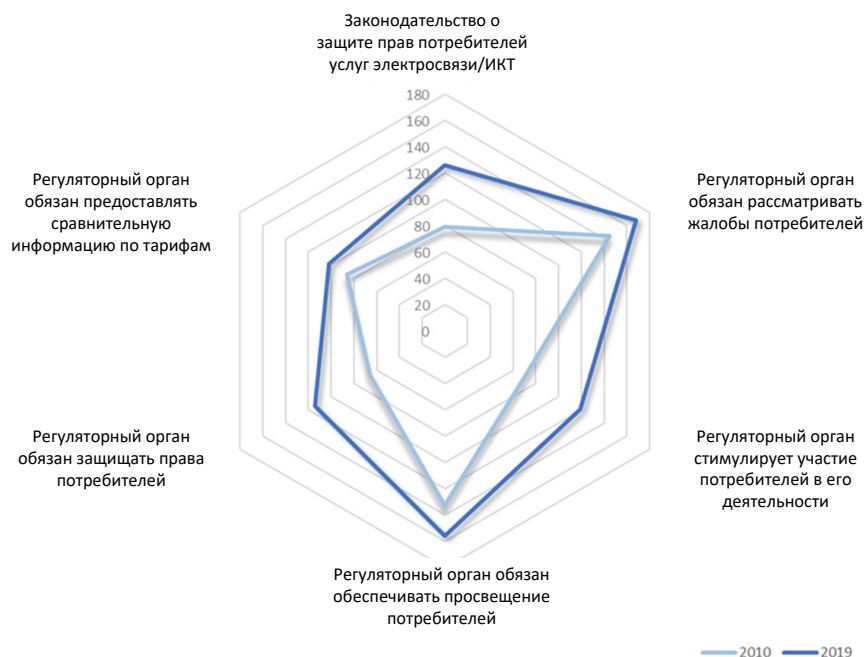
Таблица 4.2. Ответственность за вопросы, связанные с защитой потребителей услуг ИКТ, и соответствующее законодательство в странах мира

		Африка и Арабский регион	Азиатско-Тихоокеанский регион и СНГ	Северная и Южная Америка	Европа
Общее количество стран региона		65	49	35	46
Данные обследования МСЭ 2019 года о мерах по защите прав потребителей					
Ответственность за вопросы защиты прав потребителей в секторе электросвязи/ИКТ (%)	Регуляторный орган электросвязи/ИКТ	62	29	34	26
	Орган по защите прав потребителей	5	6	20	9
	Оба органа	17	24	31	48
Существует отдельный орган по защите прав потребителей (%)		31	41	57	72
За рассмотрение жалоб потребителей отвечает регуляторный орган (%)		91	76	83	85
Существует особое законодательство/подзаконные акты по защите потребителей в области электросвязи (%)		65	55	46	83
Данные краткого обзора ЮНКТАД о принятии законодательства об электронной торговле в странах мира					
Существует общий закон о защите прав потребителей (%)		42	31	80	74
Существует закон о защите данных/неприкосновенности частной жизни (%)		51	45	77	91
Существует закон об электронных сделках (%)		71	69	94	91
Существует закон о киберпреступности (%)		69	67	86	91

Источник: на основании данных МСЭ и ЮНКТАД.

Примечание. – Данные ЮНКТАД получены 21 мая 2020 года на веб-сайте https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx (данные постоянно обновляются). Фраза "существует закон" означает, что был получен положительный ответ. Данные МСЭ взяты из ответов, полученных в ходе обследования 2019 года.

Рисунок 4.1. Сообщения регуляторных органов ИКТ о деятельности, связанной с вопросами защиты прав потребителей, 2010 и 2019 годы



Источник: МСЭ.

Среднестатистические потребители и уязвимые потребители

Законодательство о защите прав потребителей часто ориентируется на абстрактных *среднестатистических потребителей*, которые, как предполагается, являются "разумными и осмотрительными" и могут позаботиться о себе. Вместе с тем регуляторные органы уделяют все больше внимания *уязвимым потребителям*, которые, вероятно, чаще, чем среднестатистические потребители, испытывают затруднения в определенных ситуациях. Категория уязвимых потребителей может определяться по-разному. Например, люди с пониженным слухом чаще, чем обычные потребители, испытывают сложности с голосовой беседой, а малообеспеченные лица с большей вероятностью, чем среднестатистические потребители, прекратят пользоваться услугой, если цена на нее повысится. Любой человек может на какое-то время оказаться уязвимым, например, из-за потери работы или утраты близких.

То, как регуляторным органам следует соотносить внимание, уделяемое интересам уязвимых потребителей в сравнении со среднестатистическими (или привилегированными) потребителями, нередко является проблемой политического характера. Законодательство, построенное на принципах равноправия, часто требует разумного учета потребностей лиц с ограниченными возможностями, а правительства могут предоставить руководящие указания по вопросам социальной политики. Экономический анализ предполагает допущения относительно совокупной пользы или совокупного благосостояния, которые могут не совпадать с интуитивными представлениями об этих вопросах¹⁵. Какой бы экономический подход ни применялся, регуляторным органам необходимо четко осознавать, что среди потребителей существуют огромные различия с точки зрения их поведения вообще и поведения в цифровой среде, желаний и ресурсов, и оценивать последствия политических решений для различных категорий потребителей, в том числе наиболее уязвимых¹⁶.

¹⁵ Подробнее о подходе с точки зрения взвешенного благосостояния, основной принцип которого — представление, что повышение цены на 1 долл. США является более значимым для лица, располагающего 10 долл. США, чем для лица, располагающего 100 долл. США, см. в Cowell and Gardiner (1999).

¹⁶ См., например, Ofcom (2019) и UKRN (2020). Последняя публикация — это хороший пример сотрудничества в сфере регулирования и использования данных, равно как и учета уязвимости пользователей.

Переход к использованию онлайн-данных

В последнее десятилетие серьезно изменились показатели внедрения цифровых услуг и их использования потребителями¹⁷. На рынке, где прежде ведущее положение занимала голосовая телефонная связь, теперь доминируют данные. Голосовая связь по-прежнему остается весьма популярным средством связи, но теперь ее часто осуществляют по протоколу Интернет (IP) и оплачивают в составе пакета услуг интернета или пакета данных. Защита интересов потребителей в том, что касается данных, – это лишь одна из целого ряда мер политического характера, необходимых для содействия в развитии безопасной и эффективной экономики, основанной на данных¹⁸.

Электронные средства связи всегда создавали проблемы, касающиеся конфиденциальности и связанные как с контентом, так и со сложившимися условиями (то есть метаданные, в число которых обычно входят номер абонента и номер вызываемого лица, а также время, дата, продолжительность и место вызова).

Сегодня пользование интернетом (часто через приложения) привело к резкому увеличению как объема, так и видов данных, которые поставщики могут собирать о потребителях. Зачастую к числу таких данных относятся местонахождение потребителей, их интересы, история просмотров веб-страниц и финансовые операции, а также их контакты в социальных сетях. Кроме того, "умные" объекты, такие как голосовые помощники в доме и камеры видеонаблюдения и подключенные автомобили на улицах, могут собирать и передавать информацию о людях, не подозревающих о сборе подобных данных. Эти так называемые большие данные в совокупности поступают на еще более мощные устройства обработки данных, которые, применяя технологии искусственного интеллекта (ИИ), могут сегодня выделять общие характеристики таких данных и делать вероятностные выводы о группах и отдельных физических лицах.

Такие серьезные изменения могут идти как во благо, так и во вред потребителям¹⁹. Наиболее известным примером из опыта 2020 года является использование данных в борьбе с глобальной пандемией COVID-19 – это может помочь в выявлении потенциальной инфекции, но одновременно вызывает обеспокоенность по поводу несанкционированного наблюдения. Многие страны вводят в действие или ужесточают законодательство о защите данных, а также создают специальные регуляторные органы по защите данных или расширяют их полномочия²⁰. Параллельно с этим по всему миру идут дебаты в отношении этического аспекта использования данных.

4.2 Система поддержки потребителей

Задачи в области защиты потребителей цифровых услуг и расширении их прав и возможностей

В документе МСЭ (ITU 2018a) наглядно показано, что в разных странах действуют разные институциональные механизмы решения проблем защиты потребителей – как общего характера, так и отраслевые; одной из отраслей (связанной с множеством других) является цифровая. Любая институциональная система призвана решать определенный круг задач. В таблице 4.3 формулируются конкретные задачи и определяются типовые структуры, на которые может быть возложено их решение. Общинные объединения и социальные сети могут быть весьма полезными инструментами, позволяющими поделиться опасениями и информацией, но при этом возникают и риски ненамеренного или сознательного введения в заблуждение, что вновь подтверждается примерами, связанными с пандемией COVID-19.

¹⁷ См., например, главу 3, рисунок 3.1 "Количество физических лиц, пользующихся интернетом, и темпы роста этого показателя".

¹⁸ См. главу 5 "Защита данных и доверие".

¹⁹ См. World Bank (2019a).

²⁰ См. ITU (2018a), главы 4 и 5, в которых рассматриваются круг ведения и полномочия регуляторных органов ИКТ и их взаимоотношения с другими регуляторными органами.

Таблица 4.3. Круг задач в отношении защиты потребителей цифровых услуг

Задачи в отношении защиты потребителей цифровых услуг	Структуры, в полномочия которых обычно входит решение этих задач
Политика в отношении потребителей и отраслевая политика	Министерства (при активном участии общественности), антимонопольное ведомство
Изучение запросов потребителей	Объединения потребителей, регуляторные органы , поставщики услуг
Законодательство о защите прав потребителей	Исполнительная ветвь власти, парламент, суды
Нормы и правила по защите прав потребителей	Регуляторные органы , ассоциации поставщиков услуг, организации по стандартизации
Информирование потребителей	Поставщики услуг, веб-сайты, на которых сопоставляются цены на товары и приводятся отзывы о них, сетевые форумы, объединения потребителей, регуляторные органы
Просвещение потребителей	Школы и вузы, телерадиовещательные компании, пресса, регуляторные органы
Мониторинг функционирования рынка	Поставщики услуг, регуляторные органы , антимонопольное ведомство
Рассмотрение жалоб	Поставщики услуг, регуляторные органы , органы по альтернативному урегулированию споров, суды
Обеспечение соблюдения законов и норм	Регуляторные органы , местные органы власти, полиция, суды

В таблице 4.3 понятие "регуляторные органы" включает все регуляторные органы, занимающиеся защитой интересов потребителей в процессе их взаимодействия с поставщиками посредством цифровых технологий. К числу таких регуляторных органов относятся органы по защите прав потребителей, регуляторные органы по защите данных, регуляторы финансовых услуг, а нередко и другие структуры, например регуляторные органы в сфере энергетики, если потребители взаимодействуют с поставщиками электроэнергии в онлайн-режиме. Обычно регуляторный орган ИКТ выполняет все перечисленные выше функции, касающиеся обеспечения возможности соединений, а также решает некоторые вопросы в отношении онлайн-контента, и ему необходимо работать в тесном сотрудничестве с другими упомянутыми в таблице структурами, в том числе с другими регуляторными органами.

Взаимоотношения между потребителями и поставщиками услуг

Компании часто заявляют, что они знают своих потребителей и потенциальных потребителей лучше, чем какие бы то ни было регуляторные органы, и поэтому регуляторным органам нет необходимости заниматься изучением потребителей или консультировать их. Первое здесь верно: у компаний есть и стимулы, и средства, чтобы разобраться, что именно нужно их потребителям. Однако из первого еще не следует второе. Очевидно, что компаниям важно знать только своих собственных потребителей (или, возможно, потребителей своих непосредственных конкурентов) и направлять ресурсы в наиболее доходные сегменты рынка. Для выполнения возложенных на них обязанностей регуляторным органам необходимо изучать нужды всех потребителей и потенциальных потребителей, в том числе и находящихся "в основании пирамиды" и не слишком интересующих некоторых поставщиков услуг.

Регуляторные органы не должны вставать между компаниями и потребителями, за исключением тех случаев, когда прямые взаимоотношения между ними заходят в тупик (или, в исключительных случаях, когда есть основания подозревать серьезные неправомерные действия). Удовлетворенные потребители — это лучший способ рекламы для компании: доброжелательный прием претензий, принятие решения по каждому обращению индивидуально и использование их в качестве источника для сбора сведений о рынке помогают улучшить качество обслуживания клиентов и повысить конкурентоспособность. Регуляторным органам следует содействовать успешному развитию таких взаимоотношений, поддерживая диалог и с потребителями, и с поставщиками услуг. Цифровые средства массовой информации, например опросы в сети, могут быть полезны для выстраивания диалога с потребителями, но при этом важно знать, какие категории потребителей участвуют в таких опросах, а какие не имеют такой возможности.

Функции регуляторных органов в области ИКТ

Ниже приводится перечень конкретных функций регуляторных органов ИКТ. Как было сказано выше, значимость этих структур повышается, и сегодня в сферу их полномочий зачастую входят вопросы, связанные с контентом и данными, равно как и с возможностью установления соединений. Что еще важнее, цифровая среда может сегодня помочь им лучше справляться со своими задачами, например, за счет краудсорсинга мнений потребителей о качестве услуг.

- Регулирование порядка рассмотрения компаниями жалоб от потребителей на качество услуг и мониторинг соблюдения норм регулирования.
- Исполнение или содействие исполнению функций последней инстанции при рассмотрении сложных дел по жалобам потребителей.
- Мониторинг жалоб, поступающих по всем соответствующим каналам, в целях оценки эффективности процедур, отслеживания тенденций и выявления вновь возникающих проблем.
- Создание специальной страницы на своем веб-сайте или отдельного веб-сайта, где потребители имеют возможность получить в интерактивном режиме консультации по своим проблемам. Здесь могут быть размещены, например, списки поставщиков, предоставляющих услуги в конкретных районах или имеющих специальные предложения, в том числе для групп с особыми потребностями (например, для лиц с определенным видом инвалидности), а также перечни наиболее выгодных покупок для отдельных видов использования.
- Помощь в создании местных, региональных или национальных объединений потребителей, поддержка отдельных пользователей, сталкивающихся с проблемами, и сбор мнений потребителей по вопросам, связанным с цифровыми услугами.
- Взаимодействие с такими группами в целях оказания им содействия в просвещении потребителей и выяснения их мнения об эффективности текущих мер политики.
- Проведение целевых исследований для выявления приоритетов и предпочтений потребителей, а также сбор сведений о любой другой подобной деятельности, в том числе о поведенческих исследованиях.
- Разработка в тесном сотрудничестве с объединениями потребителей и органами по защите прав потребителей (там, где они существуют) нормативных актов и сводов правил в области расширения прав и возможностей потребителей и их защиты.
- Привлечение объединений потребителей к консультациям по вопросам политики и поощрение выражения ими своего мнения, особенно в тех случаях, когда соответствующая политика напрямую затрагивает потребителей.
- Сотрудничество с другими структурами, чтобы помочь потребителям должным образом определить, куда им следует обращаться за необходимой поддержкой.

Соответствующие международные органы

Международные органы могут оказывать национальным регуляторным органам разнообразную помощь в рассмотрении вопросов, касающихся защиты потребителей, в том числе²¹:

- обеспечение учета интересов потребителей в нормах, регулирующих международную торговлю и сотрудничество, – например, Конференция Организации Объединенных Наций по торговле и развитию (ЮНКТАД) и Трансатлантический диалог потребителей (ТАСД);
- взаимная поддержка усилий по обеспечению соблюдения норм в отношении трансграничной электронной торговли и борьбы с незаконной деятельностью – например, Международная сеть защиты прав потребителей и правоприменительной практики (ICPEN) и Сеть по противодействию нежелательным сообщениям (UCENET);

²¹ Более подробную информацию об этом и полезные ссылки см. в тематическом разделе "Международные организации, занимающиеся вопросами защиты потребителей" *Платформы цифрового регулирования*.

- разработка международных стандартов, в том числе в отношении ИКТ и соответствующих цифровых продуктов и услуг, – например, МСЭ, Международная организация по стандартизации (ИСО) и ANEC (структура, выражающая мнение европейских потребителей по вопросам стандартизации);
- организация обучения и подбор примеров наиболее эффективной практики в сфере ИКТ и вопросов, касающихся потребителей цифровых услуг, прежде всего для регуляторных органов и других официальных структур – например, МСЭ;
- разработка правовых и политических рамок для рассмотрения вопросов, касающихся потребителей, обеспечение их повсеместного внедрения и применения – например, ЕС и ОЭСР;
- выражение мнений потребителей в отношении вопросов, связанных с ИКТ и цифровой средой, – например, Международный союз потребителей и BEUC (Европейская организация потребителей).

Полезную роль играют и многие другие международные организации, прежде всего региональные ассоциации.

4.3 Конкретные проблемы, касающиеся потребителей

Цена и качество услуг

Цена, как правило, является для потребителей самым главным фактором при выборе услуги и пользовании ею. Дешевые пакеты привлекательны для многих потребителей даже в том случае, когда низкая цена подразумевает и более низкое качество. Для привлечения первых клиентов цены, предлагаемые вновь выходящими на рынок компаниями, как правило, на несколько процентных пунктов ниже цен операторов, занимающих существенное положение на рынке, и конкурентная борьба почти всегда ведется вокруг цен, равно как и вокруг характеристик услуги.

Роль регуляторных органов в контроле и мониторинге цен рассматривается в другом разделе настоящего Справочника²². Регуляторным органам следует и далее помогать потребителям, добиваясь, чтобы информация о ценах поставщиков была доступной, понятной и точной. Веб-сайты сравнения цен могут помочь потребителям выбрать оптимального для них поставщика и оптимальный пакет услуг, как правило, только путем сопоставления цен; некоторые регуляторные органы предоставляют такие сведения, тогда как другие стимулируют к этому поставщиков или коммерческие организации²³. В другой главе настоящего Справочника рассматривается вопрос о том, каким образом регуляторные органы могут помочь потребителям оценить, на какое качество обслуживания им следует рассчитывать²⁴.

Вопрос о контенте с "нулевым рейтингом", который бесплатно предоставляют пользователям некоторые поставщики услуг, например Facebook в рамках базового бесплатного набора услуг, вызвал неоднозначную реакцию²⁵. С одной стороны, многие пользователи, особенно относящиеся к менее обеспеченным группам населения и пользующиеся тарифами с ограниченным объемом данных, приветствовали это предложение, а в некоторых странах оно, по-видимому, способствовало ускорению распространения интернета, а также расширению использования Facebook. С другой стороны, некоторые регуляторные органы считают такие предложения дискриминационными и противоречащими принципу сетевого нейтралитета; ярким примером развивающейся страны, запретившей на этом основании контент с "нулевым рейтингом", служит Индия. В исследовании ОЭСР (OECD 2019a) был сделан вывод, что "эффект от «нулевого рейтинга» может быть весьма разнообразным и в значительной степени зависит от ситуации в той или иной стране..." и что "анализ каждого отдельного случая является практически обязательным". Несколько ранее Альянс за доступный интернет (A4AI) провел собственное исследование, в котором пришел к аналогичным выводам, а также дал регуляторным органам рекомендации по использованию "нулевого рейтинга" для расширения доступа при одновременном сохранении конкуренции.

²² См. главу 2 "Конкуренция и экономика".

²³ См., например: <https://www.comreg.ie/compare/#/services> (веб-сайт Комиссии по вопросам регулирования связи Ирландии); <http://www.anacom.pt/tarifarios/PaginalInicial.do> (веб-сайт Национального органа связи Португалии (ANACOM)); или <https://www.meilleurtarif.be/> (веб-сайт Бельгийского института почтовых услуг и электросвязи (BIPT)). По мере того как на рынках появляется больше поставщиков услуг и предлагаются более разнообразные пакеты услуг, проводить сравнения становится все сложнее, и некоторые регуляторные органы передали эту работу внешним поставщикам, как, например, чешский регуляторный орган (см. <https://www.ctu.eu/price-calculators>). Возможно, в процессе перестройки находится и прежде образцово действовавшая система LetsCompare (см. www.consumerinfo.my).

²⁴ См. главу 8 "Техническое регулирование", в которой рассматривается вопрос качества обслуживания.

²⁵ Как и более обширная тема сетевого нейтралитета, включающая "нулевой рейтинг" и рассмотренная в главе 2.

Контракты и предоплата

Первоначально отношения между поставщиками услуг и потребителями требовали заключения подробных соглашений в письменной форме, известных как контракты. Они по-прежнему широко распространены и зачастую являются предпочтительным вариантом для поставщиков соединений, поскольку обеспечивают прогнозируемый поток доходов. Как правило, они позволяют потребителям в конце каждого месяца вносить плату за пользование услугой, которая уже была им оказана; этот механизм известен как кредит или последующая оплата.

После заключения контракты с последующей оплатой могут действовать без ограничения срока (до расторжения одной из сторон, как правило, по истечении определенного срока уведомления), или в течение установленного периода, обычно составляющего год или более. Регуляторные органы могут ограничивать срок действия контрактов, поскольку контракты с чрезмерно продолжительным сроком действия могут ослабить конкуренцию и препятствовать выходу потребителей из сделок, которые перестали их устраивать.

С момента своего появления в 1990-х годах предоплатная модель предоставления услуг подвижной связи приобрела чрезвычайную популярность во всем мире, поскольку она гарантирует пользователям отсутствие у них долгов, обходит формальности традиционных контрактов и предоставляет потребителям возможность гораздо более гибкого расходования средств²⁶. Хотя эту модель особенно ценят менее обеспеченные потребители, защита прав потребителей в рамках взаимоотношений на предоплатной основе развита заметно слабее, чем в рамках контрактов с последующей оплатой. Некоторые регуляторные органы приняли меры в этой сфере; так, в Индии TRAI²⁷ предписывает операторам использовать стандартный цветовой код для предоплаченных ваучеров, чтобы эти тарифы были более понятны потребителям, а также предоставлять потребителям как текущие, так и ретроспективные данные о том, как пользование услугами влияет на остаток средств на их лицевых счетах.

В частности, в сфере электронной коммерции условия договоров (часто размещаемые на сетевых ресурсах) нередко являются источником раздражения и жалоб. Они зачастую неоправданно длинны и сложны, потребители редко их читают, и у них часто возникает ощущение, что им не остается ничего другого, как принять их²⁸. Правительство Соединенного Королевства опубликовало материалы (Behavioural Insights Team 2019), содержащие практические рекомендации по улучшению этой ситуации, и в настоящее время на их основе ведется разработка международного стандарта.

Порядок выставления счетов и осуществления платежей

Цифровые платежи за полученный цифровой контент и услуги связи часто можно проводить через поставщиков соединений. Оплата покупок из приложений может происходить с использованием специализированных виртуальных валют, однако в конечном итоге счет потребителя, возможно, потребуется пополнить извне "реальными" деньгами, вначале конвертировав их в электронные деньги, например, с помощью счета в системе мобильных платежей, такой как M-Pesa в Кении и других странах. Общепринятый механизм приема платежей включает звонки и сообщения, за которые взимается дополнительная плата, часть которой передается поставщику контента. Этот метод и альтернативные способы²⁹, позволяющие производить оплату через поставщика соединений, привели к недовольству многих потребителей, которое зачастую связано с тем, что поставщик контента может "спрятаться" за поставщика соединений и даже исчезнуть. Существуют различные системы защиты прав потребителей³⁰, часто предполагающие совместное регулирование, но в целом наблюдается тенденция к отказу от этих косвенных платежных механизмов в пользу приложений для мобильных платежей, таких как mPay Wallet в Малайзии, которые обычно регулируются аналогично финансовым учреждениям.

²⁶ См. тематический раздел "Предоплатная модель предоставления услуг подвижной связи" *Платформы цифрового регулирования*.

²⁷ См. TRAI (2018), глава 1.

²⁸ См., например, Which? (2018).

²⁹ Например, применяемый в Соединенном Королевстве механизм мобильных платежей Payforit, принцип действия которого разъясняется здесь: https://www.resolver.co.uk/consumer-rights/three_pay_monthly-payforit-complaints.

³⁰ Характерным примером является регуляторный орган Соединенного Королевства, занимающийся регулированием услуг с оплатой по повышенному тарифу, – PhonePaid Services Authority. Обзор регуляторных механизмов в 20 странах за 2011 год доступен по адресу: <https://psauthority.org.uk/-/media/Files/PhonepayPlus/Research/Mason-International-Markets.pdf?la=en&hash=3AAF54A57288481AE77FA4727BF4226020033F47>.

Доступные потребителям варианты осуществления платежей в пользу поставщиков услуг могут также существенно влиять на привлекательность этих услуг. В идеале следует принимать оплату как в наличной форме, так и в виде электронных платежей, без взимания существенных комиссий. Сроки оплаты счетов при системе с последующей оплатой должны быть разумными и учитывать возможные задержки с доставкой (особенно для бумажных счетов).

В случае неоспариваемой неоплаты выставленных счетов или длительного неиспользования услуги поставщики услуг могут приступить к процедуре ограничения предоставления услуг и, в конечном итоге, к их отключению. Регуляторным органам ИКТ следует убедиться в том, что эти процедуры справедливы и понятны для потребителей, в отношении которых они применяются, чтобы потребители имели разумные возможности восстановления обслуживания в полном объеме.

Разумеется, взимаемые с клиентов суммы должны точно соответствовать выбранному ими тарифному плану и услугам, доступ к которым предоставляется на его основе, а любая дополнительная плата за пользование должна очевидным образом соответствовать фактическому использованию. Значительная часть жалоб потребителей связана, как правило, с неправильным выставлением счетов.

Обслуживание клиентов, рассмотрение жалоб и возмещение ущерба

Клиентам необходимо иметь возможность взаимодействия со своими поставщиками услуг и получения от них своевременных ответов. В идеальном варианте поставщики услуг предоставляют своим клиентам на выбор ряд различных каналов связи, к которым относятся, например, центры обслуживания, телефон, электронная почта, текстовые сообщения или онлайн-обмен сообщениями. Такие варианты имеют особое значение в тех случаях, когда у клиента возникает проблема, в результате которой он не может воспользоваться предоставляемой ему услугой, например, чтобы сообщить о сбое или возобновить пользование отключенной услугой. Качество обслуживания клиентов является важным аспектом общего качества обслуживания, и, как и в случае с другими аспектами качества обслуживания, регуляторные органы могут в той или иной степени вмешиваться в работу рынков.

Однако рассмотрение жалоб часто требует вмешательства регуляторных органов, поскольку рыночные стимулы надлежащего обращения поставщиков услуг с неудовлетворенными клиентами слишком слабы. Как правило, регуляторные органы требуют, чтобы поставщики услуг подтверждали получение жалоб и отвечали на них в течение определенного срока, а также организуют или предоставляют возможность дополнительного рассмотрения жалоб, которые не были разрешены поставщиками услуг удовлетворительным для клиентов образом. Возмещение ущерба может принимать различные формы, включая принесение извинений, исправление ошибок и выплату компенсаций³¹.

Как упоминалось выше, наибольшее количество жалоб, поступающих в регуляторные органы, как правило, связаны с выставлением счетов и осуществлением платежей; второе место занимают жалобы по вопросам качества сетевых услуг и качества обслуживания клиентов. Однако за последнее десятилетие, в частности, в некоторых англоговорящих юрисдикциях серьезную проблему стали представлять нежелательные звонки и сообщения коммерческого характера, которые в настоящее время распространяются на все большее количество стран. Чаще всего они представляют собой попытки телефонного маркетинга (или выглядят схожим образом), но некоторые из них носят откровенно мошеннический характер (например, звонки "wangiri", которые обрываются до того, как на них успевают ответить, поощряя дорогостоящий ответный звонок, доход от которого идет в пользу мошенника).

В качестве профилактической меры часто применяются списки "не звонить"³², в которые потребители, не желающие получать незапрашиваемые звонки или сообщения коммерческого характера, могут внести свой номер телефона, и в этом случае подлинные телемаркетинговые структуры не имеют права им звонить. Автоматические звонки (известные как автообзвон) также являются незаконными во многих юрисдикциях. Однако злоумышленники с легкостью обходят эти правила, поэтому имеющиеся механизмы по обеспечению их соблюдения приходится концентрировать в тех сферах, где они дают максимум отдачи.

³¹ Более подробно этот вопрос, а также рассмотрение коллективных жалоб и коллективного возмещения ущерба рассматриваются в тематическом разделе "Возмещение ущерба" *Платформы цифрового регулирования*.

³² Также известные как "списки Робинзона", названные так по имени героя произведения Даниэля Дефо Робинзона Крузо, который много лет прожил в одиночестве на острове.

Все чаще в сетях, приложениях и оконечном оборудовании применяются технические меры, чтобы нежелательные вызовы не могли достичь своей цели³³.

Содействие потребителям в ориентации в цифровой экономике

В одной финансовой операции потребителя цифрового продукта (например, оплате доступа к музыкальной композиции) может принимать участие длинная цепочка поставщиков услуг (в данном примере это исполнитель исходной композиции, студии звукозаписи, агентства, агрегаторы контента, интернет-магазины, структуры, управляющие счетами в онлайн-платежных системах, и поставщики услуг интернета). Если потребителю требуется консультация до момента покупки или что-то идет не так, например происходит двойное списание средств, к какой структуре следует обратиться потребителю и как ее найти? В этом может помочь система "одного окна", которая направит потребителей в нужном направлении.

МСЭ подчеркнул³⁴ важность совместной работы регуляторных органов в различных секторах и на различных уровнях, которая приобретает особую актуальность при оказании помощи потребителям, чтобы они могли справиться с проблемой самостоятельно. Эта ситуация сложна даже для экспертов, и большинство людей не могут разобраться в ней без посторонней помощи.

Всем структурам – коммерческим, государственным или НПО, предлагающим помощь потребителям, должен быть как минимум предоставлен доступ к постоянно обновляемой совместно используемой базе данных, в которой определено, за какую тему отвечает каждая из структур. Как правило, удобнее всего, если эта совместно используемая база данных размещена в интернете, а потребителям может быть предоставлен непосредственный доступ к одной из ее версий³⁵. Она также должна служить ценным источником информации для организаций и телефонных горячих линий, которые предоставляют консультации и поддержку потребителям, способствуя обеспечению последовательного подхода.

Поиск в интернете поможет продвинутым интернет-пользователям найти то, что им нужно, однако многие люди по-прежнему предпочитают использовать голосовые услуги (или могут использовать только их). В идеальном варианте для поддержки потребителей создается широко разрекламированная горячая линия с легко запоминающимся номером, звонок на который будет бесплатным. Запросы можно отправлять с использованием интерактивного голосового ответа или чат-ботов. В идеале обращающимся в службу поддержки также следует предоставлять возможность пообщаться с компетентными и отзывчивыми "живыми" операторами, разговаривающими на их языке, однако это, по всей вероятности, приведет к росту затрат. Для ограничения спроса на "живых" операторов можно выделить особые номера для людей, которые в наибольшей степени нуждаются в их помощи, например для людей с определенными ограничениями возможностей.

Добросовестные предприниматели выиграют от хорошей осведомленности и уверенности потребителей и могут осуществлять добровольные взносы в денежной или натуральной форме на цели оказания поддержки потребителям. Регуляторные органы также могут требовать осуществления таких взносов; например, индийский регуляторный орган TRAI требует, чтобы поставщики услуг вносили в Фонд защиты прав и просвещения потребителей любые суммы, которые причитаются потребителям, но не могут быть им выплачены³⁶. Защита прав потребителей и их просвещение могут представлять собой еще один вариант использования средств фондов универсального доступа и обслуживания³⁷.

Положения, касающиеся потребителей с ограниченными возможностями

Старение населения планеты неизбежно влечет за собой увеличение доли людей, имеющих некоторые нарушения: физические (например, потеря конечности), сенсорные (например, слепота или глухота) или когнитивные (например, дислексия). Конвенция Организации Объединенных Наций о правах инвалидов

³³ Эта тема рассматривалась в публикации МСЭ (2017b), где описывались меры, принятые в период с 2014 по 2017 год, и будет рассмотрена более детально в последующем томе данной публикации. Описание ситуации в международном масштабе в 2016 году см. в Milne (2016).

³⁴ Например, в публикации ITU (2018a).

³⁵ С примером из практики Соединенного Королевства можно ознакомиться по адресу: <https://www.iwf.org.uk/resources/useful-links>.

³⁶ См. пресс-релиз TRAI в отношении поправки, внесенной в январе 2020 года, по адресу: https://trai.gov.in/sites/default/files/PR_No.08of2020.pdf.

³⁷ См. главу 3 "Доступ для всех".

требует обеспечения равного обращения для лиц с ограниченными возможностями³⁸, а конкретные законы и нормативные акты обычно разъясняют, что это должно означать на практике.

Часто первое конкретное признание особых потребностей людей с ограниченными возможностями со стороны регуляторных органов ИКТ происходило в рамках политики обеспечения универсального доступа³⁹. Регуляторные органы также все чаще реализуют политику доступности ИКТ, которая может касаться, например, специального оборудования и удобства использования онлайн-ресурсов. Согласно данным обследования МСЭ, проведенного в 2019 году, только у 29% из 195 регуляторных органов по всему миру отсутствовала стратегическая концепция доступности ИКТ, при этом отдельное внимание уделялось подвижной связи, ТВ- и видеопрограммам, доступности интернета и доступности услуг ИКТ в общественных местах, а также другим аспектам. Однако в Африке процентная доля регуляторных органов, не имеющих стратегической концепции доступности, достигла 48%.

В рамках южноафриканского регуляторного органа ICASA действует Консультативный совет потребителей⁴⁰, в состав которого входят представители лиц с ограниченными возможностями. ICASA также разработал всеобъемлющий Кодекс защиты прав лиц с ограниченными возможностями⁴¹, в котором перечислены различные требования к операторам в целях удовлетворения особых потребностей.

В Австралии уже давно существует активное движение лиц с ограниченными возможностями и действует режим, учитывающий особые потребности. На специальном веб-сайте о "доступной электросвязи"⁴² представлены как широкий спектр оборудования и услуг, так и понятные и доступные пояснения. Регуляторный орган утвердил ряд отраслевых сводов норм и правил в отношении доступности⁴³. Обязательным является соблюдение требований к представлению информации (чтобы дать людям возможность выбрать оборудование, в наибольшей степени соответствующее определенным потребностям).

Цифровые технологии могут не только обеспечить равный доступ, но и компенсировать инвалидность и улучшить жизнь людей за счет широкого спектра социальных и экономических благ. Так, недавно проведенное исследование, целью которого являлось обеспечение возможности использования технологии "умного" дома людьми с потерей слуха, подчеркнуло важность разработки базовых технологий с гибкими пользовательскими интерфейсами⁴⁴. Например, следует предусмотреть возможность визуального выражения звуковых сигналов для пользователя.

"Умные" пользовательские устройства

Регулирование электросвязи сосредоточено на сетях, а не на оборудовании. Нормативные обязанности в отношении устройств обычно ограничиваются обеспечением их соответствия стандартам, разработанным для защиты пользователей и сетей и борьбы с контрафакцией. В главе 6 "Управление использованием спектра" рассматривается важный вопрос радиационной безопасности излучения электромагнитных полей (ЭМП). Потребители имеют право на получение надежных и независимых советов по безопасному использованию беспроводных устройств, особенно с появлением сетей 5G.

Появление "умных" устройств ставит вопрос о расширении сферы ведения регуляторных органов на другие аспекты связанных с устройствами вопросов, имеющих существенное значение для конкуренции и потребителей. Французский регуляторный орган ARCEP изучил, в какой мере устройства ограничивают открытость интернета (например, в связи с необходимостью обеспечить совместимость приложений с проприетарными операционными системами), и рекомендовал меры по ограничению этого ущерба (ARCEP 2018⁴⁵).

³⁸ <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html>.

³⁹ См. главу 3 "Доступ для всех".

⁴⁰ <https://www.icasa.org.za/pages/consumer-advisory-panel>

⁴¹ <https://www.icasa.org.za/uploads/files/Code-for-People-Disabilities-2014.pdf>

⁴² При поддержке как регуляторного органа ACMA, так и организации потребителей ACCAN. <https://www.accessibletelecoms.ideas.org.au/telecom-home.html>

⁴³ Их разработку и поддержку осуществляет отраслевой Альянс связи. <https://www.commsalliance.com.au/Documents/Publications-by-Topic/accessibility>

⁴⁴ <https://petras-iot.org/update/people-with-hearing-loss-and-connected-home-technologies/>

⁴⁵ Вводная информация по этим вопросам в формате комиксов представлена по адресу: https://en.arcep.fr/uploads/tx_gspublication/comic-strip-devices-feb2018-ENG.pdf.

Но multifunctional смартфоны уже получили повсеместное распространение. Они используются не только в качестве телефонов, но и как камеры, часы, калькуляторы, телевизоры, радиоприемники и навигаторы, а также предоставляют доступ к интернету, часто при помощи приложений. В настоящее время к смартфонам привязываются "умные" часы, "умные" колонки и другие подключенные устройства, используемые дома или в дороге, которые активно применяются потребителями в развитых странах и распространяются по всему миру.

Эти возможности открывают для потребителей новые способы оставаться на связи с семьей, друзьями и коллегами, а также учиться, зарабатывать, тратить, копить и играть. Но они также являются источником новых рисков, к которым относятся, например, риск потери времени и денег или риск быть введенным в заблуждение, обманутым или разочарованным. В крайних случаях эти возможности могут даже приводить к развитию зависимостей, как правило, от игр или азартных игр, или просто к чрезмерному использованию социальных сетей.

Эти сложные функции охватывают различные аспекты, показанные на рисунке 7.7 в главе 7, а приложения могут предоставлять потребителям доступ к таким разноплановым областям, как здравоохранение и сельское хозяйство⁴⁶. Регуляторные органы ИКТ не могут и не обязаны защищать и поддерживать потребителей во всех сферах, доступ к которым может предоставить смартфон. Они должны выполнять основные функции, возложенные на них в их стране, в сфере, на которую распространяется их юрисдикция, и сотрудничать с другими органами в целях расширения охвата.

Регуляторным органам также необходимо помнить, что характер доступа к "умным" устройствам и их использования по-прежнему далек от всеобщего. Даже в развитых странах с фактически всеобщим доступом к приемлемым в ценовом отношении услугам фиксированной и подвижной широкополосной связи часть потребителей не пользуются интернетом, будь то по собственному желанию или из-за препятствий, таких как инвалидность или отсутствие доверия. В менее развитых странах уровень доступности и приемлемости в ценовом отношении часто оказывается ниже, а препятствий возникает больше, что приводит к росту доли населения, не имеющего доступа в интернет. Пользование с помощью третьих лиц (например, когда молодой человек помогает представителю старшего поколения) – это один из распространенных способов воспользоваться некоторыми преимуществами цифрового мира, оставаясь при этом вне сети. Другим примером являются посреднические службы, доступные через обычные телефоны, которые, например, позволяют фермерам получить информацию о текущих ценах на урожай путем голосового взаимодействия. Такие услуги могут рассматриваться как цифровые, даже если доступ к ним не является таковым.

Для доверия необходима надежность

Процветание цифровой экономики – как и реальной – зависит от доверия потребителей, то есть их веры в то, что другие будут действовать честным и этичным образом. Доверие, в свою очередь, зависит от оценки надежности других участников. В реальном мире люди полагаются на собственные знания или рекомендации в отношении заслуживающих доверия лиц или организаций.

В сфере цифровой экономики собственные знания или рекомендации также играют роль, однако их совершенно недостаточно, поскольку других участников слишком много, они могут находиться в любом уголке планеты и могут быть не тем, чем представляются. Веб-сайты с отзывами потребителей, такие как Trustpilot и TripAdvisor, могут представлять определенную ценность, но тоже содержат элемент риска (OECD 2019b): поскольку подделывать отзывы очень легко, отраслевые кодексы поведения могут повысить их надежность, однако не позволяют решить вопрос полностью. Повысить доверие потребителей к цифровой экономике весьма непросто, не в последнюю очередь из-за повторяющихся неудач, когда негативный опыт приводит к подрыву доверия. К негативному опыту можно отнести вмешательство в подключение (например, спам и фишинг, а также нарушения безопасности, такие как вредоносное программное обеспечение или хакинг), а также трудности при осуществлении деятельности в интернете и проведении операций (например, дублирование платежей, разочаровывающий контент или несуществующие продукты). Безопасность и особенно конфиденциальность, как выяснилось, представляют собой новые серьезные проблемы для потребителей, даже если их поведение, возможно, говорит об обратном⁴⁷.

⁴⁶ Анализ экономического потенциала приложений и сложностей, связанных с их регулированием, см. в ITU (2017a).

⁴⁷ См. результаты исследования отношения и поведения потребителей, проведенного группой Which? в 2018 и 2019 годах, по адресу: <https://consumerinsight.which.co.uk/articles/consumer-data-summary>. Непосредственное отношение к этому имеют и выводы исследований в области поведенческой экономики.

Регуляторные органы ИКТ могут способствовать укреплению доверия со стороны потребителей, требуя использования передовых методов ведения бизнеса, демонстрирующих надежность, или поощряя их. Они также могут помочь в информировании потребителей, с тем чтобы они научились избегать такой неприемлемой практики, как продажа их данных, приводящая к нежелательной целевой рекламе. Там, где это возможно, они могут принимать принудительные меры в отношении злоумышленников, осуществляя трансграничное сотрудничество со своими коллегами в других местах. Крупные споры могут быть переданы на рассмотрение суда, если он имеет соответствующую юрисдикцию.

Безопасность детей в онлайн-среде

Во всем мире дети (к которым относятся лица в возрасте до 18 лет) нередко лучше, чем их учителя или родители, разбираются в использовании смартфонов и других подключенных устройств и с энтузиазмом "цифровых аборигенов" воспринимают новые технологии. Они охотно учатся, общаются и играют, используя эти технологии. Однако им еще не хватает жизненного опыта, и они могут пострадать от причиняемого ущерба. Обычно риски подразделяются на следующие четыре категории:

- риски, связанные с содержанием: дети подвергаются воздействию вредоносных материалов (таких, как порнография, а также материалы, призывающие к разжиганию ненависти и насилию);
- риски, связанные с контактом: дети оказываются вовлечены в онлайн-деятельность, инициатором которой являются взрослые (например, совращение, преследование, сексуальная эксплуатация);
- риски, связанные с поведением: дети оказываются жертвами или правонарушителями в рамках однорангового обмена (например, запугивание, сообщения сексуального характера, "порноместь");
- коммерческие риски: дети подвергаются воздействию ненадлежащей рекламы, маркетинговых схем или скрытых расходов (например, целевая реклама, мошенничество, обман).

Некоторые из них могут быть нейтрализованы законодательными мерами, например, имеющими отношение к защите данных или нежелательному контенту, но эти и другие нормы полезны только в той степени, в которой обеспечивается их соблюдение. Обеспечение быстрого удаления из интернета даже явно незаконных материалов оказалось серьезной проблемой, наилучшим путем решения которой является сотрудничество между поставщиками услуг интернета в контексте защиты детей. Европейская сеть горячих линий INHOPE насчитывает 46 национальных членских организаций, которые совместно работают над изъятием противоправных материалов⁴⁸.

Разумеется, окружающие детей взрослые стремятся защитить их от вреда, и это может приводить к строгому контролю времени работы с устройствами или даже полному запрету на пользование ими. Однако проведенные в различных странах масштабные исследования показали важность оказания детям помощи в использовании многочисленных преимуществ онлайн-деятельности⁴⁹, а также значение взвешенного и соответствующего возрасту подхода к контролю использования интернета детьми. Цель заключается в том, чтобы к достижению юношеского возраста они являлись уже вполне компетентными интернет-пользователями, которые знают не только о преимуществах, которыми они могут воспользоваться (например, поиск работы или получение дальнейшего образования), но и о том, как избежать введения в заблуждение, обмана или эксплуатации. В рамках работы, проведенной в 2019 году Рабочей группой по безопасности ребенка в онлайн-среде Комиссии по широкополосной связи⁵⁰, была принята всеобщая декларация⁵¹, где были изложены шаги, которые следует предпринять государственным и частным структурам для защиты детей в интернете, что дополняет работу МСЭ в области защиты детей в интернете⁵².

⁴⁸ <https://www.inhope.org/EN>

⁴⁹ См., например, <http://globalkidsonline.net/>. Многие другие полезные ресурсы представлены на специальном веб-сайте МСЭ, посвященном вопросам защиты детей в онлайн-среде: <http://www.itu.int/cop>.

⁵⁰ <https://www.broadbandcommission.org/workinggroups/Pages/WG1-2018.aspx>

⁵¹ <http://www.childonlinesafety.org/>

⁵² <https://www.itu.int/en/cop/Pages/guidelines.aspx>

Безопасность взрослых в онлайн-среде

Взрослые также могут быть уязвимы в отношении вредных факторов, аналогичных тем, что воздействуют в интернете на детей, особенно если они не обладают достаточным опытом или принадлежат к уязвимым группам населения. Проблемы, с которыми сталкиваются женщины в онлайн-среде, уже включают насилие через подключенные объекты⁵³.

Кроме того, выступая в роли потребителей, взрослые могут понести убытки в результате электронной коммерции или других онлайн-финансовых операций с использованием виртуальных и электронных денег (которые заслуживают, но пока, как правило, не имеют такой же правовой защиты, как "реальные" деньги). Кроме того, поскольку они являются гражданами, онлайн-рассылка сообщений, особенно в рамках социальных сетей, может оказывать влияние на их выбор во время голосования, а также на другие аспекты политического поведения.

Как и в случае с детьми, легких ответов здесь не существует. Теперь, когда интернет стал такой неотъемлемой частью жизни, ограничение доступа к нему редко бывает оправданно. Сбалансированный и эффективный подход может включать сочетание следующих действий государства:

- улучшение навыков работы в интернете и медийной грамотности, чтобы люди научились как находить в интернете то, что им нужно, так и оценивать вероятную безопасность и надежность онлайн-среды;
- обеспечение всеобщего беспрепятственного онлайн-доступа к контенту, который является законным в соответствии с национальным законодательством, с должным соблюдением социальных норм⁵⁴;
- поощрение этических норм деловой практики⁵⁵, в рамках которых предприятия, действующие в онлайн-режиме, придерживаются достойного поведения и стремятся к достижению социальных целей, поскольку осознают, что это в наибольшей степени отвечает интересам их акционеров, сотрудников и клиентов, а также уменьшает жесткость надзора со стороны регуляторных органов;
- предоставление регуляторному органу полномочий на стимулирование и контроль ответственного поведения платформ и компаний, работающих в социальных сетях. В настоящее время этот процесс только начинается в некоторых странах с развитой экономикой, однако, поскольку соответствующие компании часто являются глобальными, улучшения, достигнутые в одной части света, будет легче внедрять где-либо еще с учетом местных условий.

Меры такого рода, особенно упомянутые последними, – это новшество, но, несомненно, в ближайшие годы их число увеличится⁵⁶.

Цифровая идентичность и автоматизированное принятие решений

У каждого человека вполне правомерно может быть несколько вариантов его самоидентификации, связанных с различными аспектами его жизни (ITU 2018b). Например, женщина по имени Мерон Кабеде может быть "мамой" для своих детей, "Мерон" для друзей и "Г-жой Кабеде" для своего босса – и с этими именами связаны различные варианты самоидентификации, воспринимаемые самим человеком и окружающими. То же самое происходит и в цифровой сфере, где с легкостью можно иметь столько вариантов идентификации личности, сколько заблагорассудится, а незнакомцу будет сложнее связать различные варианты идентификации с одним и тем же человеком.

Первым вариантом цифровой идентификации личности для многих людей, особенно в развивающихся странах, стал номер мобильного телефона. Прежде при использовании предоплатной модели номер телефона не позволял идентифицировать человека, однако меры по борьбе с преступностью все чаще

⁵³ См. сводную информацию об опыте угандийских женщин по адресу: https://cipesa.org/?wpfb_dl=329, а также исследовательский проект Соединенного Королевства "Гендерные вопросы и интернет вещей" по адресу: <https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot>.

⁵⁴ "Коалиция за свободу в интернете" (The Freedom Online Coalition), <https://freedomonlinecoalition.com/>, представляет собой партнерство правительств 31 страны, работающее над расширением свободы в интернете.

⁵⁵ См., например, информацию о развитии событий и предложениях в Соединенном Королевстве в публикации Hodges and Steinholtz (2018), а о международном движении за этическую бизнес-практику – на веб-сайте <https://bcorporation.net/>.

⁵⁶ См. главу 2 "Конкуренция и экономика", в которой, в частности, рассматривается вопрос о регулировании деятельности цифровых платформ.

приводили к требованиям введения регистрации для предоплатных тарифных планов в соответствии с принципом "знай своего клиента", который часто используется в банковском секторе, вследствие чего номер телефона связан как минимум с именем, а также, вероятно, с датой рождения, а часто и адресом; три этих параметра в совокупности однозначно идентифицируют зарегистрированное лицо. Номера мобильных телефонов также используются для идентификации личности во многих приложениях.

К другим вариантам цифровой идентификации личности относятся адреса электронной почты, учетные записи в социальных сетях и, все чаще, официальные документы, такие как водительские удостоверения, карты медицинского страхования и паспорта⁵⁷. Официальные документы, естественно, содержат и другие персональные данные (например, для водительского удостоверения таковыми являются сертификат о сдаче экзамена на получение водительского удостоверения и данные о нарушениях правил дорожного движения), а наличие их в цифровом формате позволяет легко связывать воедино различные данные о человеке. В перспективе государственные должностные лица могут получить доступ ко всем этим данным в рамках централизованной системы цифровой идентификации, такой как индийская Aadhaar⁵⁸. На сегодняшний день предоставление данных для системы Aadhaar остается добровольным, но, поскольку она используется для важных официальных целей (например, при обращении за пособиями), возможность отказа от ее использования, вероятно, станет чисто теоретической.

Подобные всеобъемлющие системы цифровой идентификации могут предоставлять значительные преимущества с точки зрения эффективности, но одновременно вызывают опасения, связанные с чрезмерной властью государства, что может приводить, например, к ограничению возможности передвижения или доступа к медицинскому обслуживанию для лиц, чьи взгляды не приветствуются правительством. Ведется разработка систем цифровой идентификации, контроль за которыми осуществляет непосредственно физическое лицо и которые раскрывают только информацию, необходимую для решения рассматриваемого вопроса. Например, для покупки алкогольных напитков человеку, возможно, понадобится указать свой возраст, для получения займа – продемонстрировать платежеспособность, а для получения работы – указать статус пребывания в стране⁵⁹.

Вопрос автоматизированного принятия решений также вызывает в настоящее время значительный общественный интерес и беспокойство. Системы, осуществляющие рассмотрение заявок (например, о приеме на работу, предоставлении места в колледже или получении займа), используют методы ИИ, чтобы сделать вывод о вероятностной успешности заявителей на основе сравнения их цифровых идентичностей с идентичностями предыдущих успешных заявителей⁶⁰. Алгоритмы, подготовленные на основе данных за предшествующие периоды, с высокой долей вероятности будут воспроизводить предшествующие успешные модели, продолжая заложенную в них дискриминацию, если не будут приняты конкретные усилия по предотвращению этого. В потребительской сфере можно признать полезность персонализированных рекомендаций, однако приходится сожалеть об утрате возможности сделать осознанный свободный выбор⁶¹.

4.4 Основные выводы

Введение в права потребителей цифровых услуг

- Удовлетворение интересов потребителей и других пользователей является основной целью рынков, и конкурентные рынки обычно являются наилучшим способом повышения качества услуг для потребителей. Однако сами по себе рыночные силы не всегда обеспечивают наилучшие возможные результаты для всех потребителей, и регуляторные органы играют чрезвычайно важную роль в выявлении подобных случаев и принятии соответствующих мер.

⁵⁷ Для получения более подробной информации о преобразующем потенциале цифровых идентификационных систем см. Инициативу Всемирного банка ID4D по адресу: <https://id4d.worldbank.org>.

⁵⁸ <https://uidai.gov.in/my-aadhaar/get-aadhaar.html>

⁵⁹ Проект "Идентичности" (Identities Project), <https://www.identitiesproject.com/>, основанный на опыте ряда жителей Индии, увязан с документом World Bank (2019b). См. также Consumers International (2017). История беженцев, представленная на веб-сайте <https://readymag.com/u82923304/refugee-id-journey/8/>, информативна и легко читается.

⁶⁰ Подробнее рассматривается в главе 7 "Реагирование регуляторных органов на развитие технологий".

⁶¹ См. Consumers International (2019).

- Исследования, проведенные в развивающихся странах, свидетельствуют о конвергенции между ожидаемыми правами потребителя и ожидаемыми правами гражданина, благодаря чему формируются новые идеи о цифровых правах всех людей.
- К группам потребителей, которые с наименьшей вероятностью будут охвачены качественными услугами только за счет рыночных сил, относятся группы с высокой себестоимостью обслуживания (которая зачастую обусловлена проживанием в отдаленных районах или потребностью в специализированном оборудовании в связи с тем или иным видом инвалидности), а также группы лиц, чьи средства не позволяют оплачивать желаемые объемы услуг. Они, а также иные лица, являющиеся или становящиеся уязвимыми, требуют особого внимания со стороны регуляторных органов.

Система поддержки потребителей

- Ответственность регуляторных органов за решение проблем потребителей цифровых услуг может быть разделена между различными ведомствами, такими как специальный регуляторный орган по защите прав потребителей, антимонопольная служба, регуляторный орган по защите данных, а также регуляторный орган в области ИКТ. В зависимости от этапа и темпов цифровой трансформации директивным органам следует определить, какая регуляторная структура в сфере защиты прав потребителей является наиболее подходящей с учетом ситуации в их стране.
- Регуляторным органам в области ИКТ необходимо поддерживать тесные контакты со всеми остальными ведомствами, занимающимися вопросами защиты прав потребителей цифровых услуг, и совместно определять способы коллективной работы, чтобы обеспечить надлежащий учет всех аспектов.
- Основы защиты прав потребителей цифровых услуг часто закреплены в общем законе о защите прав потребителей. Законодательным органам необходимо время от времени пересматривать этот закон, а регуляторным органам ИКТ следует обеспечить его дополнение соответствующими внутриотраслевыми мерами защиты, например нормативными требованиями, которые должны соблюдать поставщики услуг.
- Регуляторные органы ИКТ должны играть важную роль в обеспечении соблюдения таких нормативных требований; на них также могут возлагаться аналогичные обязанности в отношении нарушений общего законодательства о защите прав потребителей со стороны поставщиков услуг связи и любых других структур, подлежащих регулированию.
- Важной частью обязанностей большинства регуляторных органов ИКТ является обеспечение справедливого, быстрого и эффективного рассмотрения жалоб потребителей. Как правило, сначала потребители должны направить жалобу своему поставщику услуг, который обязан предоставить ответ в соответствии с подробными правилами. Потребители, оставшиеся неудовлетворенными, могут затем подать жалобу либо в сам регуляторный орган, либо в независимую службу альтернативного разрешения споров.
- Вне зависимости от того, несут ли регуляторные органы основную ответственность за рассмотрение жалоб потребителей, которые не были урегулированы на уровне компаний, эти жалобы являются для регуляторных органов ценным источником информации о том, что беспокоит потребителей.
- Именно сами потребители и их представители способны наилучшим образом сформулировать изменяющиеся запросы потребителей. Поставщики услуг признают это и проводят изучение своих рынков, однако регуляторные органы также несут ответственность за содействие в формулировании запросов потребителей (особенно запросов потребителей из числа уязвимых групп населения, удовлетворить которые рынки, возможно, не могут).
- Регуляторные органы ИКТ могут оказывать содействие потребителям цифровых услуг в формулировании их запросов, используя различные методы, в том числе:
 - оказание поддержки в создании и функционировании организаций потребителей, укомплектованных высококвалифицированными сотрудниками, опыт работы которых включает вопросы, связанные с защитой потребителей цифровых услуг. Организации могут представлять как потребителей в целом, так и определенные их группы, например лиц с ограниченными возможностями;

- инициирование и поддержание диалога с представителями потребителей в рамках как устойчивых структур (таких, как группы и форумы потребителей), так и ситуативных неформальных обсуждений конкретных вопросов;
- стимулирование прямого взаимодействия поставщиков услуг с представителями потребителей;
- самостоятельное изучение потребительского спроса.

Конкретные проблемы, касающиеся потребителей

- В условиях быстрого изменения рынков рекомендуется проводить периодический обзор мер защиты, которые предлагаются клиентам поставщиков услуг связи как с предоплатной, так и с постоплатной системой расчетов, и которые касаются, в частности, корректности и прозрачности произведенных платежей, процедур компенсации в случае возникновения ошибок и предоставления потребителям возможности смены оператора. В процессе обзора может быть выявлена потребность в совершенствовании обеспечения соблюдения существующих правил либо во внесении в них изменений или разработке новых нормативных требований.
- Ориентированное на потребителя сравнение цен регуляторными органами – это важное средство содействия потребителям в выборе поставщика услуг, но по мере расширения рынка становится все сложнее поддерживать масштабность, точность и актуальность этой информации. Вместо самостоятельного решения этой проблемы некоторые регуляторные органы предпочитают заказывать или доверять проведение сравнения внешним поставщикам.
- Регуляторные органы ИКТ и другие органы, отвечающие за поддержку потребителей, могут сообщать потребителям в получении консультаций или поддержки, необходимых им в этой постоянно усложняющейся сфере, возможно, посредством онлайн-овой "системы одного окна" или телефонных горячих линий.
- Чтобы потребители с ограниченными возможностями могли получить равный доступ к цифровым технологиям, может потребоваться адаптация оборудования или услуг, а возможность использования цифрового доступа для этих людей может стать источником более масштабных социально-экономических выгод. Регуляторные органы могут повлиять на изменение положения людей с ограниченными возможностями в лучшую сторону посредством как принятия нормативных мер, так и поощрения добровольных инициатив.
- Регуляторные органы ИКТ могут способствовать укреплению доверия со стороны потребителей, требуя использования передовых методов ведения бизнеса, демонстрирующих надежность, или поощряя их. Они также могут помочь в информировании потребителей, с тем чтобы они научились избегать такой неприемлемой практики, как продажа их данных, приводящая к нежелательной целевой рекламе.
- Регуляторные органы ИКТ должны быть осведомлены о вызывающих беспокойство потребителей вопросах, касающихся сетевой безопасности и использования их персональных данных, часть из которых рассматриваются в этой главе. Если, как это часто бывает, непосредственная ответственность за защиту данных и соблюдение норм регулирования в области конфиденциальности возлагается на другой регуляторный орган, регуляторным органам ИКТ следует работать в тесном контакте с этим иным регуляторным органом, с тем чтобы обеспечить полный охват всех проблем потребителей.

Справочные материалы

- A4AI (Alliance for Affordable Internet). 2016. *Policy Guidelines for Affordable Mobile Data Services*. Research Brief No. 3. https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2016/11/MeasuringImpactsOfMobileDataServices_ResearchBrief3.pdf
- ARCEP (L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). 2018. *Devices, the Weak Link in Achieving an Open Internet*. Paris: ARCEP. https://en.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf
- Behavioural Insights Team. 2019. *Contractual Terms and Privacy Policies: How to Improve Consumer Understanding*. London: Department for Business, Energy and Industrial Strategy. <https://www.gov.uk/government/publications/contractual-terms-and-privacy-policies-how-to-improve-consumer-understanding>
- BEREC (Body of European Regulators for Electronic Communications). 2020. *BEREC Strategy 2021-2025*. BoR (20) 43. https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/9039-draft-berec-strategy-2021-2025
- Consumers International. 2017a. *Connecting Voices: A Role for Consumer Rights in Developing Digital Society*. London: Consumers International. https://www.consumersinternational.org/media/154869/ci_connecting-voices_2017_v2.pdf
- Consumers International. 2017b. *Digital ID in Peer to Peer Markets*. London: Consumers International. <https://www.consumersinternational.org/media/154884/digital-id-report.pdf>
- Consumers International. 2019. *Artificial Intelligence: consumer experiences in new technology*. London: Consumers International. <https://www.consumersinternational.org/media/261949/ai-consumerexperiencesinnewtech.pdf>
- Cowell, Frank, and Karen Gardiner. 1999. *Welfare Weights*. London: London School of Economics. [http://darp.lse.ac.uk/papersDB/Cowell-Gardiner_\(OFT\).pdf](http://darp.lse.ac.uk/papersDB/Cowell-Gardiner_(OFT).pdf)
- Dutta-Powell, Ravi, Zoe Powell, and Nathan Chappell. 2019. *Behavioural Biases in Telecommunications: A Review for the Commerce Commission*. Wellington, New Zealand: Behavioural Insights Team. https://comcom.govt.nz/_data/assets/pdf_file/0026/146681/BIT-Behavioural-biases-in-telecommunications-13-May-2019.PDF
- Evans, Phil. 2003. *The Consumer Guide to Competition: A Practical Handbook*. London: Consumers International. <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/34850/126821.pdf>
- Hodges, Christopher and Ruth Steinholtz. 2018. *Ethical Business Practice and Regulation*. London: Bloomsbury. <https://www.bloomsbury.com/au/ethical-business-practice-and-regulation-9781509916375/>
- Hogg, Tim. 2020. "Framing Fairness". *InterMEDIA* 48 (1): 29-31. https://www.iicom.org/wp-content/uploads/IM-April-2020-Vol-48-Issue-1_Hogg.pdf
- МСЭ. 2014. *Руководящие указания на основе примеров передового опыта по защите прав потребителей в цифровом мире*. Женева: МСЭ. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/BestPractices/GSR14_BPG_ru.pdf
- ITU. 2016. *Digital Financial Services: Regulating for Financial Inclusion: An ICT Perspective*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT02-2016-PDF-E.pdf
- ITU. 2017a. *The App Economy in Africa: Economic Benefits and Regulatory Directions*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.APP_ECO_AFRICA-2017-PDF-E.pdf
- МСЭ. 2017b. *Заключительный отчет 1-й Исследовательской комиссии МСЭ-D по Вопросу 6/1: Информация для потребителей, их защита и права: законы, нормативные положения, экономические основы, сети потребителей*. Женева: МСЭ. <https://www.itu.int/pub/publications.aspx?lang=en&parent=D-STG-SG01.06.3-2017>
- ITU. 2018a. *Global ICT Regulatory Outlook: Regulatory Collaboration: "Power Coupling"*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2018-PDF-E.pdf

- ITU. 2018b. *Digital Identity in the ICT Ecosystem: An Overview*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.ID01-2018-PDF-E.pdf
- ITU. 2018c. *Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf
- Lunn, Peter. 2014. *Regulatory Policy and Behavioural Economics*. Paris: OECD. https://www.oecd-ilibrary.org/governance/regulatory-policy-and-behavioural-economics_9789264207851-en
- Lunn, Peter, and Sean Lyons. 2018. "Consumer Switching Intentions for Telecoms Services: Evidence from Ireland". *Heliyon* 4(5). <https://doi.org/10.1016/j.heliyon.2018.e00618>
- Milne, Claire. 2016. "Nuisance Calls and Texts: What Can Be Done?". Presentation for MIIT/ITU meeting in Chongqing, China. <http://public.antelopeweb.fmail.co.uk/publications/what%20can%20be%20done%20about%20nuisance%20calls%20and%20texts.pdf>
- OECD. 2019a. *The Effects of Zero Rating*. Paris: OECD. <https://www.oecd-ilibrary.org/docserver/6eefc666-en.pdf>
- OECD. 2019b. *Understanding Online Consumer Ratings and Reviews*. Paris: OECD. <https://www.oecd-ilibrary.org/docserver/eb018587-en.pdf>
- Ofcom. 2019. *Access and Inclusion in 2018: Consumers' Experiences in Communications Markets*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0018/132912/Access-and-Inclusion-report-2018.pdf
- Ofcom. 2020. *Making Communications Markets Work Well for Customers: A Framework for Assessing Fairness in Broadband, Mobile, Home Phone and Pay TV*. Policy Statement, January 23. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0033/189960/statement-fairness-framework.pdf
- Russell, Graham, and Christopher Hodges. 2020. *Regulatory Delivery*. London: Bloomsbury. <https://www.bloomsburyprofessional.com/uk/regulatory-delivery-9781509918584/>
- TRAI. 2018. *Consumer Handbook on Telecommunications*. New Delhi. https://traai.gov.in/sites/default/files/TRAI_Handbook_2018_Eng.pdf
- UKRN (U.K. Regulators Network). 2020. *Driving Fair Outcomes for Vulnerable Consumers across UK Markets*. Event Report. London: UKRN. <https://www.ukrn.org.uk/wp-content/uploads/2020/03/Driving-Fair-Outcomes-for-Vulnerable-Consumers-Report.pdf>
- ЮНКТАД (Конференция Организации Объединенных Наций по торговле и развитию). 2016. *Руководящие принципы Организации Объединенных Наций для защиты интересов потребителей*. Женева: ЮНКТАД. https://unctad.org/system/files/official-document/ditccplpmisc2016d1_ru.pdf
- Which? 2018. *Control, Alt or Delete: Consumer Research on Attitudes to Data Collection and Use*. London: Consumers' Association. <https://www.which.co.uk/policy/digitisation/2707/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use>
- World Bank. 2019a. *Information and Communications for Development 2018: Data-Driven Development*. Washington, DC: World Bank. <https://elibrary.worldbank.org/doi/book/10.1596/978-1-4648-1325-2?chapterTab=true>
- World Bank. 2019b. *Principles on Identification for Sustainable Development: Toward the Digital Age*. Washington, DC: World Bank. <http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>

Глава 5. Защита данных и доверие



5.1 Введение

Данные иногда называют "нефть цифровой экономики"¹, а их использование в цифровой экономике – "капитализм слежки"². Если первый термин имеет относительно положительный оттенок, то последний вызывает прямые опасения по поводу использования персональных данных³. В настоящей главе основное внимание уделяется аспектам регулирования данных с акцентом на персональные данные.

Процесс цифровой трансформации неизбежно привлёк внимание к вопросам адекватности нормативно-правовой базы, регулирующей информационные продукты, услуги и платформы, и необходимости в ней. Законы об интеллектуальной собственности, особенно об авторском праве, пришлось пересмотреть с учетом растущего значения нематериальных активов. Для борьбы с киберпреступностью, предотвращения новых форм злонамеренного поведения и создания условий для проведения эффективных расследований потребовалось внести поправки в законы и процедуры уголовного права. Аналогично, поскольку персональные данные становятся все более ценным стратегическим коммерческим активом, возникает потребность в правилах, обеспечивающих защиту таких данных и предоставляющих людям возможность контроля за сбором, обработкой, и использованием своих данных, в том числе за их неправомерным использованием. Широко признано, что наличие режима защиты данных является одним из ключевых факторов содействия цифровой трансформации (African Union 2020). Контроль считается критически важным с точки зрения формирования доверия к работе в онлайн-среде у субъектов данных, будь то граждане, потребители или друзья, что само по себе стимулирует распространение, участие и потребление (ITU 2018).

В настоящей главе исследуется природа режимов защиты данных с уделением особого внимания их регуляторным аспектам – особенность, которая приводит к интересным аналогиям с сектором электросвязи. В ней изучается степень, в которой должны и могут затрагиваться появляющиеся технологии и услуги, а также меры контроля над трансграничным потоком персональных данных и вытекающие из этого последствия для торговли. Вопросы защиты данных и неприкосновенности частной жизни особенно пересекаются при рассмотрении необходимости введения специальных правил, регулирующих нашу

¹ Сравнение данных (неисчерпаемый предмет, не вызывающий соперничества) с нефтью (конечный ресурс, за который может вестись соперничество), вероятно, ошибочно.

² Термин "капитализм слежки" (surveillance capitalism) был введен Шошаной Зубофф (Zuboff 2019).

³ Настоящая глава посвящена защите данных, а не неприкосновенности частной жизни. Хотя эти понятия связаны между собой, они не являются синонимами. См., например, World Bank 2021 (готовится к печати). Иногда они используются как взаимозаменяемые, а иногда – как общее понятие ("защита конфиденциальности данных и неприкосновенности частной жизни" или "конфиденциальность данных"); здесь проводится различие, чтобы четко поместить понятие защиты данных в регуляторный контекст.

коммуникативную деятельность. Также исследуется сложное соотношение между защитой данных и информационной безопасностью. Наконец, предлагаются некоторые важные концепции для регуляторных органов.

5.2 Режимы защиты данных

Хотя защита данных четко связана и частично пересекается с правом на неприкосновенность частной жизни, ей также присущи некоторые характерные особенности, отделяющие ее от традиционных понятий закона о неприкосновенности частной жизни. Во-первых, защита данных прочно укоренилась в сфере цифровой экономики, то есть обработки данных с помощью информационно-коммуникационных технологий (ИКТ) во многих ее формах, так что она актуальна для настоящего Справочника. Между тем законы о неприкосновенности частной жизни распространяются и на те ее стороны, которые могут быть далеки от информационных технологий. Во-вторых, режимы защиты данных, как правило, применимы ко всем данным, относящимся к определенному лицу и именуемым "персональные данные", независимо от того, можно ли эти данные охарактеризовать как конфиденциальные или открытые. Следовательно, то, что человек публикует на своей странице в Facebook, также заслуживает защиты в рамках этого режима, как и то, что хранится в защищенном паролем файле, хотя и не в такой же степени. В-третьих, персональные данные, как правило, могут обрабатываться только на неких законных основаниях, таких как согласие, когда бремя ответственности возлагается на лицо, владеющее персональными данными, в оправдание контроля над ними; традиционный же закон о неприкосновенности частной жизни направлен на контроль за случаями вмешательства в личную жизнь человека, приводящего к причинению материального или морального ущерба. В-четвертых, соблюдение мер защиты данных, как правило, должно контролироваться надзорным органом. Именно эта особенность делает защиту данных регуляторным режимом – режимом, далеко выходящим за рамки нашего традиционного представления о праве на неприкосновенность частной жизни.

Защита данных как нормативная концепция впервые появилась в Конвенции Совета Европы о защите данных 1981 года (более известной как Конвенция 108⁴). Основанная на праве на неприкосновенность частной жизни, закрепленном в статье 8 Европейской конвенции о правах человека (ЕКПЧ), она была связана исключительно с "автоматической обработкой персональных данных". В 1995 году с принятием Директивы о защите данных⁵ акцент сместился на Европейский союз (ЕС). Эта директива быстро стала основным инструментом, на который равнялось большинство других законов и инициатив. В мае 2018 года Директиву заменил Общий регламент по защите данных (GDPR), который в целом признан основным законом в этой области.

Хотя идея защиты данных родилась в Европе, режимы защиты данных с тех пор получили широкое распространение во всем мире, так что почти в 140 странах действует тот или иной правовой режим (Greenleaf 2020), а также множество других региональных инструментов, включая Рамочное соглашение по защите конфиденциальности персональных данных Азиатско-Тихоокеанского экономического сотрудничества⁶ и Конвенцию Африканского союза о кибербезопасности и защите персональных данных⁷ (2014 год). Однако, как отмечает Международный союз электросвязи (МСЭ), несмотря на такое обилие инструментов и законов, наблюдается "тенденция к принятию законов по "европейскому" образцу"⁸. Вероятно, последней страной, представившей законопроект о защите данных, стал Китай⁹.

⁴ Совет Европы – это межправительственный орган из представителей 47 государств-членов, ответственный за *Европейскую конвенцию о правах человека* (ЕКПЧ) и *Конвенцию о защите частных лиц в отношении автоматизированной обработки данных личного характера*, Страсбург, 28 января 1981 года (Конвенция 108). В Конвенцию 108 недавно были внесены изменения для приведения ее в соответствие с GDPR, и ее текст доступен по адресу: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

⁵ Директива 95/46/ЕС "О защите физических лиц в связи с обработкой персональных данных и о свободном движении таких данных", ОJ L 281/31, 23.11.1995.

⁶ Впервые принято в 2005 году, пересмотрено в 2015 году.

⁷ https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

⁸ Сноска 1 на с. 35.

⁹ Китай опубликовал для ознакомления проект закона о защите персональных данных, который во многих отношениях отражает положения GDPR. См., например <https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/>.

Хотя эти разнообразные правовые инструменты значительно различаются по объему и в деталях, большинство режимов защиты данных основано на общем наборе "принципов защиты данных", которые объекты регулирования должны соблюдать при обработке персональных данных. В целом эти принципы можно подразделить на две категории:

- принципы, ориентированные на качество персональной информации и информационных систем, такие как необходимость обеспечения точных данных и безопасных систем;
- принципы, применяемые к владельцам обрабатываемых данных, такие как принципы справедливости и прозрачности (Bygrave 2002).

Как и в сфере электросвязи, регуляторный характер защиты данных проистекает как из характера обязательств, возлагаемых на объекты регулирования, так и из роли надзорного органа в осуществлении полномочий по надзору и правоприменению в отношении не соблюдающих требований объектов регулирования. Каждый национальный орган (и некоторые органы регионального уровня) издает различные виды мнений, руководств и рекомендаций, которые составляют часть нормативной базы для объектов регулирования, хотя, как правило, не являются обязательными. Кроме того, существуют многочисленные отраслевые инициативы по саморегулированию, такие как кодексы поведения, часто отраслевого уровня, которые развивают и дополняют эти правовые нормы.

Наконец, вопросы защиты данных включены в стандарты, такие как стандарты Международной организации по стандартизации (ИСО¹⁰), которые также можно сделать частью регуляторного режима путем прямого включения или путем превращения в практическую рекомендацию *де-факто*. С кодексами поведения и стандартами защиты данных связано появление режимов сертификации, которые позволяют организациям проводить внешнюю проверку, подтверждающую, что применяемые ими методы и процедуры соответствуют необходимым стандартам, а также объявлять о таком соответствии путем использования штампов, знаков или этикеток¹¹.

Весь этот спектр мер – от "жесткого" до "мягкого" законодательства – составляет регуляторный режим защиты данных. Что касается объектов регулирования, то здесь основную роль играет "контролер", действующий в одиночку или совместно с другими, как лицо, определяющее цель и средства обработки данных. В большинстве законов присутствует вторая категория объектов регулирования – "обработчик", который обрабатывает персональные данные от имени контролера. Прямые обязательства, основанные на законе, которые возлагаются на обработчика, такие как соблюдение принципов, обычно менее обременительны, чем обязательства, возлагаемые на контролера, хотя часто присутствует требование заключения контракта, регулирующего отношения между контролером и обработчиком, который может перераспределять обязанности соответствующих сторон. Определение роли лица как контролера и/или обработчика, а, следовательно, и их соответствующих нормативных обязательств может само по себе составлять сложный и спорный вопрос. Это особенно актуально с учетом все возрастающей сложности цифровых цепочек поставок и рынков, таких как интернет вещей (IoT), объединяющих в себе продукты, услуги и программное обеспечение.

5.3 Регуляторные органы

Как уже отмечалось, одним из отличительных признаков защиты данных как регуляторного режима, а не просто нормативно-правовой базы, является учреждение органа или назначение уполномоченного по надзору за его соблюдением и преследованием нарушителей. Действительно, в соответствии с Хартией Европейского союза об основных правах необходимость такого органа закреплена в самом праве: "Соблюдение этих правил подлежит контролю со стороны независимого органа" (статья 8(3)). Хотя в некоторых международных документах вначале не признавалась необходимость подобного органа, при их последующих пересмотрах такое требование было включено¹².

Таким образом в режимах защиты данных следует различать материальный и процедурный компоненты. Первый включает в себя обязательства, возложенные на объекты регулирования, и права, предоставленные отдельным субъектам данных, а последний касается характера и полномочий регуляторного органа. При сравнении национальных режимов следует учитывать, что оба компонента одинаково важны и,

¹⁰ ISO, 27018: 2014 "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

¹¹ Например, Truste Privacy Program Standards, см. <https://trustarc.com/consumer-info/privacy-certification-standards/>.

¹² Например, Дополнительный протокол к Конвенции Совета Европы (2001 год), ОЭСР (2013 год) и АТЭС (2015 год).

несомненно, могут иметь регуляторные последствия. Например, согласно законодательству ЕС, когда Европейская комиссия оценивает, обеспечивает ли третья страна "адекватный уровень защиты" при передаче персональных данных, важной частью анализа является соответствие процедурных элементов¹³.

Между национальными регуляторными органами в области электросвязи и защиты данных имеются явные параллели в отношении их характера и полномочий. Орган должен быть независим от объектов регулирования, в число которых обычно входят государственные и общественные организации. Хотя действующий оператор может полностью или частично принадлежать государству, а может и не принадлежать ему, основным сборщиком и обработчиком персональных данных, безусловно, будет государство. Однако во многих странах применение законов о защите данных либо ограничено частным сектором, либо, если в них включены государственные органы, для государственного сектора сделаны исключения, не распространяющиеся на контролеров из частного сектора. Достижение реальной независимости регуляторных органов может быть проблематичным, поскольку для этого необходимы адекватные финансовые ресурсы, возможности и опыт. Что касается полномочий, то органам по защите данных, как правило, предоставляются как *априорные* полномочия по вмешательству, такие как разрешение определенных действий, так и полномочия по ведению расследования *постфактум*, например право требования раскрытия информации. Поскольку это государственный орган, надлежащее осуществление им полномочий входит в сферу административного права, при этом возникает беспокойство по поводу того, должным ли образом осуществляется принятие решений и другие виды деятельности.

Определение роли и значения органа по защите данных может вызывать проблемы в отдельных странах, особенно там, где еще мало устоялось понятие независимого регулирования и отсутствует соответствующий опыт. Однако регуляторные органы по защите данных могут посчитать отсутствие эффективного и независимого регуляторного органа в другой стране поводом для запрета или ограничения передачи персональных данных в эту страну в целях защиты субъектов данных. Для решения этой проблемы вместо создания совершенно нового органа с сопутствующей необходимостью обеспечения его ресурсами и формирования культуры независимости можно рассмотреть возможность расширения сферы полномочий существующего национального регуляторного органа, такого как регуляторный орган по электросвязи или ИКТ или орган по защите прав потребителей, с тем чтобы он охватывал вопросы защиты данных.

¹³ Article 29 Working Party, *Adequacy Referential (updated)*, WP 254, November 2017.

Вставка 5.1. Глобальная ассамблея по вопросам конфиденциальности



Глобальная ассамблея по вопросам конфиденциальности (GPA) – это международная организация, объединяющая более 130 регуляторных органов по защите данных и обеспечению конфиденциальности, а также наблюдателей из различных международных организаций и НПО. Впервые она была созвана в 1979 году как международная конференция. GPA принимает специальные резолюции и коммюнике, включая недавний призыв к расширению сотрудничества между органами по защите данных, защите прав потребителей и конкуренции. В GPA также действует несколько рабочих групп, в том числе одна по международному сотрудничеству в области правоприменения, в обязанности которой входит рассмотрение правовых решений. В качестве форума для взаимодействия, сотрудничества и обмена опытом и ноу-хау GPA может оказывать поддержку национальным органам по защите данных в наименее развитых странах.

Источник: <https://globalprivacyassembly.org>

5.4 Технологии и услуги

Как отмечалось выше, одно из различий между защитой данных и защитой неприкосновенности частной жизни заключается в том, что в первом случае рассматриваются исключительно персональные данные, обрабатываемые ИТ-системами. По этой причине нельзя сказать, что закон о защите данных является технологически нейтральным, поскольку именно компьютеризация дала повод для беспокойства о персональных данных в 1960-х и 1970-х годах, и современная нормативная база в первую очередь ориентирована на обработку таких данных. Обработке, как правило, дается широкое законодательное определение, охватывающее весь процесс от сбора данных до их окончательного удаления или, в качестве альтернативы, их обезличивания, не позволяющего идентифицировать отдельные субъекты данных. Такой широкий диапазон распространяет применение режимов защиты данных на физическую сферу, например управление ручным сбором данных, предназначенных для последующей обработки.

Однако в то же время принципы защиты данных, составляющие основу национальных и международных режимов защиты данных, рассчитаны на то, чтобы не быть слишком строго регламентирующими в отношении определенных типов технологий и услуг, которые развиваются быстрыми темпами. Регулирование, основанное на принципах, призвано помочь избежать технологической избыточности правил и регуляторных положений и, что еще хуже, торможения инноваций.

Несмотря на "технологическую нейтральность", соблюдение принципов защиты данных может прямо влиять на разработку контролерами конкретных технологий и услуг, а также косвенно на тех, кто производит компоненты и приложения, входящие в состав внедряемых технологий и услуг, располагаясь выше в цепочке поставок. В частности, в конструкции приложений и систем должен быть отражен принцип минимизации данных.

Вставка 5.2. Исследование конкретной ситуации: приложения для отслеживания COVID-19

С начала пандемии COVID-19 одной из главных задач было отслеживание людей, у которых развиваются симптомы заболевания, и всех тех, с кем они находились в тесном контакте во время инкубационного периода вируса, чтобы предотвратить заражение ими других людей. Для этого были разработаны различные приложения, отслеживающие контакты, которые могут использоваться на мобильных телефонах. Такие приложения могут различаться по сбору данных на децентрализованной или централизованной основе, а также по типу собираемых данных, например данные о местоположении или об удаленности. Такие проектные решения приводят к компромиссу между правами пользователей в отношении своих данных и соображениями общественного здравоохранения.

- Система, разработанная Apple и Google, основана на децентрализованном протоколе DP-3T Bluetooth, что означает, что вся обработка и хранение данных происходят на устройстве пользователя. Сохраненные данные хранятся в устройстве только 14 дней, и система не позволяет собирать данные о местоположении.
- Правительства некоторых стран разработали системы с использованием централизованной модели, позволяющей медицинским работникам получать доступ к большому количеству данных, которые помогают им лучше отслеживать перемещения людей, а также предоставлять данные для текущих исследований вируса и последствий эпидемии в системе здравоохранения.

Международное и национальное законодательство признает, что в чрезвычайных обстоятельствах некоторые основные права, включая право на защиту данных, могут быть ограничены при условии соблюдения основных демократических принципов и гарантий, а также при условии, что ограничение является законным, временным и не произвольным¹.

¹ См.: World Bank 2021 (готовится к печати), Spotlight 6.1.

Хотя принципы защиты данных применимы ко всем технологиям и услугам, это не мешает юрисдикциям определять, что конкретные технические или коммерческие разработки заслуживают принятия дополнительных правил для решения явных общественных проблем и удовлетворения интересов общества¹⁴. Двумя важными примерами служат появление искусственного интеллекта (ИИ) и социальных сетей.

ИИ позволяет компьютерам выявлять закономерности в наборах больших данных и создавать репрезентативные модели, которые можно использовать для автоматизированного принятия решений – от рекомендаций по покупкам для потребителей и диагностики заболеваний до вынесения приговоров преступникам. Очевидно, что такое автоматизированное принятие решений может иметь не всегда желаемые или заслуженные реальные последствия для отдельных людей. В законах о защите данных учтены два аспекта такого автоматизированного принятия решений: справедливая и прозрачная обработка и возможность потребовать пересмотра решения. В первом случае субъект данных должен быть проинформирован о трех вещах: а) о применении автоматизированного процесса принятия решений; б) о том, как было принято решение, то есть получить значимую информацию о логике, заложенной в алгоритм, определяющий результат; и с) о возможных проистекающих из обработки последствиях для субъекта данных. Такая прозрачность направлена на то, чтобы предоставить субъекту данных возможность эффективно контролировать процесс использования своих данных. Что касается проверки, то субъектам данных может быть дано право вмешиваться в процесс принятия решений при определенных обстоятельствах, которое часто характеризуют как "человек в контуре управления" (Wang 2019). Это отражает широко распространенное мнение о том, что должна быть предусмотрена возможность обжаловать решение, принятое машиной в отношении человека, хотя вопрос о том, способствует ли это принятию лучших решений, остается спорным.

¹⁴ Например, Мексика, статья 52 "Обработка персональных данных при облачных вычислениях" Положений к Федеральному закону о защите персональных данных, хранящихся у частных лиц (2011 год).

Компании – операторы социальных сетей, такие как Facebook и Weibo, служат ярким примером явления, получившего название "капитализм слежки". Субъекты данных получают бесплатные услуги в обмен на предоставление поставщикам возможности использовать их персональные данные, продавая их рекламодателям, – так называемый двусторонний рынок. Одна из проблем социальных сетей заключается в том, что потребители могут оказаться "привязанными" к поставщику, услугами которого они пользуются, из-за трудностей с перемещением опубликованного ими контента в альтернативную сеть. Для решения этой проблемы в рамках некоторых режимов защиты людям предоставляется право на переносимость данных, которое может включать право требовать передачи их данных непосредственно от действующего поставщика услуг выбранному альтернативному поставщику¹⁵. Это можно рассматривать как аналог обязательств по обеспечению переносимости телефонных номеров в секторе электросвязи, что позволяет абонентам быстро, дешево и легко менять поставщиков услуг без необходимости изменять свои номера¹⁶. Благодаря снижению затрат на переход, связанных со сменой поставщика услуг, попадание в зависимость становится менее вероятным. Хотя это достигается законом о защите данных, такое расширение прав и возможностей пользователей можно рассматривать и как меру по обеспечению конкуренции со стороны спроса, а также как компонент режимов защиты потребителей¹⁷.

Другие инновационные и прорывные технологии могут вызывать проблемы с защитой данных, которые, хотя и не решаются введением конкретных регуляторных мер, могут потребовать от регуляторных органов уделяния особого внимания использованию этих мер в соответствии с требованиями защиты данных. Например, технология блокчейн при ее развертывании с использованием распределенной архитектуры вызывает опасения по поводу роли соответствующих сторон и способности субъектов данных осуществлять свои права¹⁸.

Как часто отмечается, закон имеет тенденцию отставать от технологий, что является неизбежным результатом разных условий, в которых они работают. Органы по защите данных могут попытаться сократить это отставание с помощью руководящих указаний и рекомендаций мягкого законодательства, основанных на применении принципов защиты данных в новых ситуациях обработки. Такое вмешательство регуляторного органа может гарантировать, что права и интересы субъектов данных будут должным образом учтены без чрезмерного ограничения инноваций негибкими правилами.

5.5 Последствия для трансграничной передачи данных и торговли

Цифровая экономика является транснациональной по своей природе, при этом имеется возможность передачи данных через границы в соответствии с эффективным построением сетей и параметрами распределения ресурсов, которые часто скрыты для пользователей. Глобальный характер сетей также предоставляет благоприятные экономические возможности тем, кто способен обрабатывать данные в одной стране, получая доступ к рынкам других стран. Однако с точки зрения защиты данных такие трансграничные потоки данных ведут к потенциальному ослаблению защиты, гарантированной субъектам данных национальным законодательством. Поэтому режимы защиты данных обычно включают правила, регулирующие передачу персональных данных за пределы юрисдикции.

Контроль за трансграничной передачей данных может принимать разные формы, но, как правило, основан на установлении или достижении некоторого порогового стандарта защиты между двумя юрисдикциями, предусматривающего наличие шлюза, посредством которого осуществляется управление передачей данных. Стандарт, который должен соблюдаться для упрощения трансграничной передачи данных, может быть выражен разными терминами, такими как "эквивалентный", "адекватный", "соответствующий", "сопоставимый", "достаточный", и его соблюдение может достигаться с помощью различных механизмов.

- **Международное соглашение.** Страны могут заключать двусторонние или многосторонние соглашения по управлению потоками данных в целом¹⁹, отдельными категориями персональных данных или в определенных целях (например, в целях обеспечения соблюдения законов).

¹⁵ GDPR, статья 20.

¹⁶ В ЕС см. Директиву 2002/22/ЕС "Об универсальных услугах и правах пользователей в отношении электронных сетей связи и услуг" (ОJ L108/51, 24.2.2002), статья 30. С декабря 2020 года применимым положением будет статья 106 Европейского кодекса по электронным средствам связи (Директива (ЕС) 2018/1972, ОJ L 17.12.2018).

¹⁷ Для получения более подробной информации см. главу 4 "Вопросы, касающиеся потребителей".

¹⁸ Например, см. CNIL 2018.

¹⁹ Например, система Правил трансграничной защиты конфиденциальности АТЭС (CBPR), по которой могут сертифицироваться компании.

- **Определение юрисдикции.** Страна может решить, что правовая база иностранного государства адекватна в целом или на отраслевом уровне и, следовательно, никаких дополнительных ограничений не требуется²⁰.
- **Национальный режим лицензирования/выдачи разрешений.** Национальный регуляторный орган может лицензировать или разрешать передачу данных на индивидуальной или групповой основе.
- **Механизмы частного права.** Частные организации могут иметь возможность заключать обязательные и имеющие исковую силу юридические соглашения, такие как контракты, регулирующие обработку данных при передаче между юрисдикциями.

Большинство режимов также предусматривают отступления или исключения из этих механизмов контроля при определенных условиях, например когда передача осуществляется нечасто или затрагивает лишь ограниченное количество субъектов данных.

Достижение совместимости различных законов о защите данных в нашей глобальной экономике остается постоянной проблемой, поскольку разные культуры и режимы присваивают разные приоритеты конкурирующим общественным интересам, и защита данных является лишь одним из них. Действительно, возможность трансграничной передачи и получения информации затрагивает права людей в той же степени, что и права на защиту данных и неприкосновенность частной жизни.

Очевидно, что характер такого контроля над трансграничными потоками персональных данных может иметь последствия для торговли. В соответствии с Генеральным соглашением по торговле услугами (ГАТС) Всемирной торговой организации (ВТО) государства-члены, взявшие на себя обязательство по либерализации сектора услуг, таких как услуги электросвязи или услуги по предоставлению информации²¹, могут по-прежнему полагаться на исключения, когда это касается "защиты от вмешательства в частную жизнь отдельных лиц при обработке и распространении сведений личного характера и защиты конфиденциальности сведений о личной жизни"²². Это положение может оправдать действия стран, вводящих правила локального хранения данных под предлогом защиты данных при обработке всех или определенных категорий персональных данных, таких как медицинские или финансовые данные. Подробные правила могут либо запрещать обработку персональных данных за пределами конкретной территории, либо ограничивать такие потоки и устанавливать условия, такие как местонахождение данных, требующие, чтобы копии персональных данных сохранялись в пределах юрисдикции происхождения. Однако с точки зрения сферы применения и применимости законы о защите данных должны действовать таким образом, чтобы ограничивать международную торговлю лишь в той мере, в какой это необходимо и соразмерно защите интересов отдельных лиц, а не использоваться в качестве инструмента для маскирования внетарифных торговых барьеров.

Законы о защите данных становятся все более важной частью международной торговой политики и переговоров. Учитывая интересы многих заинтересованных сторон и общественные интересы, можно заключить, что большая совместимость и взаимодействие между национальными режимами защиты данных не только послужат защите интересов субъектов данных, но и позволят снизить затраты на соблюдение нормативных требований для предприятий, особенно МСП, и будут способствовать дальнейшему росту международной торговли и инвестиций (UNCTAD 2016).

5.6 Конфиденциальность сообщений

В законе об электросвязи содержатся внутриотраслевые правила, тогда как правила защиты данных обычно применяются горизонтально по всем отраслям. Таким образом, эти правила могут частично совпадать в определенных областях, например в области безопасности. Действительно, в некоторых странах закон об электросвязи служит единственным источником правил защиты данных или содержит дополнительные специальные правила защиты данных для участников отрасли.

²⁰ Например, GDPR EC, статья 45; к примеру, Исполнительное решение Комиссии (ЕС) 2019/419, январь 2019 года, в отношении Японии.

²¹ КОП, версия 2.1 (2015 год), Секция 8, раздел 84 "Услуги по передаче информации".

²² ГАТС, статья XIV (с) (ii).

В ЕС Директива о защите данных, когда она была впервые предложена, дополнялась отраслевыми мерами, относящимися к конфиденциальности и к электронной связи²³. Эти меры скорее касаются неприкосновенности частной жизни, чем защиты данных, отражая тот факт, что наша деятельность в области связи традиционно рассматривается как часть основного права на неприкосновенность частной жизни²⁴. Эти положения можно разделить на четыре разных типа отношений, касающихся защиты неприкосновенности частной жизни, применяемых в секторе связи.

Во-первых, это отношения между поставщиком услуг и абонентом или пользователем. При предоставлении услуг связи оператор, очевидно, находится в потенциально привилегированном положении в отношении обработки данных пользователя как в части информационного содержания, так и в части соответствующих данных о соединении: "кто", "когда", "где" и "как" устанавливал связь. Закон об электросвязи часто прямо запрещает сотрудникам компаний-операторов использовать это положение в коммерческих или иных целях²⁵. Благодаря цифровой трансформации ценность и объем данных, генерируемых в сетях электросвязи, растут в геометрической прогрессии. Как следствие, в некоторых юрисдикциях приняты отраслевые правила, ограничивающие возможность операторов обрабатывать персональные данные пользователей, за исключением обработки в ограниченных целях, таких как выставление счетов конечным пользователям и обработка платежей за междосетевое соединение, или при соблюдении ограничительных условий, например "только на основе согласия". Одним из аспектов сохраняющихся разногласий в секторе электросвязи является неодинаковость текущих правил регулирования, поскольку в некоторых юрисдикциях традиционные операторы электросвязи подлежат строгому контролю за использованием персональных данных, а поставщики услуг связи по технологии over-the-top (OTT), такие как Skype и Gmail, не попадают под такой контроль и могут бесплатно монетизировать данные своих клиентов. Раздаются призывы к согласованию подхода и устранению этой регуляторной асимметрии, при этом ЕС предлагает двигаться в направлении введения ограничений для всех поставщиков услуг связи²⁶.

Второй тип отношений, касающихся защиты неприкосновенности частной жизни, – это отношения между абонентом услуг связи и пользователем этих услуг. Примером, когда этот сценарий может вызывать опасения, могут служить отношения между работодателем и сотрудниками, поскольку первый может пожелать отслеживать и записывать сообщения сотрудников или других пользователей системы, например клиентов, обращающихся в центр обработки вызовов, в то время как эти пользователи на законном основании предполагают, что они могут делать неприслушиваемые частные звонки или получать уведомления о наличии такого контроля. Поэтому для защиты неприкосновенности частной жизни пользователей закон может требовать, чтобы в детализированных счетах, рассылаемых абонентам, не регистрировались звонки, за которые не взимается плата, например звонки по бесплатному номеру.

Третий тип отношений, касающихся защиты неприкосновенности частной жизни, – это отношения между двумя поддерживающими связь сторонами, традиционно называемыми вызывающей стороной и вызываемой стороной. Примером мер, разработанных для защиты неприкосновенности частной жизни получателя от сообщений отправителя, служат правила, регулирующие использование идентификации линии вызывающего абонента (CLI) и запрещающие передачу незапрашиваемых сообщений, хотя последнее также может быть предназначено для защиты сети от вредоносных действий²⁷. Именно стремление отрегулировать эти отношения с учетом неприкосновенности частной жизни привело к появлению баннеров cookie, столь распространенных в нашей онлайн-среде, которые устроены так, чтобы пользователи были проинформированы (и могли дать свое согласие), когда веб-сайт, с которым взаимодействует пользователь, пытается разместить эти cookie на устройстве пользователя либо в своих собственных целях, либо в интересах третьей стороны.

²³ Первоначальная мера была принята в 1997 году, но впоследствии в нее внесли изменения и заменили Директивой 02/58/ЕС Европейского парламента и Совета в отношении "обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи". OJ L 201/37, 31.7.2002 (Директива ePrivacy).

²⁴ Например, статья 12 Всеобщей декларации прав человека (1948 год) гласит: "Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств".

²⁵ Например, Закон об информации и связи Кении, глава 411A, раздел 30 "Модификация и т. д. сообщений" и раздел 31 "Перехват и раскрытие".

²⁶ Проект Положения об уважении неприкосновенности частной жизни и защите персональных данных в электронных сообщениях, COM (2017) 10 final, 10.1.2017.

²⁷ См. МСЭ, Регламент международной электросвязи (Дубай, 2012 год), статья 7 "Незапрашиваемые массовые электронные сообщения".

Последний тип отношений, касающихся защиты неприкосновенности частной жизни, — это отношения между пользователем и государством. Вводится регулирование обстоятельств и условий, при которых государство может вести слежку за сообщениями в правоохранных целях; в первую очередь это перехват сообщений и получение данных о соединениях, хотя оно распространяется и на требования к хранению данных операторами²⁸. Отношения между пользователями и государством являются важнейшей проблемой неприкосновенности частной жизни и служат причиной того, что "переписка" всегда была элементом стандартного конституционного права на конфиденциальность²⁹.

Возможность и порядок регулирования каждого из этих типов отношений, касающихся неприкосновенности частной жизни, различаются в зависимости от страны; иногда они рассматриваются как часть общего режима защиты данных, секторально в рамках системы электросвязи, в соответствии с трудовым законодательством, как элемент закона о защите прав потребителей³⁰ и/или в рамках уголовно-процессуального законодательства.

5.7 Защита данных и информационная безопасность

Если рассматривать их в виде диаграммы Венна, то защиту данных, обеспечение конфиденциальности и информационную безопасность можно изобразить как три разных, но перекрывающихся множества. Одним из широко признанных основополагающих принципов защиты данных является необходимость реализации "надлежащих" технических и организационных мер безопасности при обработке персональных данных для защиты от случайного и преднамеренного поведения, приводящего к потере, изменению, раскрытию или уничтожению данных. Истинное значение понятия "надлежащая безопасность" варьируется в зависимости от характера обрабатываемых персональных данных, при этом для конфиденциальных персональных данных требуется более сильная защита. Что именно представляют собой конфиденциальные персональные данные, например данные о здоровье и финансовые данные, может быть указано в законодательстве, но вместе с тем должен быть указан и характер обработки, поскольку вредные последствия, такие как непреднамеренная потеря или раскрытие персональных данных, зависят от конкретного контекста. Характер принимаемых мер безопасности также необходимо пересматривать и со временем изменять, чтобы он отражал как технологические достижения, так и сопутствующие риски и угрозы. Следует также отметить, что обязательства по обеспечению безопасности не следует рассматривать как дихотомические в том смысле, что любая утечка приводит к нарушению и потенциальной ответственности, поскольку регуляторный орган может установить, что контролер как объект регулирования принял все надлежащие меры, тем не менее нарушение все же произошло.

Связь между защитой данных и информационной безопасностью рассматривается главным образом как взаимодополняющая по своей природе. Законы и требования в области информационной безопасности, как правило, налагают на операторов систем обязательства по обеспечению безопасности и прозрачности:

- обязательства по охране, которые требуют принятия надлежащих мер безопасности, особенно если организация эксплуатирует критически важную государственную инфраструктуру или предоставляет услуги для нее; и
- обязательства по обеспечению прозрачности, которые обычно принимают форму требований уведомления о нарушениях безопасности, для соответствующих органов и/или индивидуального субъекта данных, если им грозит ущерб и они могут предпринять шаги для смягчения последствий.

Законы о защите данных часто налагают аналогичные обязательства на контролеров и обработчиков. Хотя такая взаимодополняемость полезна, важно, чтобы стандарты, устанавливаемые соответствующими режимами, такие как временные рамки для сообщения о нарушениях, были согласованы таким образом, чтобы не создавать юридических неопределенностей и дополнительной нагрузки на объекты регулирования.

²⁸ Например, в России Федеральный закон 374-ФЗ 2016 года требует, чтобы поставщики хранили контент и данные о соединениях в течение шести месяцев.

²⁹ Резолюция Организации Объединенных Наций 68/167 "Право на неприкосновенность личной жизни в цифровой век", 18 декабря 2018 года.

³⁰ Более подробную информацию см. в главе 4 "Вопросы, касающиеся потребителей".

Вставка 5.3. Цена утечки данных



В январе 2019 года группа гостиниц Marriott сообщила, что хакеры получили доступ к учетным записям примерно 339 млн. гостей из базы данных бронирования ее подразделения Starwood, приобретенного в 2016 году. Похищенные данные включали имена, адреса, номера телефонов, адреса электронной почты, данные кредитных карт, номера паспортов и информацию о поездках. Однако из 25 млн. паспортов данные 20 млн. были зашифрованы, поэтому Marriott предположила, что они останутся защищенными. Что касается расходов, то Marriott, как ожидается, придется выплатить пострадавшим клиентам, особенно тем, которые впоследствии стали жертвами мошенничества, около 500 млн. долл. США. Утечка расследовалась Канцелярией Комиссара по информации Управления по защите данных Соединенного Королевства, которая наложила штраф в размере 99 млн. фунтов стерлингов в пользу 7 млн. гостей, которые являлись гражданами Соединенного Королевства.

Вопросы безопасности также могут вступать в противоречие с законами о защите данных. Получение доступа к информации или передача информации могут рассматриваться как необходимая мера защиты безопасности общества, что может противоречить положениям о защите данных, ориентированным на защиту прав человека. Два ключевых вопроса, вызывающих политические дебаты во многих странах, – это безопасность в онлайн-среде и нынешняя пандемия COVID-19.

Безопасность в онлайн-среде. Темная сторона интернета как среды заключается в том, что он может способствовать противозаконным и наносящим вред действиям – от взлома систем до показа детям непристойных материалов и распространения фейковых новостей. Борьба с *противозаконными* действиями в киберпространстве сопряжена с трудностями ввиду эфемерного характера онлайн-деятельности, ее трансграничной природы и технической сложности (см. Walden 2016 и др.). Принятие мер против *наносящих вред* (но законных) действий порождает еще большие проблемы для директивных, законодательных и регуляторных органов. Несмотря на широкое признание того, что для эффективности предпринимаемых действий требуется участие субъектов как государственного, так и частного секторов, во многих странах ведутся очень жаркие дебаты по вопросу об определении соответствующих ролей и обязанностей. Одно из направлений этих дебатов относится к той мере, в которой для расследования, предотвращения и выявления противозаконных и наносящих вред действий должны использоваться персональные данные. Анонимность в интернете, обеспечиваемая виртуальными частными сетями (VPN) и сквозным шифрованием, в равной степени защищает как политического диссидента или человека, информирующего общество о нарушениях и злоупотреблениях, так и растлителя несовершеннолетних или террориста.

COVID-19. Как отмечено во вставке 5.2, пандемия породила противоречие между необходимостью защиты здоровья людей и ограничением на использование персональных данных и их злоупотреблением. Собираемые данные о физических лицах могут не только помочь остановить распространение болезни, но и способствовать более глубокому изучению вируса с помощью их агрегирования и анализа с течением времени, чтобы в будущем государственные органы могли лучше справляться с подобными чрезвычайными ситуациями в сфере общественного здравоохранения. Страны должны определить ряд вещей, которые имеют прямое отношение к субъектам данных и их персональным данным: типы данных о физических лицах, которые можно собирать (например, данные о местоположении); является ли раскрытие информации обязательным или добровольным; можно ли объединять собранные данные с другими данными о человеке

(например, с удостоверением личности); диапазон целей, для которых могут использоваться данные (например, уход и лечение или исследования); и сроки хранения данных.

Важная тема дискуссий в сфере защиты данных – псевдонимизация или обезличивание персональных данных с использованием таких методов, как шифрование. Что касается псевдонимизации, то она хотя и помогает защитить персональные данные, остается предметом регулирования защиты данных, поскольку процесс может быть обращен вспять и данные повторно идентифицированы. Напротив, эффективное обезличивание выводит данные из-под действия режима защиты данных, поскольку они перестают быть персональными данными. Споры ведутся вокруг того, действительно ли определенные методы обезличивания эффективно предотвращают повторную идентификацию физических лиц при наличии достаточной мотивации, технических возможностей и возможности сопоставить данные с другими наборами данных (Ohm 2010). Методы псевдонимизации и обезличивания служат инструментами эффективной информационной безопасности, но могут рассматриваться и как потенциальное "оружие", имеющее как гражданское, так и военное применение, а также делающее интернет "темным" и препятствующим законным расследованиям со стороны правоохранительных органов. Обеспечение баланса этих многочисленных и конфликтующих друг с другом интересов – трудный политический выбор для правительств и законодательных органов.

Справочные документы

- African Union. 2020. *The Digital Transformation Strategy for Africa (2020-2030)*. Addis Ababa: African Union. <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>
- Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.
- CNIL (Commission Nationale Informatique & Libertés). 2018. *Blockchain: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*. Paris: CNIL. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf
- Greenleaf, G., and B. Cottier. 2020. "2020 Ends a Decade of 62 New Data Privacy Laws." *Privacy Laws and Business International Report* 163 (February): 24-26.
- ITU (International Telecommunication Union). 2018. *Regulatory Challenges and Opportunities in the New ICT Ecosystem*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT03-2018-PDF-E.pdf
- Ohm, P. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* (57) 6: 1701-1777. <https://www.uclalawreview.org/pdf/57-6-3.pdf>
- UNCTAD (United Nations Conference on Trade and Development). 2016. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. New York and Geneva: UNCTAD. https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
- Walden, I. 2016. *Computer Crimes and Digital Investigations*. Oxford: Oxford University Press.
- Wang, G.E. 2019. "Humans in the Loop: The Design of Interactive AI Systems." *Human-centred Artificial Intelligence Blog*, October 20, 2019. <https://hai.stanford.edu/blog/humans-loop-design-interactive-ai-systems>
- World Bank. 2021 (forthcoming). *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank.
- Zuboff, S. 2019. *The Age of Surveillance Capitalism*. New York: Public Affairs.

Глава 6. Управление использованием спектра



6.1 Введение

В современном обществе, которое все больше становится цифровым, решающее значение для расширения развертывания, покрытия и охвата сетей электросвязи, предоставляющих широкие возможности для социально-экономического развития, имеют доступ к спектру и надлежащие процессы управления использованием спектра. Повышенный спрос на услуги этих сетей для поддержки различных онлайн-приложений в таких секторах экономики, как здравоохранение, транспорт, образование, сельское хозяйство, обеспечение занятости, государственное управление и финансовые услуги, приводит к необходимости эффективного использования спектра и внедрения эффективных процессов управления использованием спектра.

Часть 1 настоящей главы, подготовленная Бюро радиосвязи Международного союза электросвязи, представляет собой общее руководство по нормативной базе для управления использованием спектра на национальном уровне, начиная с определения международного контекста и процессов. Это выдержка из Отчета МСЭ-R SM.2093-3 "Руководство по регламентарной структуре для управления использованием спектра на национальном уровне", которая приводится здесь с разрешения МСЭ.

В части 2 обсуждаются ключевые применения и нормативные аспекты, определяющие использование спектра в будущем, и выделяются некоторые основные моменты, которые предлагается рассмотреть регуляторным органам на национальном уровне, исходя из соответствующего опыта разных стран. В ней представлены некоторые механизмы распределения спектра и лицензирования нового спектра с должным учетом развития технологий. В ней также рассматриваются вопросы поощрения использования спектра для этих ключевых применений и бизнес-модели, способствующие укреплению существующих и новых подходов к развертыванию сетей беспроводной широкополосной связи.

6.2 Часть 1. Руководство по регламентарной структуре для управления использованием спектра на национальном уровне

Рост использования обществом радиотехнологий и широкие возможности для социально-экономического развития, открываемые этими технологиями, подчеркивают важность радиочастотного спектра и процессов управления использованием спектра на национальном уровне. Технический прогресс постоянно создает возможности для появления множества новых применений спектра, что ведет ко все большему интересу к этому ограниченному ресурсу и растущему спросу на него. Ввиду повышенного спроса требуется эффективное использование спектра и внедрение эффективных процессов управления его использованием.

Управление использованием спектра сочетает в себе административные и технические процедуры, необходимые для обеспечения эффективного использования радиочастотного спектра всеми службами радиосвязи, определенными в Регламенте радиосвязи МСЭ, а также для работы радиосистем, не создающих вредных помех.

Роль Сектора радиосвязи Международного союза электросвязи (МСЭ-R) в управлении использованием спектра на международном уровне заключается в обеспечении рационального, справедливого, эффективного и экономичного использования радиочастотного спектра всеми службами радиосвязи, включая спутниковые службы, и проведении в неограниченном частотном диапазоне исследований, на основании которых принимаются Рекомендации и Отчеты МСЭ-R.

Регламентарную и политическую функции МСЭ-R выполняют всемирные и региональные конференции радиосвязи и ассамблеи радиосвязи при поддержке исследовательских комиссий.

В настоящей главе содержится руководство по регламентарной структуре для управления использованием спектра на национальном уровне¹.

Международный контекст

На международном уровне сектор электросвязи, включая радиосвязь, организован в рамках Международного союза электросвязи (МСЭ), который обеспечивает основу для координации и управления использованием радиочастотного спектра. Промежуточное положение между МСЭ и национальными администрациями занимают организации двух иных видов – региональные организации и специализированные международные организации, которые также участвуют в управлении использованием спектра на региональном и глобальном уровнях.

На региональном уровне созданы организации, которые объединяют администрации и в которых в ряде случаев участвуют представители отрасли или операторы радиосвязи. Целью таких организаций является выработка общих позиций при подготовке к процессу принятия решений МСЭ, согласование национальных планов распределения частот в относительно гибких, установленных МСЭ рамках в целях упрощения скоординированного внедрения новых служб, а также согласование стандартов и процедур для проведения сертификации оборудования, обеспечивающей его свободное обращение и использование в заинтересованных странах.

На глобальном и региональном уровнях также существуют специализированные международных организации в тех секторах экономики, в которых используется радиосвязь и деятельность которых, вследствие этого, зависит от доступности спектра: гражданская авиация, морской транспорт, метеорология, радиовещание, любительские радиосвязь, радиоастрономия и исследования.

Всемирная торговая организация в рамках Генерального соглашения по торговле услугами (ГАТС), признавая суверенное право государств управлять использованием спектра частот в аспекте решения собственных задач, осуществляет разработку инструментов, необходимых для того, чтобы реализация этого права не привела на практике к возникновению барьеров при торговле услугами между ее членами.

¹ Часть 1 настоящей главы взята из публикации МСЭ (2018b). Данный Отчет относится к серии публикаций по управлению использованием спектра, разработанных МСЭ-R. Список справочных документов в конце настоящей главы включает ряд других соответствующих публикаций МСЭ по управлению использованием спектра.

Международные принципы, регулирующие использование спектра

В международных соглашениях МСЭ признается, что использование спектра радиочастот является суверенным делом каждого государства, однако эффективность его использования обуславливает необходимость регулирования. Существуют базовые глобальные документы, ратифицируя которые, государства принимают на себя обязательство соблюдать общие правила совместного использования спектра, целью чего являются эффективное использование и справедливый доступ.

Документами МСЭ, касающимися управления использованием спектра, являются Устав (У), Конвенция (К) и в основном Регламент радиосвязи (РР). Только эти документы имеют для Государств-Членов обязательную силу.

Спектр радиочастот является неистощимым, но ограниченным природным ресурсом, доступным во всех странах и в открытом космосе. В силу того что любая передающая радиостанция может создавать вредные помехи для использования спектра на Земле и в космосе, спектр является общим ресурсом всего человечества, требующим рационального управления его использованием на основе соглашения уровня договора между всеми странами. В таком духе МСЭ в течение более ста лет разрабатывает правовые инструменты, с тем чтобы в основе использования спектра лежали базовые принципы, установленные в Уставе МСЭ.

Основной нормативной базой, на которую опираются государства, осуществляя эксплуатацию служб радиосвязи, и основным инструментом, определяющим использование спектра на международном уровне, является Регламент радиосвязи МСЭ (РР). Регламент имеет статус договора и периодически пересматривается (примерно каждые три года) Всемирной конференцией радиосвязи (ВКР), на которой присутствует большинство Государств – Членов МСЭ.

В РР определяются, среди прочего, полосы частот, распределенные службам радиосвязи, а также нормативные условия и процедуры, которые должны выполнять администрации при введении радиостанций, обеспечивающих работу этих служб. Руководящий принцип, лежащий в основе всех положений РР, заключается в том, что новые виды использования не должны допускать создания вредных помех службам, обеспечиваемым станциями, которые используют присвоенные им частоты в соответствии с РР и которые занесены в Международный справочный регистр частот (МСРЧ) с благоприятным заключением.

Целью РР, который был составлен на нескольких последовательно прошедших ВКР, является предоставление каждой стране максимально возможной гибкости в отношении использования спектра. В частности, согласно Таблице распределения частот (Статья 5 РР) в каждой полосе разрешается работа нескольких служб радиосвязи; эти службы необязательно совместимы на местном уровне, но каждая страна может выбрать те из них, которые пожелает внедрить на своей территории. Нормативные положения и процедуры РР обеспечивают для каждой страны возможность координации, при необходимости, станций, обеспечивающих работу выбранных служб, со станциями других стран, которые могут оказаться затронутыми, в результате чего таким образом достигается максимально эффективное использование спектра.

Преимущество этой относительно гибкой основы заключается в том, что учитывается широкий диапазон испытываемых странами потребностей в спектре и соблюдается их суверенное право удовлетворять свои нужды при условии, что это не создает чрезмерных ограничений для других стран. Недостатком этой основы является ограничение экономии за счет масштаба и уровня функциональной совместимости, требуемого для развития радиосвязи, в частности в рамках всемирных служб или служб, предназначенных для общего пользования (например, подвижная телефонная связь, спутниковое радиовещание). Вследствие этого в течение прошедших лет прилагались значительные усилия, направленные на гармонизацию использования спектра на региональном и даже глобальном уровне, в частности в области подвижной телефонии. Проводится деятельность по гармонизации, с тем чтобы определить конкретные полосы частот для применений, соответствующих определенным стандартам. Целью такой гармонизации является повышение уровня экономии за счет масштаба и снижение уровня помех и несовместимости.

Принципы использования спектра на национальном уровне

Спектр радиочастот представляет собой общественное достояние. Как таковой спектр находится в ведении государства, и управление его использованием должно осуществляться эффективно, с тем чтобы обеспечивались максимальные выгоды для всего населения. Такое управление использованием

спектра обычно осуществляется в рамках нормативной базы, которую составляют законодательство, регулирование, процедуры и меры политического характера.

Вследствие права государств на управление использованием спектра правомочные пользователи спектра получают преимущества права и несут соответствующие обязательства в отношении доступа к спектру и его использования.

Распределение полос частот для правительственного или административного использования, радиовещания и электросвязи в частном промышленном и коммерческом секторах с учетом Таблицы распределения частот МСЭ (Статья 5 РР), а также с должным учетом международных обязательств государств лежит на государстве или получившем соответствующие полномочия регуляторном органе.

Управляющий орган составляет национальную таблицу распределения частот и национальный регистр частот, в котором перечисляются присвоения частот, и осуществляет их обновление.

В процессе координации введения на национальной территории радиостанций должно обеспечиваться оптимальное использование имеющихся мест расположения, с тем чтобы добиться максимально возможной общей электромагнитной совместимости.

Государство может включать в свою нормативную базу положения, направленные на защиту передающих и приемных радиоцентров от электромагнитных помех. Государство или управляющий орган может вводить эффективный и надлежащий порядок использования спектра, принимая во внимание имеющиеся технологии и уровень развития общества.

Для обеспечения оптимального использования спектра частот управляющий орган может повторно подтвердить, что указанная задача выполнима либо путем непосредственного осуществления полномочий, либо в рамках переговорного процесса, включающего финансовые соображения, или на основе процедуры, сочетающей оба эти подхода. Например, управляющий орган может применять перераспределение спектра.

Что касается сферы государственного управления, управляющий орган может устанавливать правила, в том числе имеющие односторонний порядок (например, аннулирование лицензии для отмены использования присвоенных частот), в целях надлежащего исполнения миссий в государственных интересах.

Использование спектра для радиовещания и для целей электросвязи в частном коммерческом и промышленном секторах

Использование частот в пределах национальной территории либо для передачи, либо для приема сигналов требует административного разрешения (то есть лицензии). Государство или имеющий полномочия управляющий орган (который в ряде стран не обязательно является регуляторным органом, упоминавшимся в предыдущем разделе) выдает отдельные разрешения на использование спектра в пределах национальной территории посредством присвоения конкретных частот.

В случае радиостанций, расположенных в экстерриториальных зонах (море, космос), государство или уполномоченный орган также могут выдавать разрешения в соответствии с РР и любыми соответствующими международными соглашениями.

В исключительных случаях и при условиях, определенных в национальных нормативных правилах, маломощные устройства радиосвязи малого радиуса действия и устройства, не использующие частоты, конкретно присвоенные их пользователю, могут вводиться без ограничений. Государство может потребовать от имеющих разрешение операторов выплачивать компенсацию за право использования спектра. Такая компенсация должна быть пропорциональна оценочной стоимости ресурса.

Государство или имеющий полномочия управляющий орган может ввести для имеющих разрешение операторов сроки и условия, обуславливаемые общественными интересами.

Компетентный орган должен определять технические стандарты и основополагающие требования в части:

- здравоохранения;
- электромагнитной совместимости;

- эффективного использования спектра, распределенного наземным или космическим станциям, и ресурсов орбиты, с тем чтобы не допускать создания вредных помех.

Радиооборудование, использование которого разрешено в пределах национальной территории, должно соответствовать этим стандартам и основополагающим требованиям.

Предотвращение и устранение помех

Государство или его уполномоченные органы должны обеспечивать использование спектра в соответствии с условиями, предусмотренными в национальных и международных регламентах, в частности в Статье 15 РР. Они должны добиваться, чтобы оборудование, не соответствующее основополагающим стандартам и требованиям, которые установлены в национальных нормативах, не поступало в продажу. Они должны также принимать меры для предотвращения неправомерного использования спектра, применяя такие методы, как:

- контроль за использованием спектра и отыскание неразрешенных радиостанций;
- управление выдачей лицензий, предоставляющих доступ к спектру, и контроль технических и эксплуатационных условий работы радиостанций;
- выявление источников помех в ответ на поступающие жалобы.

Государство или его управляющие органы должны прекращать причинение любых признанных вредных помех.

В зависимости от национального законодательства ответственность государства может возникать в случае нарушения какого-либо интереса. Претензию может предъявить любое лицо, в том числе иностранное, которое несет убыток. Государство может нести ответственность за различные нарушения – бездействие, недостаток средств, безрезультатность, задержку действия, серьезность нарушения общего интереса и т. д., такое нарушение должно соответствовать законодательству данной страны.

Права и обязанности зарегистрированных пользователей

Разрешение (или лицензия) предоставляет не право собственности на участок спектра, но лишь право использовать этот участок в течение периода времени, определенного в таком разрешении, и в соответствии с правилами, содержащимися в перечне условий, прилагаемых к данному разрешению.

Государство или его уполномоченный управляющий орган может ограничивать число разрешений, предоставляющих доступ к спектру, в силу технических ограничений, характерных для доступности частот. Разрешение не подлежит передаче, если это не предусмотрено в национальной нормативной базе.

Государство или уполномоченный орган прилагает усилия для обеспечения определенного уровня защиты пользователей от вредных помех. Зарегистрированные пользователи должны выполнять общие правила и правила, определенные в условиях, и могут использовать только те частоты, которые им присвоены.

Условия, определяемые для операторов электросвязи, которым разрешено создание сети общего пользования, могут включать также обязательства общего характера, такие как:

- минимальный охват населения или территории;
- минимальное число услуг, предоставляемых потребителям, и минимальный уровень качества;
- гарантированная защита личных данных и частной жизни пользователей и безопасный электронный обмен информацией.

Зарегистрированный пользователь лишается выданного ему разрешения в случае несоблюдения им своих обязательств. В зависимости от серьезности нарушения могут применяться следующие наказания:

- полное или частичное приостановление, сокращение срока или отзыв выданного разрешения;
- штраф, если несоблюдение не составляет уголовного преступления.

В национальном законодательстве могут определяться уголовные наказания (тюремное заключение и/или денежное взыскание), применяемые в случае наиболее серьезных нарушений, таких как:

- незаконное создание или поддержание в нарушение решения о приостановлении или отзыве разрешения;
- причинение помех зарегистрированной службе путем несанкционированного использования частоты или путем использования средства радиосвязи, не отвечающего основополагающим требованиям;
- в случае радиовещания нарушение положений относительно мощности или местоположения передатчика.

Прозрачность управления использованием спектра на национальном уровне

В области управления использованием спектра одной из кардинальных задач, стоящих перед каждой администрацией, является определение категорий пользователей в зависимости от применяемого режима управления и составление национальной таблицы распределения частот, в которой использование спектра распределяется по категориям пользователей с определением их соответствующих прав и обязанностей.

Требование обеспечения прозрачности изменяется в зависимости от рассматриваемого типа пользователя. Как отмечалось выше, прозрачность представляет собой крайне желательный метод управления в условиях конкурентных рынков; в других областях однако, где особое значение имеют конфиденциальность и секретность, прозрачность не является ни требуемой, ни желательной. Действительно, даже при регулировании рынков, открытых для конкуренции, прозрачность частично ограничивается правом на защиту общественных потребностей и коммерческой тайны.

Например, значительная часть спектра распределяется обычно для неотъемлемых государственных функций, таких как оборона, политика и безопасность. Эти функции требуют особой защиты, и прозрачность в их управлении не является правилом. В случае другой деятельности, для которой важна безопасность, такой как морские и воздушные перевозки, может применяться ограниченная прозрачность. Вместе с тем при использовании спектра следует осуществлять прозрачное управление, за исключением упомянутых выше случаев.

Прозрачность может применяться, в частности, в следующих областях:

- распределение частот службам, планирование частот (участие в создании соответствующих частей национальной таблицы распределения частот);
- выдача лицензий, присвоения станциям, заявление для МСЭ;
- условия совместного использования частот;
- установка/группирование станций;
- подготовка к переговорам по международным договорам, касающимся управления использованием спектра (в частности ВКР, на которых вносятся поправки в РР). На практике, несмотря на то что договоры обсуждаются правительствами, они могут изменять национальные нормы, применяемые к другим участникам, которые, следовательно, должны иметь возможность принять участие, при необходимости, в подготовке к таким переговорам на национальном уровне.

Взаимосвязь между регулированием на международном и национальном уровнях

Как и в любой другой области, национальное законодательство разрабатывается с должным учетом принятых государством обязательств в рамках его международной деятельности. Что касается радиочастот и связанных с ними орбит, права и обязанности государств регулируются главным образом РР, в котором предусматривается, что эти орбиты и частоты надлежит использовать рационально, эффективно и экономно, так, чтобы обеспечить справедливый доступ к этим орбитам и к этим частотам разным странам.

РР дополняет Устав и Конвенцию Союза. РР имеет статус международного договора, и, следовательно, национальное законодательство должно быть согласовано с его положениями. Это правило, очевидно, является основополагающим для разработки национального законодательства. Однако следует учитывать, что РР подвергается пересмотру на ВКР, которые проходят в среднем каждые три года. Поэтому следует обеспечивать обновление национальных норм с такой же периодичностью.

Государства могут быть связаны другими обязательствами перед какой-либо региональной организацией или в рамках двусторонних или многосторонних соглашений.

Контроль за использованием спектра

Для гарантии того, что спектр используется в соответствии с существующими нормами и выданными разрешениями, должна существовать система мониторинга спектра, состоящая из оборудования фиксированной и подвижной связи.

Это оборудование применяется для проверки того, что частоты используются в соответствии с полученным разрешением. Оно может также использоваться для обнаружения источника помех.

Состав таких средств весьма широк, и они должны по возможности использоваться на основе альянсов. Они могут применяться для рассмотрения международных запросов по просьбе МСЭ-R или иностранной администрации в случае наличия помех².

Передовая практика управления использованием спектра на национальном уровне

Относясь с должным вниманием к Конвенции и Уставу МСЭ, данный раздел описывает передовую практику управления использованием спектра на национальном уровне³. Международные методы не включены. Однако некоторые из описанных ниже методов служат интерфейсом или переходом к международным методам, например тем, которые способствуют сотрудничеству с коллегами в других странах или координации, вроде той, что наблюдается при двусторонних или многосторонних консультациях, предшествующих ВКР, или на международной встрече по спутниковой координации. Эти методы будут способствовать формированию гармонизированной – до разумных пределов – глобальной политики в области управления использованием спектра за счет применения национальными администрациями согласованных методов.

Передовая практика

- Создание и поддержка национальной организации по управлению использованием спектра, ответственной за управление радиочастотным спектром в интересах общества, либо независимой, либо в составе регуляторного органа в области электросвязи.
- Продвижение прозрачной, справедливой, экономически эффективной и действенной политики управления использованием спектра, то есть такое выполнение регуляторных функций, которое способствует эффективному и адекватному использованию спектра, обеспечение отсутствия вредных помех и возможность наложения технических ограничений в целях служения интересам общества.
- Публикация, по возможности, национальных планов распределения частот и данных о частотных присвоениях, чтобы поощрять открытость и облегчать развитие новых систем радиосвязи, то есть проводить общественные консультации по обсуждению предложенных изменений в национальные планы распределения частот и решений по управлению использованием спектра, которые могут затронуть поставщиков услуг, что позволит заинтересованным сторонам участвовать в процессе принятия решения.
- Поддержание стабильности процесса принятия решения, который предусматривает учет общественных интересов в управлении использованием радиочастотного спектра, то есть обеспечение законной уверенности в наличии справедливых и прозрачных процессов выдачи лицензий на использование спектра, применяя, когда необходимо, конкурентоспособные механизмы.
- Обеспечение в национальном процессе распределения спектра в специальных случаях, когда это оправдано, возможности выдачи отказа по использованию спектра.
- Наличие механизма для пересмотра принятых решений по управлению использованием спектра.
- Уменьшение избыточного регулирования.

² Для получения более подробной информации см. МСЭ (2011).

³ Содержание настоящего раздела представляет собой выдержку из публикации МСЭ (2015b), Приложение 2.

- Поощрение политики радиосвязи, направленной на гибкое, до реальной степени, использование спектра, учитывающей развитие служб⁴ и технологий, использующей ясно определенные методы, то есть:
 - устранение регуляторных барьеров и распределение частот по принципу облегчения выхода на рынок новых участников;
 - поощрение эффективности использования спектра за счет сокращения или устранения ненужных ограничений на использование спектра, таким образом поощряя конкуренцию и принося выгоды потребителям; а также
 - продвижение инноваций и введение новых областей использования и радиотехнологий.
- Установление открытой и справедливой конкуренции на рынках оборудования и предоставления услуг и устранение любых барьеров на пути к открытой и справедливой конкуренции.
- Согласование, насколько это реально, эффективной внутренней и международной политики использования спектра, включая использование радиочастот для космических служб, для любой орбитальной позиции на геостационарной спутниковой орбите или характеристик спутников на любых других орбитах.
- Работа в сотрудничестве с региональными и другими международными органами по разработке скоординированных методов регулирования, то есть обеспечение отсутствия вредных помех за счет тесного сотрудничества с регуляторными органами других регионов и стран.
- Удаление любых регуляторных барьеров на пути к свободному обращению и глобальному роумингу подвижных оконечных устройств и аналогового оборудования радиосвязи.
- Использование международных рекомендованных форматов данных и элементов данных для обмена данными и целей координации, например форматов и элементов данных, описанных в Приложении 4 к РР и в Словаре данных по радиосвязи МСЭ (Рекомендация МСЭ-R SM.1413).
- Использование правил управления проектами "по контрольным точкам", чтобы контролировать и управлять внедрением долговременной системы радиосвязи.
- Принятие технологически нейтральных решений, которые учитывают развитие новых областей применения радиослужб.
- Облегчение своевременного внедрения соответствующих новых приложений и технологий при защите существующих служб от воздействия вредных помех, включая разработку механизма, позволяющего компенсацию для систем, которые должны перейти в другие полосы частот, для того чтобы дать возможность удовлетворения новых потребностей использования спектра.
- Рассмотрение эффективной политики уменьшения ущерба, который мог бы быть нанесен пользователям существующих служб при перераспределении спектра.
- Когда спектр дефицитен, необходимо обеспечить его совместное использование с помощью доступных методов (то есть частотное, временное, пространственное, кодовое разнесение, новые методы модуляции, обработка сигналов и т. д.), включая, до известной степени, использование методов уменьшения воздействия помех и экономического стимулирования.
- Использование механизмов принуждения, если уместно, то есть применение санкций за несоблюдение обязательств и за неэффективное использование радиочастотного спектра при соблюдении процессов обжалования.
- Использование региональных и международных стандартов всякий раз, когда возможно, и, при необходимости, их соответствующее отражение в национальных стандартах.
- Отдавать предпочтение, по мере возможности, промышленным стандартам, в том числе тем, которые включены в Рекомендации МСЭ, а не национальным правилам.

⁴ Всякий раз, когда в этом Справочнике используется термин "службы", он означает области применения и определенные МСЭ службы радиосвязи.

6.3 Часть 2. Ключевые применения и нормативные аспекты, определяющие использование спектра в будущем

Введение

В среде, которая все больше становится цифровой, решающее значение для расширения развертывания сетей электросвязи и их покрытия, а также удовлетворения постоянно растущего спроса на услуги передачи данных имеет адекватный доступ к спектру. Эти сети поддерживают множество онлайн-приложений, что распространяет влияние управления использованием спектра на ряд секторов экономики, изменяя способы доступа людей к ресурсам в таких секторах, как здравоохранение, транспорт, образование, сельское хозяйство, обеспечение занятости, государственное управление и финансовые услуги. Поскольку спектр является ограниченным ресурсом, от регуляторных органов требуется надлежащее управление им в целях обеспечения справедливого доступа и свободной от помех среды для разнообразных пользователей и служб, а также для внедрения новых технологий. Соответственно нужно найти правильный баланс между нормативными требованиями, обеспечивающими определенность и защиту потребителей, и необходимостью обеспечения гибкости для разработки новых беспроводных технологий.

В настоящей главе обсуждаются ключевые применения, определяющие использование спектра в будущем, и выделяются некоторые основные моменты, которые предлагается рассмотреть регуляторным органам на национальном уровне, исходя из соответствующего опыта разных стран⁵. В ней представлены некоторые механизмы распределения спектра и лицензирования нового спектра с должным учетом развития технологий. В ней также рассматриваются вопросы поощрения использования спектра для этих ключевых применений и бизнес-модели, способствующие укреплению существующих и новых подходов к развертыванию сетей беспроводной широкополосной связи. Еще один обсуждаемый аспект – осуществление политики, которая позволит заинтересованным сторонам использовать новые технологии, такие как технологии подвижной связи пятого поколения (5G) и интернет вещей (IoT).

Основные тенденции в управлении использованием спектра для внедрения новых технологий

Управление использованием спектра имеет своей целью определение распределений спектра службам радиосвязи, технических спецификаций и типов услуг и технологий, которые могут эксплуатироваться в стране. Таким образом оно может определять темпы внедрения таких технологий.

Беспроводные технологии стали самым распространенным способом доступа в интернет во всем мире с использованием как лицензируемых, так и нелицензируемых полос частот, а также разнообразных устройств. Необходимость использовать больше приложений для удаленной работы и электронного обучения, а также растущая популярность онлайн-развлечений (таких как потоковая передача кинофильмов и музыки и игры) способствуют росту трафика данных, особенно иницируемого использованием смартфонов и планшетов. По состоянию на конец 2019 года абонентами услуг подвижной широкополосной связи были около 5,3 млрд. человек, что подчеркивает ее важность для обеспечения возможности установления соединений (ITU 2019c). Доступ к услугам беспроводной широкополосной связи можно получить разными способами, включая сети подвижной связи, точки доступа Wi-Fi, спутники, а в последнее время – БПЛА и аэростаты. Эффективная политика в области использования спектра призвана способствовать внедрению разнообразных услуг в условиях постоянного технического прогресса.

Подвижный широкополосный доступ требует достаточного спектра, который должен быть определен для услуг Международной подвижной электросвязи (IMT) – широко известных как 3G, 4G и 5G, – а для технологий, использующих нелицензируемый спектр, требуется достаточное количество нелицензируемого/освобожденного от лицензирования спектра. В результате государственные органы должны определить наилучшие возможные способы планирования, распределения и присвоения спектра для удовлетворения будущих потребностей операторов и потребителей, обеспечивая при этом эффективное использование ценных ресурсов спектра и стимулируя конкуренцию. Поскольку спектр играет критически важную роль в реализации всеобщего доступа к возможностям широкополосной связи, его эффективное использование оказывает прямое социально-экономическое воздействие на множество сегментов общества.

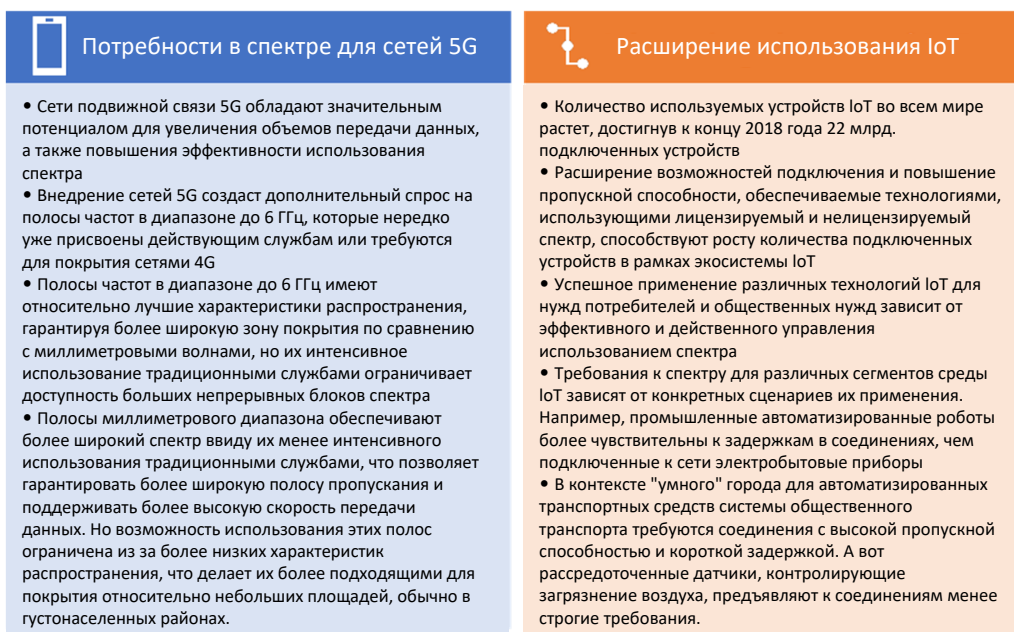
⁵ Более подробное рассмотрение тем, затронутых в настоящей главе, см. в соответствующих тематических разделах *Платформы цифрового регулирования*.

В последнее время разработаны новые технологии и приложения в целях повышения качества и расширения доступа к широкополосным соединениям. Регуляторным органам следует учитывать их при рассмотрении национальных планов управления использованием спектра, обеспечивая при этом развитие существующих технологий. Например, в дополнение к наземным сетям 5G также развиваются такие применения, как станции на высотной платформе (HAPS) и спутники на негеостационарной орбите (НГСО), способствуя расширению охвата существующими услугами электросвязи. Кроме того, цифровые приложения в целом и экосистема IoT в частности состоят из разнообразных приложений с широким диапазоном требований к спектру.

Технологические инновации, определяющие спрос на новые участки спектра

Спрос на доступ ко многим участкам спектра растет, поскольку новые технологии позволяют использовать более широкий диапазон полос частот. Например, применения IMT с использованием сетей 5G уже конкурируют с традиционными службами в диапазонах низких, средних и высоких частот. Сегодня наиболее распространенные полосы частот для сетей подвижной связи находятся в диапазонах низких и средних частот, однако интерес к использованию для сетей 5G диапазонов высоких частот, таких как диапазон миллиметровых волн (mmWave) 24–86 ГГц, привлекает внимание и к ним. Этот повышенный спрос придает еще большее значение эффективному использованию спектра. К тому же такие применения, как HAPS и спутники НГСО, повышают потребность в доступе к спектру и в других диапазонах. В то же время растет количество взаимосвязанных устройств, работающих на основе таких технологий, как Bluetooth и Wi-Fi, что еще больше обостряет конкуренцию за ценный и ограниченный ресурс спектра (см. рисунок 6.1).

Рисунок 6.1. Технологии, определяющие спрос на спектр



 Развитие Wi-Fi • Технологии беспроводных сетей имеют решающее значение для внедрения подключенных устройств и развития экосистемы IoT. • Wi-Fi и другие беспроводные технологии работают в нелицензируемом спектре и позволяют вести передачу в относительно широком диапазоне частот. • В дополнение к ранее использовавшимся диапазонам 900 МГц, 2,4 ГГц и 5 ГГц более новые технологии Wi-Fi внедряются в диапазонах 60 ГГц (57–66 ГГц) и 6 ГГц (5925–7125 МГц). • Некоторые страны (например, Соединенные Штаты и Соединенное Королевство) повышают доступность диапазона 6 ГГц для безлицензионного использования. • Новые правила Соединенных Штатов предоставляют возможность нелицензируемого использования полосы 1200 МГц в диапазоне 6 ГГц. • В целом регуляторные органы при распределении и присвоении спектра должны помнить о потенциальной ценности нелицензируемых технологий, включая Wi-Fi.	 Соединения HAPS • Системы HAPS (то есть радиостанций, расположенных в стратосфере на высоте от 20 до 50 км над поверхностью Земли) позволяют расширить доступ к беспроводным соединениям. • Технология HAPS поддерживает другие наземные технологии, благодаря чему возможность установления соединений и предоставления услуг электросвязи может быть распространена на сельские и отдаленные районы. • HAPS может служить инструментом расширения существующих наземных сетей и предоставления более качественных услуг в подключенных районах, а также обеспечить возможность установления соединений в чрезвычайных ситуациях. • Для систем HAPS могут использоваться полосы частот, присвоенные либо непосредственно поставщику услуг HAPS, либо его партнеру – традиционному оператору связи, такому как оператор подвижной связи.  Спутники НГСО • Спутниковые системы НГСО, состоящие из сотен или даже тысяч спутников, обеспечивают возможность установления соединений в тех районах, которые в настоящее время не охвачены наземной инфраструктурой электросвязи. • Это создает некоторые проблемы для управления использованием спектра в отношении управления использованием различных полос частот и обеспечения возможности одновременной работы спутниковых систем ГСО и НГСО при снижении риска создания вредных помех.
--	--

Источник: МСЭ (без даты); МСЭ 2016, Mercer 2019; Wi-Fi Alliance 2020; Ofcom 2020a; FCC 2020b; FCC 2020c.

Реагирование на изменение спроса на спектр для новых технологий

Примеры, приведенные в предыдущем разделе, показывают, как новые технологии используют новые полосы частот. Однако следует отметить, что эти технологии также несут в себе технические достижения, обеспечивающие возможность более эффективного использования имеющегося спектра. Существуют различные отраслевые решения, и важно понимать предоставляемые ими возможности и их влияние на национальные системы. Один из способов – получение информации в процессе консультаций для анализа того, как осуществляется регулирование присвоения спектра. Это дает отрасли возможность продемонстрировать, что проблемы, связанные с помехами или совместным использованием частот, могут быть решены.

Кроме того, регуляторным органам следует признать необходимость гибких структур, способствующих развертыванию спектра для новых применений. Для максимального использования ограниченных ресурсов спектра и полной реализации потенциальных потребительских преимуществ этих новых технологий, а также для достижения более широких социально-экономических целей с общим прицелом на расширение доступа к соединениям необходимо эффективное управление конкурирующими потребностями в спектре. Совместное использование спектра как для лицензируемых, так и для нелицензируемых применений может способствовать расширению рынка, усилению конкуренции между поставщиками и понижению нагрузки на сети электросвязи (García Zaballos and Foditsch 2015, 21). Эти преимущества расширяют выбор для потребителей и позволяют им использовать новые и более эффективные технологии электросвязи. Важно, чтобы после распределения полос частот регуляторные органы использовали гибкость подходов к регулированию для максимального повышения эффективности конкурирующих услуг в этих полосах.

Управление использованием спектра и стандарты новых технологий

Элементы управления использованием спектра

Управление использованием спектра – важный инструмент, позволяющий органам государственной власти оптимизировать использование ограниченного государственного ресурса. Поскольку потребность в спектре постоянно растет, конкуренция за определенные полосы частот будет еще больше обостряться, а требование эффективного использования этого спектра становится все более важным.

Эффективное управление использованием спектра должно:

- обеспечивать защиту частот, используемых критически важными службами, от вредных помех;
- выявлять возможности для достижения максимальной эффективности;
- обеспечивать возможности для разработки и внедрения новых технологий в гибких рамках; и
- понижать стоимость оборудования электросвязи.

Чтобы идти в ногу с растущим спросом и характером использования спектра, регуляторным органам следует внедрять передовой опыт в области планирования спектра, его технической разработки и выдачи разрешений на его использование. Это означает, что они должны быть в курсе того, каким образом новые и существующие технологии используют спектр. Ключевым аспектом этого процесса является контроль за текущим использованием спектра для определения тех областей, в которых можно добиться повышения эффективности. Контроль за использованием спектра позволяет регуляторным органам обеспечить соблюдение пользователями спектра действующих нормативных актов, выявлять и решать проблемы, связанные с помехами, а также оценивать эффективность использования различных полос частот. Поскольку новые технологии конкурируют с существующими службами по всему спектру, ощущается все большая потребность в применении упреждающего и современного подхода к контролю (Lu et al. 2017). Оценка эффективности использования спектра может вызвать сложности, поскольку относительные преимущества, обеспечиваемые различными службами, бывает трудно сравнить. Государственным органам следует рассмотреть вопрос о повышении эффективности за счет стимулирования пользователей спектра к внедрению более эффективных технологий, а также за счет разрешения совместного использования, аренды или торговли спектром. Например, в 2017 году Управление по развитию информационно-коммуникационных технологий Сингапура (IMDA) потребовало от операторов поэтапного отказа в соответствии с графиком от их сетей 2G в пользу более эффективных технологий подвижной связи (IMDA 2017). Подобные усилия важны для повышения эффективности использования спектра на национальном уровне. Сотрудничество же на международном уровне дает дополнительные преимущества и открывает возможности для повышения эффективности с точки зрения предотвращения помех.

Гармонизация распределений частот на глобальном и региональном уровнях может принести потребителям значительные выгоды, поскольку позволяет производителям выпускать устройства и оборудование в больших масштабах, снижая свои затраты, а потребителям – применять свои устройства в разных странах, эффективно используя роуминг. Долгосрочную стратегию международной гармонизации и сбалансированного распределения спектра между конкурирующими службами определяют решения, принятые на всемирных конференциях радиосвязи (ВКР) Международного союза электросвязи (МСЭ). Для реализации этих решений на национальном уровне и успешного внедрения новых услуг правительства разных стран должны активно интегрировать решения ВКР в национальную нормативно-правовую базу.

Например, итоги ВКР-19 включали несколько важных решений по спектру, в особенности связанных с новыми технологиями, таких как новые распределения частот для NAPS и спутниковых систем НГСО. Конференция также определила дополнительные полосы частот для использования ИМТ в целях содействия развертыванию применений 5G. В рамках подготовки к ВКР-23 проводятся новые исследования, включающие определение новых частот для ИМТ в диапазонах низких и средних частот, а также разработку нескольких предложений по спутниковым сетям НГСО в полосах существующей фиксированной спутниковой службы (ФСС). Эти исследования продолжают усилия в области управления дефицитным спектром, обеспечивающие возможность работы нескольких служб, и могут служить ориентиром для долгосрочного планирования национальных инициатив по управлению использованием спектра.

Роль регуляторного органа в решении вопросов использования спектра на национальном уровне

Важно, чтобы администрации учитывали, как решаются вопросы по использованию спектра в структуре национальных органов власти. В силу технического характера функций управления использованием спектра часто возникает необходимость разработки регуляторных структур и внутренних процедур для оптимизации использования имеющихся ресурсов и повышения их эффективности. Это становится еще более очевидным при поддержке внедрения новых технологий.

Важно создать орган управления или административный орган, обеспечивающий руководство и надзор за осуществлением планирования использования спектра, поскольку долгосрочное планирование почти

всегда является первоочередной задачей на уровне руководства и не может быть делегировано в связи с последствиями и значимостью принимаемых решений (МСЭ 2019а, 4). В большинстве стран функции управления использованием спектра возложены на подразделение соответствующего регуляторного органа или министерства, ответственного за информационно-коммуникационные технологии (ИКТ), и примерно в каждой пятой стране существует отдельный специализированный орган по управлению использованием спектра (ITU 2019d). Также важно четко отделить вопросы спектра от обсуждений контента, особенно в тех случаях, когда вопросами ИКТ, телерадиовещания и СМИ занимаются отдельные подразделения в структуре правительства.

Рисунок 6.2. Орган управления использованием спектра



Источник: ITU 2019d.

Долгосрочное планирование использования спектра создает серьезные трудности для специалистов по управлению использованием спектра, поскольку требует прогнозирования спроса на спектр в далеком будущем, обычно на периоды от 10 до 20 лет. Это подчеркивает важность хорошо отлаженной структуры для обеспечения прозрачности процесса, что приводит к более стабильной нормативно-правовой среде. Это актуально для любой страны, но особенно важно для развивающихся стран, которым необходимо привлекать инвестиции для развития инфраструктуры. Механизмы обеспечения прозрачности могут включать в себя проведение консультаций с общественностью, дорожные карты использования спектра, программы регулирования, доступ общественности к реестру спектра и доступность спектра, а также планы использования спектра для конкретных служб. Например, Управление по связи и средствам массовой информации Австралии (АСМА), национальный регуляторный орган в области ИКТ, регулярно публикует подробные отчеты о консультациях с общественностью по вопросам использования спектра, а также ежегодный пятилетний прогноз использования спектра, в котором излагаются план действий и приоритеты регулирования (АСМА 2019). В целях повышения прозрачности и учета общественного мнения перед официальной публикацией текст отчета публикуется для широкого обсуждения. АСМА также ведет онлайн-отчет о ходе работ, чтобы заинтересованные стороны могли отслеживать выполнение его текущего плана действий (АСМА 2020).

Важность технических стандартов для подвижного широкополосного доступа и других применений

Широкое распространение технологий в глобальном масштабе зависит от наличия устойчивого консенсуса по техническим стандартам. Технические стандарты согласовываются в ходе обсуждений в МСЭ, а также в различных организациях по разработке стандартов (ОРС) электросвязи. Например, Проект партнерства третьего поколения (3GPP) – это группа ассоциаций, которая публикует спецификации технологий

подвижной связи⁶. Регуляторным органам необходимо учитывать работу, проделанную в ОРС, чтобы лучше прогнозировать новые события, которые могут потребовать изменений в их структурах спектра и подготовиться к ним.

Вставка 6.1. Руководящие принципы по ограничению воздействия электромагнитных полей на человека

Еще одним важным аспектом международных стандартов является соблюдение руководящих принципов по ограничению воздействия электромагнитных полей (ЭМП) на человека. Развитие новых технологий, особенно с развертыванием сетей 5G, приводит к уплотнению сетей электросвязи. Развертывается все больше и больше малых сот, поддерживающих сети с высокой пропускной способностью в компактных районах с высокой плотностью населения. К тому же предыдущие издания стандартов для расчета максимально допустимых пределов излучений, на которые часто ссылаются в национальных нормативных актах, не включали полосы частот миллиметрового диапазона.

Для решения этой проблемы Международная комиссия по защите от неионизирующего излучения (МКЗНИ) обновила свои руководящие принципы по ограничению воздействия ЭМП для защиты людей, подвергающихся воздействию радиочастотных электромагнитных полей (РЧ-ЭМП) в диапазоне 100 кГц – 300 ГГц (ICNIRP 2020). По состоянию на июнь 2020 года ни одна из стран официально не приняла новые руководящие принципы, хотя большинство стран мира и почти все страны Азии, Европы и Южной Америки приняли руководящие принципы 1998 года, включив их в национальные нормативные акты по ЭМП (GSMA 2019). Некоторые страны вводят более жесткие пределы, чем те, которые указаны в руководящих принципах МКЗНИ, включая их в национальную нормативную базу. Как отмечается в исследовании МСЭ, в странах и регионах, где ограничения на ЭМП значительно жестче, чем в руководящих принципах МКЗНИ, к 2022 году не будет удовлетворяться до 63% потребностей в трафике мобильных данных. Это подчеркивает необходимость согласования пределов воздействия ЭМП во всем мире (ITU 2019e). Регуляторным органам следует принять во внимание руководящие принципы МКЗНИ и обновить свою национальную нормативно-правовую базу, чтобы соблюдать ограничения при использовании новых технологий, таких как 5G и малые соты.

Источник: GSMA 2019; ICNIRP 2020; ITU 2019e.

Лицензирование спектра на национальном уровне

Спектр – это ограниченный природный ресурс, управление которым и присвоение которого осуществляют национальные администрации с учетом решений, принятых на региональном и международном уровнях. Региональные соглашения могут облегчить процесс лицензирования спектра в определенном районе, особенно для координации возможных трансграничных вопросов. Кроме того, Регламент радиосвязи (PP) МСЭ – это международный договор, регулирующий управление использованием спектра.

Спектр используется для поддержки множества различных применений, включая подвижную, фиксированную, спутниковую, радиовещательную и любительскую службы. Для управления широким кругом различных служб и уменьшения вредных помех регуляторные органы публикуют национальные таблицы распределения частот и устанавливают системы лицензирования, определяющие порядок предоставления спектра в стране. В большинстве случаев спектр лицензируется с помощью одного из механизмов, приведенных на рисунке 6.3.

⁶ <https://www.3gpp.org/about-3gpp>

Рисунок 6.3. Механизмы лицензирования спектра



Индивидуальные лицензии на использование спектра обычно выдаются на основе присвоения спектра административным методом или путем проведения конкурса или аукциона либо применения гибридного подхода, включающего как элементы прямого присвоения, так и элементы аукциона. Спектр для подвижной связи обычно предоставляется по индивидуальной лицензии на использование спектра посредством прямого присвоения, аукциона или применения гибридного подхода.

Лицензии на оборудование обычно выдаются путем прямого присвоения спектра в порядке очереди. Лицензии на оборудование разрешают эксплуатацию отдельного устройства или типа устройств в целях предоставления утвержденных услуг в определенном месте. Они часто используются для фиксированных линий связи пункта с пунктом в полосах с достаточным предложением спектра для удовлетворения спроса различных пользователей. Например, Австралия выдает разрешения на работу фиксированных линий связи в рамках лицензии на оборудование.

Нелицензируемый спектр – это полосы частот, освобожденные от лицензирования, которые обычно используются для работы маломощных устройств малого радиуса действия. Устройства, работающие в нелицензируемых полосах, должны соответствовать определенным техническим условиям, чтобы гарантировать непричинение вредных помех другим пользователям услуг радиосвязи. Нелицензируемые полосы частот позволяют широко применять различные технологии, включая Bluetooth, Wi-Fi и интернет вещей.

Все три типа лицензий играют важную роль в национальных системах лицензирования спектра, а также в концепции технологической нейтральности условий лицензирования. Ключевую роль в поддержке сетей подвижной связи играют лицензии для оборудования фиксированных линий транзитной передачи. Например, Соединенные Штаты ввели упрощенную модель лицензирования для фиксированных линий связи пункта с пунктом. В рамках этой модели Федеральная комиссия по связи (ФКС) выдает неисключительные общенациональные лицензии, применимые в диапазонах 71–76 ГГц, 81–86 ГГц и 92–95 ГГц, после чего лицензиат должен зарегистрировать каждую линию связи через назначенного стороннего администратора базы данных (FCC 2003).

Ввиду общей сложности индивидуального лицензирования спектра по сравнению с другими типами лицензий регуляторные органы часто проявляют осторожность при разработке процессов присвоения, учитывая конъюнктуру рынка и способствуя созданию благоприятной инвестиционной среды. Регуляторные органы стремятся повысить уровень регламентарной определенности и стимулировать инвестиции, выдавая лицензии на более длительный срок. Хотя сроки действия лицензий могут варьироваться в пределах до 25 лет, чаще всего они выдаются на срок от 10 до 20 лет (ITU 2019d). Например, в Соединенном Королевстве предпочтительным подходом считается выдача лицензии на неопределенный срок с указанием начального периода, по истечении которого Управление связи (Ofcom) может отозвать спектр по конкретным причинам, связанным с управлением использованием спектра, уведомив об этом лицензиата (Ofcom 2005). В Колумбии также наблюдается тенденция к более длительным срокам лицензирования: с принятием нового Закона о модернизации ИКТ срок действия лицензий продлен с 10 до 20 лет с возможностью продления еще на один период до 20 лет (закон № 1978 от 25 июля 2019 года, статья 12). Европейским кодексом по электронным средствам связи Европейского союза устанавливается 20-летний срок действия лицензий, хотя некоторые государства-члены по-своему

интерпретировали эти общие указания, выдавая лицензии на 15-летний срок с возможностью продления на пять лет (Директива 2018/1972, статья 49⁷). В Бразилии новые поправки к закону об электросвязи позволяют продлевать лицензии на использование спектра любое количество раз на срок до 20 лет в соответствии с правилами, которые будут определены Национальным агентством электросвязи (Anatel) (закон № 13879 от 3 октября 2019 года, статья 167). В большинстве африканских стран по-прежнему используются лицензии для определенных технологий с фиксированным сроком действия от 10 до 15 лет.

Эти примеры показывают, как регуляторные органы добиваются все большего баланса между обеспечением регламентарной определенности для операторов и некоторой степенью гибкости для регуляторного органа, чтобы приспособиться к конъюнктуре рынка. В приведенных выше примерах операторам гарантируется спектр на определенный период времени, а регуляторные органы сохраняют некоторый контроль и гибкость в отношении продления лицензий. Это позволяет им согласовывать ресурсы спектра с конъюнктурой рынка и обеспечивать наиболее эффективное их использование, оставляя за собой право реорганизовать использование полосы в соответствии с рыночным спросом.

В дополнение к необходимости более длительных сроков действия лицензий в целях повышения регламентарной определенности для операторов регуляторные органы также учитывают затраты на инвестиции и развертывание, которые должны нести операторы в целях совершенствования сетей. Эти затраты в сочетании с другими накладными расходами, такими как плата за использование спектра, могут повлиять на инвестиционную способность операторов. Недавние присвоения с использованием административных, аукционных и гибридных подходов продемонстрировали компромисс между максимизацией доходов от спектра и достижением других политических целей, таких как обеспечение доступа к соединениям для всего населения.

Последние тенденции в области процессов присвоения административными методами

Административные присвоения общеприняты для лицензий для многих видов служб, таких как лицензии на фиксированные линии связи, земные станции сопряжения и другие типы лицензий на оборудование, а также служат подходом к лицензированию спектра для служб подвижной связи. При обычном использовании спектра, например для фиксированных линий транзитной передачи, процесс присвоения, как правило, прост и четко определен. Поскольку большинство регуляторных органов уже выдали такие лицензии, обычно имеются руководящие указания и соответствующие формы заявок, и такие заявки обрабатываются и распределяются по мере поступления. Что касается других типов лицензий, которые запрашиваются не так часто, или лицензий для новых технологий, применяемые системы и процедуры лицензирования могут быть определены не столь четко. Это повышает регламентарную неопределенность для потенциальных подателей заявок при использовании ими новых технологий или бизнес-моделей, поскольку процедура, время обработки заявки и вероятность положительного решения часто бывают неизвестны.

Спектр для оборудования подвижной связи регуляторные органы также предоставляют путем прямого присвоения. В отличие от других служб, присвоение спектра для служб подвижной связи обычно осуществляется не по мере поступления; чаще регуляторный орган собирает заявки, чтобы сразу распределить весь доступный спектр в определенной полосе или его часть. При присвоении спектра многие регуляторные органы руководствуются критериями, согласованными с политическими целями. Если некоторые аукционы спектра для сетей 3G и 4G были основаны на стремлении максимизировать государственные доходы, что приводило к неудачным итогам этих аукционов, то в последнее время страны уделяют основное внимание требованиям к развертыванию сетей, таким как расширение зоны покрытия и обеспечение доступа к более быстрой подвижной широкополосной связи в недостаточно обслуживаемых районах. Высокие ожидаемые затраты на развертывание сетей 5G побудили некоторые регуляторные органы к предложению скидки на спектр или спектра в обмен на инвестиции в сети и обязательства по развертыванию в целях поощрения развития сетей 5G в стране. Недавними примерами стран, принявших этот подход, могут служить Япония и Китай (MIC 2019a; MIC 2019b; GSMA 2020, 44). Другие регуляторные органы, например Гонконг, Китая и Уругвая, подумав о политическом стимулировании развертывания сетей 5G и относительном изобилии спектра 5G, решили предложить или реорганизовать этот спектр без взимания комиссии (OFCA 2019b; URSEC 2019).

При присвоении спектра административным методом регуляторные органы должны четко и прозрачно указывать критерии, процедуру, соответствующие документы и сроки присвоения спектра для какой

⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN>

бы то ни было службы. Для ограниченного числа присвоений, например спектра для предоставления услуг подвижной связи, регуляторные органы должны сделать процесс открытым для новых участников рынка, публикуя правила и делая публичные объявления, избегая закрытых процессов. Как видно из приведенных выше примеров, процессы прямого присвоения позволяют регуляторным органам поощрять стремление к достижению определенных политических целей, таких как развертывание сетей 5G или расширение зоны покрытия в недостаточно обслуживаемых или необслуживаемых районах страны. Такое использование процессов присвоения дает регуляторным органам эффективный инструмент для достижения политических целей. Кроме того, включение в условия лицензий разрешения на торговлю спектром, в том числе для услуг подвижной связи, может помочь сбалансировать спрос на спектр с его предложением, позволяя операторам продавать недоиспользуемый спектр другой стороне, для которой эта лицензия представляет более высокую ценность. Система продажи прав на использование спектра создает стимулы для более эффективного использования спектра лицензиатами (МСЭ 2018а).

Помимо услуг подвижной связи разрабатывается множество новых услуг и новейших технологий, нуждающихся в спектре. Регуляторные органы должны заранее издать руководящие указания по применимым режимам лицензирования, особенно для тех услуг, решение об использовании которых было принято на региональном или международном уровне. При лицензировании новых услуг может потребоваться применение метода проб и ошибок, что подчеркивает важность предоставления временных и экспериментальных лицензий. Регуляторные органы должны открыто общаться с поставщиками новых услуг, чтобы гарантировать, что регулирование не будет невольно препятствовать внедрению инновационных услуг или бизнес-моделей. Кроме того, регуляторные органы могут рассмотреть возможность оптимизации процесса присвоения для определенных применений, где не требуется особой координации и надзора, например при подаче заявок на спектр для высоконаправленной фиксированной линии связи, когда координация легко достигается, а вредные помехи минимальны. Целью облегчения доступа и расширения услуг должно быть короткое время обработки заявок на использование спектра, принимаемых на скользящей основе. Кроме того, для заявок, в которых запрашивается спектр в перегруженном диапазоне, присваиваемый в порядке очереди, полезна публикация информации о наличии соответствующих полос.

Методы управления использованием спектра в чрезвычайных ситуациях

В общем случае регуляторные органы должны быть в курсе различных потребностей в спектре на их рынках и выделить достаточный объем спектра для поддержки применений, обеспечивающих высококачественное соединение и отображение информации, особенно в чрезвычайных ситуациях. Например, в 2020 году несколько регуляторных органов решили вопросы по использованию спектра в ответ на возросший спрос на услуги сетей связи, вызванный требованием оставаться дома в целях борьбы с распространением пандемии COVID-19 во многих странах мира⁸.

Последние тенденции в отношении аукционов и гибридных процессов

Аукционы спектра обеспечивают рыночную оценку спектра и служат обычным средством предоставления спектра. При планировании аукционов регуляторные органы обладают определенной гибкостью, что позволяет им включать конкретные целевые параметры, адаптированные к уникальным политическим целям страны и условиям рынка. При принятии решения о том, какие обязательства включить, регуляторные органы должны рассмотреть возможность проведения публичных консультаций по планируемым правилам аукциона, чтобы гарантировать реалистичные объемы и сроки выполнения таких обязательств и не отбить непреднамеренно охоту участвовать у потенциальных участников торгов. Чтобы привлечь новых участников, можно включить в правила аукциона неодинаковые обязательства со стороны традиционных и новых участников. Точно так же дополнительной мерой поддержки более мелких игроков, в конечном счете способствующей усилению конкуренции на рынке, может служить установление верхнего предела спектра или требований для победителей аукциона предоставить оптовый доступ к спектру. Аукционы, в которых имеются условия типа "используй это или потеряешь", предусматривают разумные обязательства, способствующие предотвращению потенциального накопления и эффективному использованию спектра, хотя регуляторным органам следует должным образом учитывать реалистичные сроки, необходимые операторам для освоения спектра, особенно в случае модернизации или развертывания сети.

⁸ Подборка актуальной информации об этих разнообразных инициативах размещена по адресу <https://reg4covid.itu.int/>.

В самом общем случае аукционы ориентированы на то, что решающим условием получения спектра является готовность оператора заплатить за него. Однако регуляторные органы все чаще планируют аукционы с учетом и других критериев. Для продолжения развертывания сетей 4G, а в последнее время и сетей 5G, многие страны включили в условия лицензий пункты, требующие от лицензиата соблюдения определенных требований по зоне покрытия, темпам развертывания, скорости передачи данных и других требований, предъявляемых к качеству обслуживания или направленных на поддержание конкуренции на рынке.

На нескольких аукционах, в том числе в Германии, Словацкой Республике и Чешской Республике, были приняты меры для улучшения покрытия и повышения качества предоставляемых услуг (BNetzA 2019; RU 2020; STU 2020). Другие общие элементы аукционов, такие как установление верхних пределов спектра, требование к лицензиатам предоставить оптовый доступ к спектру или требование обеспечения роуминга внутри страны, специально направлены на стимулирование конкуренции. Во многие условия лицензирования также включают политику "используй это или потеряешь", которая требует, чтобы спектр начал эксплуатироваться к определенному сроку, чтобы гарантировать его эффективное использование и предотвратить накопление.

В некоторых случаях страны снижают сборы, взимаемые за использование спектра, в обмен на обязательства по покрытию, чтобы способствовать сокращению цифрового разрыва в сельских районах. В Швеции победитель торгов на блок спектра 700 МГц с требованиями к покрытию и развертыванию получил кредит в размере 300 млн. шведских крон для оплаты стоимости спектра в обмен на обязательство выполнить эти требования и повысить качество обслуживания в недостаточно обслуживаемых районах (PTS 2018). В Соединенных Штатах на запланированном аукционе на полосу в диапазоне 3,5 ГГц операторы, предоставляющие услуги преимущественно в сельских районах, имеют право на 15%-ную скидку от цены выигравшей ставки (FCC 2020a). Закон Колумбии о модернизации ИКТ позволяет операторам при развертывании сети производить платежи натурой для покрытия части (до 40%) стоимости лицензий на использование частот (закон № 1978 от 25 июля 2019 года). Победители недавнего аукциона обязались в качестве платежей натурой предоставлять услуги в определенных сельских районах в течение следующих пяти лет (MinTIC 2019; MinTIC 2020).

Гибридные процессы, включающие элементы как прямых присвоений, так и аукционов, также преследуют цели по увеличению зоны покрытия, стимулированию развертывания сетей и обеспечению конкуренции на рынке. Примером гибридного процесса может служить процедура присвоения полосы 3400–3800 МГц во Франции. На первом этапе "прямого присвоения" право на получение одного из четырех блоков по 50 МГц имеют только участники торгов, принявшие на себя дополнительные обязательства⁹. На втором этапе аукциона участники торгов могут делать ставки на дополнительные блоки по 10 МГц в ходе последовательных раундов вплоть до верхнего предела спектра в 100 МГц на оператора. Регуляторный орган также установил минимальный предел в 40 МГц за два этапа аукциона, предположительно чтобы гарантировать всем операторам участок спектра, позволяющий предоставлять услуги 5G. Все победители торгов должны соблюдать обязательства по развертыванию, зоне покрытия и скорости передачи данных 5G, а также обязаны сделать сети подвижной связи совместимыми с IPv6 и использовать сегментацию сети (Агсер 2019).

Независимо от установленных лицензионных обязательств регуляторные органы должны иметь средства для эффективного контроля их соблюдения, то есть обеспечения зоны покрытия и своевременного развертывания, чтобы в конечном счете добиться прогресса в достижении политических целей.

Лицензирование для локальных и частных сетей

В отличие от IMT других поколений возможности сетей 5G часто обсуждаются с точки зрения новых сценариев использования и применений, которые они обеспечивают. В целях эффективного использования спектра некоторые регуляторные органы предлагают спектр для частных сетей нетрадиционным участникам рынка в целях поддержки локализованных применений 5G. Локализованный спектр позволяет операторам адаптировать частные сети в соответствии со своими конкретными потребностями, особенно для применений, в которых требуется высокая точность и короткая задержка. Затраты на развертывание

⁹ К числу дополнительных обязательств относятся меры по стимулированию инноваций путем вынесения индивидуальных решений для субъектов экономической деятельности или присвоения частот на местном уровне, обеспечения покрытия внутри помещений, предоставления услуг фиксированного доступа по сетям подвижной связи, улучшения условий хостинга операторами виртуальных сетей подвижной связи (MVNO) и повышения прозрачности (Агсер 2019).

сети в небольшой локальной зоне намного ниже, и такую сеть можно развернуть гораздо быстрее, чем дожидаться, пока национальный поставщик создаст высококачественную и надежную национальную службу для поддержки своих предполагаемых применений 5G.

Предприятия отрасли заинтересованы в возможностях выделенного спектра для поддержки различных промышленных применений в частных сетях 5G, таких как "умные" фабрики. Выделенный спектр позволяет предприятиям лучше настроить сети в соответствии со своими потребностями и применениями, которые они хотят поддерживать, чем в том случае, если бы им пришлось полагаться на сеть оператора подвижной связи. Например, Германия открыла полосу 100 МГц в диапазоне 3,7–3,8 ГГц для лицензий на локальный спектр для 5G для целей программы "Индустрия 4.0". Локализованные присвоения позволяют намного большему количеству пользователей получить широкую полосу частот в различных районах страны, что означает, что местные пользователи смогут применять до 100 МГц спектра исключительно для удовлетворения собственных частных потребностей (BNetzA 2020). Несколько регуляторных органов уже предоставили спектр для локальных сетей или планируют сделать это в будущем (таблица 6.1).

Таблица 6.1. Примеры лицензирования для локальных и частных сетей

Страна	Полоса	Предполагаемое применение
Германия	3,7–3,8 ГГц (доступна) и 24,25–27,5 ГГц (потенциальная)	Индустрия 4.0, сельское и лесное хозяйство; локализованные применения 5G (промышленность, подвижный широкополосный доступ, фиксированный беспроводной доступ)
Соединенное Королевство	1800 МГц, 2300 МГц, 3,8–4,2 ГГц и 24,25–26,5 ГГц (в порядке очереди)	Частные сети, обеспечение покрытия в сельской местности или внутри помещений, фиксированный беспроводной доступ
Чили	3,75–3,8 ГГц (планируется)	Локальные частные сети
Бразилия	3,7–3,8 ГГц (консультации)	Локальные частные сети
Япония	2575–2595 МГц и 28,2–28,3 ГГц (присвоены)	Локальная частная сеть (используется для системы безопасности с видео высокого разрешения на базе искусственного интеллекта)
Гонконг, Китай	27,95–28,35 ГГц (доступна в порядке очереди)	Предоставление локализованных услуг беспроводной связи в определенных районах площадью не более 50 кв. км
Малайзия	26,5–28,1 ГГц (планируется к присвоению в порядке очереди)	Локализованные/частные сети для предприятий и промышленных служб

Источник: BNetzA 2020; Ofcom 2019; Чили, Резолюция 2400 от 28 ноября 2019 года (<https://www.leychile.cl/Navegar?idNorma=1139171>); Anatel 2020; Fujitsu 2020; OFCA 2019a; MCMC 2019.

Тенденция к локализованному лицензированию связана со сценариями использования, поддерживаемыми технологией 5G, особенно для промышленных применений с небольшой зоной покрытия, в которых требуется высокая пропускная способность и короткая задержка. Такой подход способствует развертыванию промышленных сетей 5G, а общенациональные сети 5G развертываются более размеренными темпами – цель, которую поддерживают многие регуляторные органы. Регуляторные органы выдают эти лицензии в порядке очереди, что согласуется с целями политики по расширению доступа к спектру для быстрого развертывания и внедрения новых применений технологии 5G.

Режимы совместного использования: лицензируемый и нелицензируемый совместный доступ

Режимы совместного доступа могут быть частью лицензируемого или нелицензируемого режимов (см. рисунок 6.4). При лицензируемом совместном доступе (LSA) использование спектра разрешается лицензией для определенного набора различных типов услуг или между пользователями на условиях, определенных в лицензии. Во избежание вредных помех осуществляется управление использованием спектра между службами. Им можно управлять статически, когда при определенных условиях использование спектра запрещено, или динамически, когда условия могут варьироваться с учетом частоты, района или времени использования спектра. Количество пользователей, разрешенное в рамках режима лицензируемого совместного доступа, обычно ограничено, а приоритет пользователей в полосе частот, где пользователи традиционных услуг защищены, определяются условиями использования. При

нелицензируемом режиме лицензия регуляторного органа не требуется и количество пользователей не ограничивается. Однако пользователи, как правило, должны соблюдать технические ограничения (например, ограничения по мощности приемников и передатчиков, максимальные уровни внеполосной передачи и т. д.).

Режимы совместного доступа – один из способов для регуляторных органов открыть спектр для большего числа пользователей и способствовать эффективному использованию полос частот. Нелицензируемые полосы оказались питательной средой для инноваций, о чем свидетельствует важность технологий Wi-Fi и Bluetooth для создания новых приложений и важность Wi-Fi в режимах управления трафиком операторами подвижной связи для его разгрузки. Однако иногда регуляторные органы должны управлять совместным использованием во избежание вредных помех, что делает лицензируемый совместный доступ более привлекательным вариантом для открытия дополнительного спектра при одновременной защите существующих служб.

Рисунок 6.4. Режимы совместного использования спектра



Лицензионные соглашения о совместном доступе

Режимы лицензируемого совместного доступа позволяют извлечь выгоду из технических достижений, таких как базы данных геолокации и зондирования, которые помогают более динамично управлять спектром (OECD 2014, 25).

Структура совместного доступа, предложенная в Соединенных Штатах для диапазона 3,5 ГГц, динамически управляет использованием спектра между традиционными пользователями, лицензиатами с приоритетным доступом и пользователями общего авторизованного доступа. Традиционные пользователи максимально защищены от вредных помех, тогда как обычные пользователи не получают защиты от помех со стороны других пользователей. Для управления использованием спектра между традиционными федеральными и нефедеральными пользователями полосы и гражданскими службами широкополосной радиосвязи, а также для освоения новых применений, включая 5G и IoT (FCC 2020a), принят трехуровневый подход.

Недавняя тенденция в области лицензируемого совместного доступа заключается в локализованном лицензировании спектра подвижной связи ввиду локального характера частных сетей 5G и для обеспечения возможности сосуществования с национальными сетями подвижной связи. Соединенное Королевство и Гонконг (Китай) приняли подход лицензируемого совместного доступа в отношении своих локализованных лицензий (Ofcom 2019; OFCA 2019a). Локализованный совместный доступ применяется и в других форматах. Например, Китай выдал четырем операторам подвижной связи разрешение на совместное использование спектра, но только внутри помещений (MIIT 2020).

Эти соглашения о совместном использовании спектра служат инструментом для регуляторных органов, стремящихся присвоить новым службам спектр в полосах, уже распределенных традиционным службам. При этом подходе также можно использовать спектр, который не использовался или недостаточно использовался традиционными лицензиатами в определенных районах. Регуляторным органам, стремящимся установить лицензируемый совместный доступ в определенных полосах частот, следует определить четкие механизмы совместного использования спектра, обеспечивающие защиту

традиционных пользователей, при этом максимально повысив объем доступного спектра и степень определенности правил его использования для остальных пользователей.

Может быть актуальным как статическое, так и динамическое управление использованием спектра в зависимости от характера использования полосы основным оператором. Затраты на управление использованием спектра для реализации этих решений значительно различаются, и их следует учитывать при принятии решения о лицензионных соглашениях.

Нелицензируемый спектр

Помимо лицензий на исключительное или совместное использование спектра важную роль в структурах управления использованием спектра играет и нелицензируемый спектр. Некоторые приложения и применения, включая Bluetooth, Wi-Fi, радиочастотную идентификацию (RFID), промышленное, научное и медицинское (ПНМ) оборудование и другие устройства малого радиуса действия, работают в нелицензируемых полосах частот. Учитывая, что приложения Wi-Fi и IoT часто работают в нелицензируемых полосах, ожидается, что такие полосы сохранят свою важную роль и в будущем. Многие страны открыли некоторые полосы для безлицензионного использования, признавая их существенные преимущества и широкий спектр приложений, которые в них работают.

Малая нормативная нагрузка на эти полосы частот способствует инновациям. Особую важность безлицензионному использованию придает та роль, которую технология Wi-Fi играет в разгрузке трафика подвижной сети, а также ожидаемый рост использования IoT и числа приложений IoT в сетях 5G. Соединенное Королевство и Соединенные Штаты предоставили дополнительные полосы для безлицензионного использования спектра в диапазонах 6 ГГц и выше 100 ГГц (Ofcom 2020a; Ofcom 2020b; FCC 2020b; FCC 2019b) или рассматривают такую возможность. Другие страны рассматривают безлицензионное использование спектра как возможное решение задачи обеспечения широкополосной связи в сельской местности. Например, Аргентина провела консультации по предложению разрешить безлицензионное использование спектра на вторичной основе в сельских районах с населением менее 100 тыс. человек (Resolution 21/2019¹⁰). Некоторые другие страны, такие как Кения, рассмотрели возможность обеспечения для широкополосной связи в сельских районах сегментов неиспользуемых каналов телевизионного вещания, называемых белыми пространствами телевидения¹¹.

Регуляторным органам следует учитывать роль нелицензируемого спектра и возможность высвобождения дополнительного спектра на безлицензионной основе в определенных диапазонах для поддержки будущих сетей и приложений. Они должны осуществить процедуры надлежащего исполнения, чтобы обеспечить сосуществование с другими пользователями и предложить четкие руководящие указания и рабочие параметры безлицензионного использования во избежание вредных помех.

Торговля спектром и его аренда

Концепция торговли спектром и его аренды предполагает наличие вторичного рынка спектра, где лицензированным операторам разрешается торговать присвоенными им правами на использование спектра. Торговля спектром на вторичном рынке разрешена примерно в каждой третьей стране, главным образом в Европе (ITU 2019d).

Новые бизнес-модели и инновации в использовании спектра

Совместное использование активной инфраструктуры: совместные сети

Все больше операторов, особенно операторов подвижных сетей, объединяются с конкурентами, чтобы разделить затраты на инфраструктуру и инвестиции. Эта тенденция вызвана необходимостью уплотнения сетей в городских центрах, а также выполнения обязательств по обеспечению покрытия в менее населенных районах. Совместное использование инфраструктуры, широко применяемое в сетях 3G и 4G, особенно важно для снижения затрат на развертывание сетей 5G. Хотя сотрудничество чаще всего касается пассивной инфраструктуры, есть несколько примеров совместного использования активной инфраструктуры, включая ресурсы спектра. В Швеции операторы Tele2 и Telenor договорились развернуть совместную общенациональную сеть для предоставления услуг 5G и совместного использования спектра,

¹⁰ <https://www.boletinoficial.gob.ar/detalleAviso/primera/221017/20191111>

¹¹ <https://ca.go.ke/public-consultation-on-the-draft-dynamic-spectrum-access-framework-for-authorisation-of-the-use-of-tv-white-spaces/>

включая две полосы по 10 МГц в диапазоне 700 МГц, через свое совместное предприятие Net4Mobility. Эти два оператора уже сотрудничали в прошлом при развертывании и эксплуатации общенациональной сети 2G и 4G и возобновили свое соглашение, чтобы быстро построить совместную сеть 5G (Tele2 2018). К другим примерам совместного использования ресурсов спектра относятся соглашения о сетях радиодоступа (RAN), когда операторы соглашались совместно использовать свои соответствующие сети на определенных условиях. Соглашения о совместном использовании спектра заключили операторы подвижной связи во Франции, Финляндии, Дании и Польше, хотя эти соглашения часто дополняются условиями, определяющими географическую зону и/или временные рамки такого совместного использования (BEREC 2018, 10–11).

Такие механизмы совместного использования ресурсов позволяют операторам разделить бремя инвестиций в сети и сократить время, необходимое для развертывания общенациональных сетей. Многие регуляторные органы являются сторонниками мер, поощряющих развертывание сетей и инвестиции, которые соответствуют целям моделей совместного использования спектра. Однако эта модель несет в себе потенциальные риски для конкуренции, зависящие от условий соглашений о совместном использовании спектра, масштабов совместной деятельности и конкурентоспособности рынка. Однако регуляторный надзор обеспечивает возможность управления этими рисками. Например, может быть разрешено совместное использование спектра только на определенный период времени или до тех пор, пока не будет высвобожден достаточный спектр, чтобы не допустить развертывания всего одной национальной сети в определенном районе и поощрять резервирование сетей и конкуренцию на рынке. Могут быть приняты и другие меры, чтобы стороны не действовали как единая организация и не достигали доминирующего положения на рынке, возвышаясь над конкурентами. Регуляторные органы могут рассмотреть возможность разрешения совместного использования активной инфраструктуры для стимулирования ускоренного развертывания сетей и распределения бремени инвестиций между операторами.

Нарезка сети

Помимо новых тенденций в области лицензирования спектра регуляторными органами более эффективному использованию спектра способствуют новые типы инноваций. Например, нарезка сети, являющаяся одной из форм виртуализации сети, которая стала возможной благодаря сетям с программируемыми параметрами и виртуализации сетевых функций, позволяет обслуживать несколько сетей обслуживания, или сегментов, с помощью одной и той же физической инфраструктуры (OECD 2019, 28–29). Это дает операторам возможность предоставлять различные типы услуг в каждом сегменте сети с учетом необходимых характеристик этих услуг, таких как задержка, скорость передачи данных, безопасность или надежность.

По мере перехода операторов подвижной связи с сетей 4G на сети 5G нарезка сети может помочь им эффективно использовать свой спектр и сети для удовлетворения потребностей в обслуживании, поддерживая все больше приложений 5G с высокой нагрузкой по передаче данных. Ожидается, что после полного развертывания сетей 5G нарезка сети будет иметь наибольшее влияние, когда будут внедрены различные сценарии использования 5G и станет возможным ее широкомасштабное применение.

Перепрофилирование спектра и реорганизация его использования

В целях максимально эффективного использования спектра и, следовательно, лучшего удовлетворения спроса на него регуляторные органы принимают административные, финансовые и технические меры для возврата спектра и его перераспределения для новых применений. Концепция перепрофилирования спектра и реорганизации его использования не нова, но она приобретает все большую актуальность, поскольку страны стремятся сделать доступным больше спектра для удовлетворения потребностей в нем со стороны новых услуг и технологий. При таком подходе учитывается спектр, используемый как для существующих технологий подвижной связи, так и для других служб. Основная идея заключается в оптимизации использования одного и того же спектра путем перехода от старых технологий (например, 2G) к новым (например, 4G или 5G). Так, сети 4G примерно в 15–30 раз лучше оптимизированы в отношении использования спектра, чем сети 2G, и могут работать в диапазонах, изначально предназначавшихся для сетей 2G, таких как диапазоны 850 МГц, 900 МГц и 1800 МГц.

Общий принцип, который может применяться ко всем типам лицензий, – это принцип технологической нейтральности. Он облегчает переход от одной технологии к другой и устраняет регуляторные препятствия.

Одна из важных целей перепрофилирования связана с переходом телевизионного вещания с аналоговой передачи сигнала на цифровую, что позволяет предоставлять услуги телевидения повышенного качества при более экономном использовании спектра. Многие директивные органы направили высвобожденный спектр аналогового телевидения, называемый цифровым дивидендом, для предоставления услуг широкополосной подвижной связи. Фактически цифровой дивиденд стал основным стимулом перехода на цифровое телевизионное вещание во всем мире – около двух третей стран уже перераспределили этот спектр сотовым сетям подвижной связи (ITU 2019d).

6.4 Основные выводы

Ниже приведены основные выводы этого обзора передового опыта в области применений и регуляторных аспектов, определяющих использование спектра в будущем.

- В контексте постоянного технического прогресса эффективная политика в области использования спектра должна быть достаточно гибкой, чтобы способствовать развертыванию самых разнообразных служб. Регуляторным органам при рассмотрении национальных планов по управлению использованием спектра в будущем следует принимать во внимание новые технологии и применения. Для того чтобы справиться с растущим спросом на трафик данных, необходимо эффективное управление конкурирующими потребностями в спектре. Оно позволит полностью реализовать потенциальные потребительские преимущества новых технологий, а также решать более широкие социально-экономические задачи, преследуя общую цель улучшения и расширения доступа к соединениям.
- Администрации должны тщательно оценить важность управления использованием спектра, чтобы определить, как осуществлять его в рамках государственной структуры. Важно иметь хорошо отлаженную структуру для обеспечения прозрачности процесса, что приводит к более стабильной нормативной среде.
- В дополнение к необходимости в более длительных сроках действия лицензий в целях повышения регламентарной определенности для операторов регуляторные органы также должны учитывать затраты операторов на инвестиции и развертывание, которые они должны нести для совершенствования сетей, поскольку плата за использование спектра может повлиять на инвестиционные возможности операторов. Регуляторным органам также следует рассмотреть возможность оптимизации процесса присвоения спектра для определенных применений, требующих незначительной координации и надзора, чтобы облегчить доступ и расширить распространение услуг в стране. Размещение информации с актуальным реестром диапазонов частот и присвоений спектра различным службам также облегчит доступ к полосам частот.
- Существует тенденция к локализованному лицензированию, связанная со сценариями использования, поддерживаемыми технологией 5G, особенно для промышленных применений с небольшой зоной покрытия, в которых требуется высокая пропускная способность и короткая задержка. Такой подход способствует развертыванию промышленных сетей 5G, а общенациональные сети 5G развертываются более размеренными темпами.
- Режимы совместного доступа позволяют регуляторным органам открыть для новых пользователей спектр, который в настоящее время используется традиционными службами. Нелицензируемые полосы частот оказались питательной средой для инноваций, о чем свидетельствует важность технологий Wi-Fi и Bluetooth для создания новых приложений.
- Общий принцип, который должен применяться ко всем типам лицензий, – это принцип технологической нейтральности. Многие регуляторные органы приняли этот подход для стимулирования инноваций и снижения нормативных ограничений.
- Наконец, регуляторные органы должны провести обзор международного передового опыта в отношении лицензирования спектра. Сюда относится соблюдение международных и региональных решений о распределении частот и международных технических стандартов, обеспечивающих максимальную согласованность. Это способствует снижению затрат на оборудование и эффективному обеспечению роуминга.

Справочные документы

- ACMA (Australian Communications and Media Authority). 2020. *FYSO 2019–23: Progress Report for July–Dec 2019*. April 24, 2020. Canberra: ACMA. <https://www.acma.gov.au/fyso-2019-23-progress-report-july-dec-2019>
- ACMA (Australian Communications and Media Authority). 2019. *Five-Year Spectrum Outlook 2019–23: The ACMA'S Spectrum Management Work Program*. Canberra: ACMA. <https://www.acma.gov.au/publications/2019-09/publication/five-year-spectrum-outlook-2019-23>
- Anatel (National Agency of Telecommunications). 2020. *Public Consultation No. 9*. <https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2308&Tipo=1&Opcao=andamento>
- Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). 2019. "5G: 3.4-3.8 GHz Band Frequency Awards Procedure: Arcep Invites all Players Wanting to Participate to Submit a Bid Package." Press Release. December 31, 2019. <https://en.arcep.fr/news/press-releases/p/n/5g-10.html>
- Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). 2020. "5G: The Companies Bouygues Telecom, Free Mobile, Orange and SFR Have all Qualified to Participate in the Auction for 3.4 – 3.8 GHz Band Frequencies. The Auctions Have Been Postponed Due to the Current Health Crisis." Press Release. April 2, 2020. <https://en.arcep.fr/news/press-releases/p/n/5g-13.html>
- BEREC (Body of European Regulators for Electronic Communications). 2018. *BEREC Report on Infrastructure Sharing*. Brussels: BEREC. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/8164-berec-report-on-infrastructure-sharing_0.pdf
- BNetzA (Bundesnetzagentur). 2019. "Frequency auction 2019." https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html?nn=268128
- BNetzA (Bundesnetzagentur). 2020. "Regional and Local Networks." https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/LokaleNetze/lokalenetze-node.html
- CTU (Czech Telecommunications Office). 2020. *Call for Comments on Draft Invitation to Tender for the Award of Rights to Use Radio Frequencies for the Provision of Electronic Communications Networks in the 700 MHz and 3 440-3 600 MHz Frequency Bands*. <https://www.ctu.cz/vyzva-k-uplatneni-pripominek-k-navrhu-textu-vyhlase-ni-vyberoveho-rizeni-za-ucelem-udeleni-prav-k-7>
- FCC (Federal Communications Commission). 2003. *Allocations and Service Rules for the 71-76 GHz, 81-86 GHz and 92-95 GHz Bands*. Report and Order: FCC-03-248. <https://docs.fcc.gov/public/attachments/FCC-03-248A1.pdf>
- FCC (Federal Communications Commission). 2019a. *Amendment of Part 15 Rules for Unlicensed White Spaces Devices*. Report and Order: FCC 19-24. Washington, DC: FCC. <https://www.fcc.gov/document/amendment-part-15-rules-unlicensed-white-spaces-devices>
- FCC (Federal Communications Commission). 2019b. *FCC Opens Spectrum Horizons for New Services and Technologies*. Report and Order: FCC 19-19. Washington, DC: FCC. <https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies-0>
- FCC (Federal Communications Commission). 2020a. "FCC Establishes Procedures for 3.5 GHz Band Auction." Public Notice. <https://www.fcc.gov/document/fcc-establishes-procedures-35-ghz-band-auction-0>
- FCC (Federal Communications Commission). 2020b. *Unlicensed Use of the 6 GHz Band*. Report and Order: FCC-CIRC2004-01. Washington, DC: FCC. <https://docs.fcc.gov/public/attachments/DOC-363490A1.pdf>
- FCC (Federal Communications Commission). 2020c. "FCC Adopts New Rules for the 6 GHz Band, Unleashing 1,200 Megahertz of Spectrum for Unlicensed Use." Press Release. April 23, 2020. <https://docs.fcc.gov/public/attachments/DOC-363945A1.pdf>

- Fujitsu. 2020. "Fujitsu Launches Japan's First Commercial Private 5G Network." Press Release, March 27, 2020. <https://www.fujitsu.com/global/about/resources/news/press-releases/2020/0327-01.html>
- García Zaballos, A. and N. Foditsch. 2015. *Spectrum Management: The Key Lever for Achieving Universality*. New York: Inter-American Development. <https://publications.iadb.org/publications/english/document/Spectrum-Management-The-Key-Lever-for-Achieving-Universality.pdf>
- GSMA. 2019. "EMF Policy." <https://www.gsma.com/publicpolicy/consumer-affairs/emf-and-health/emf-policy>
- GSMA. 2020. *The Mobile Economy China*. London, United Kingdom: GSMA. <https://www.gsma.com/mobileeconomy/china/>
- ICNIRP (International Commission on Non-Ionizing Radiation Protection). 2020. "Guidelines for limiting exposure to electromagnetic fields (100 kHz to 300 GHz)". *Health Physics* 118(5):483-524. <https://doi.org/10.1097/HP.0000000000001210>
- IMDA (Infocomm Media Development Authority). 2017. "2G Services to Cease on April 1, 2017." Press Release. March 27, 2017. <https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2017/2g-services-to-cess-on-1-april-2017>
- МСЭ (Международный союз электросвязи), без даты. *HAPS-системы на высотных платформах*. <https://www.itu.int/ru/mediacentre/backgrounders/Pages/High-altitude-platform-systems.aspx>
- МСЭ (Международный союз электросвязи). 2008. *Добавление к Справочнику по контролю использования спектра*. Женева: МСЭ. <https://www.itu.int/pub/R-HDB-53>
- МСЭ (Международный союз электросвязи). 2011. *Справочник по контролю за использованием спектра*. Женева: МСЭ. <https://www.itu.int/pub/R-HDB-23>
- МСЭ (Международный союз электросвязи). 2015a. *Справочник по компьютерным технологиям управления использованием спектра (КТ)*. Женева: МСЭ. <https://www.itu.int/pub/R-HDB-01>
- МСЭ (Международный союз электросвязи). 2015b. *Справочник по управлению использованием спектра на национальном уровне*. Женева: МСЭ. <https://www.itu.int/pub/R-HDB-21>
- МСЭ (Международный союз электросвязи). 2016. *Регламент радиосвязи*. Женева: МСЭ. <https://www.itu.int/pub/R-ACT-WRC.14-2019/ru>
- МСЭ (Международный союз электросвязи). 2018a. *Экономические аспекты управления использованием спектра*. Отчет МСЭ-R SM.2012-6. Женева: МСЭ. <https://www.itu.int/pub/R-REP-SM.2012>
- ITU (International Telecommunication Union). 2018b. *Guidance on the Regulatory Framework for National Spectrum Management*. Report ITU-R SM.2093-3. Geneva: ITU. <https://www.itu.int/pub/R-REP-SM.2093>
- МСЭ (Международный союз электросвязи). 2019a. *Методы определения долгосрочных национальных стратегий использования спектра*. Отчет МСЭ-R SM.2015. Женева: МСЭ. <https://www.itu.int/pub/R-REP-SM.2015>
- МСЭ (Международный союз электросвязи). 2019b. *Развитие методов контроля за использованием спектра*. Отчет МСЭ-R SM.2355-1. Женева: МСЭ. <https://www.itu.int/pub/R-REP-SM.2355>
- ITU (International Telecommunication Union). 2019c. *The State of Broadband: Broadband as a Foundation for Sustainable Development*. Geneva: ITU. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf
- ITU (International Telecommunication Union). 2019d. *World Telecommunication/ICT Regulatory Survey*. Geneva, Switzerland: ITU. <https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx>
- ITU (International Telecommunication Union). 2019e. *The Impact of RF-EMF Exposure Limits Stricter than the ICNIRP or IEEE Guidelines on 4G and 5G Mobile Network Deployment*. Recommendation ITU-T K. Series Supplement 14. Geneva: ITU. <https://www.itu.int/rec/T-REC-K.Sup14-201909-I>
- Lu, Q., J. Yang, Z. Jin, D. Chen, and M. Huang. 2017. "State of the Art and Challenges of Radio Spectrum Monitoring in China." *Radio Science* 52(10): 1261-1267. <https://agupubs.onlinelibrary.wiley.com/doi/full/10.1002/2017RS006409>

- MCMC (Malaysian Communications and Multimedia Commission). 2019. *Allocation of Spectrum Bands for Mobile Broadband Service in Malaysia: Final Report*. https://www.skmm.gov.my/skmmgovmy/media/General/pdf/FINAL-REPORT_ALLOCATION-OF-SPECTRUM-BANDS-FOR-MOBILE-BROADBAND-SERVICE-IN-MALAYSIA_20191231.pdf
- Mercer, D. 2019. *Global Connected and IoT Device Forecast Update*. Strategy Analytics. <https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update>
- MIC (Ministry of Internal Affairs and Communications). 2019a. *Approval of a Plan to Open a Specific Base Station for the Introduction of a 5th Generation Mobile Communication System (5G) (Summary)*. https://www.soumu.go.jp/main_content/000613734.pdf
- MIC (Ministry of Internal Affairs and Communications). 2019b. *Certification of Plan to Open Specific Base Station for Introduction of 5th Generation Mobile Communication System*. https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000378.html
- MIIT (Ministry of Industry and Information Technology). 2020. "The Ministry of Industry and Information Technology Permits China Telecom, China Unicom, and China Radio and Television to Jointly Use the Indoor Frequency of the 5G System." Press Release, February 10, 2020. <http://www.miit.gov.cn/n1146290/n1146402/c7671201/content.html>
- MinTIC (Ministry of Information and Communications Technology). 2019. "Statement: Results of the Radio Spectrum Auction." Press Release, December 20, 2019. <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/124713:Comunicado-Resultados-de-la-Subasta-del-Espectro-Radioelectrico>
- MinTIC (Ministry of Information and Communications Technology). 2020. "MinTIC Issued the Resolutions that Assign the Permits to Use the Spectrum Blocks." Press Release, February 20, 2020. <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/125966:MinTIC-expidio-las-resoluciones-que-asignan-los-permisos-de-uso-de-los-bloques-de-espectro>
- OECD (Organisation of Economic Cooperation and Development). 2014. *New Approaches to Spectrum Management*. OECD Digital Economy Papers, No. 235. Paris: OECD. <https://dx.doi.org/10.1787/5jz44fnq066c-en>
- OECD (Organisation of Economic Cooperation and Development). 2019. *The Road to 5G Networks*. OECD Digital Economy Papers, No. 284. Paris: OECD. <https://doi.org/10.1787/2f880843-en>
- OFCA (Office of the Communications Authority). 2019a. *Guidelines for Submission of Applications for Assignment of Shared Spectrum in the 26 GHz and 28 GHz Bands*. Hong Kong: OFCA. <https://www.coms-auth.hk/filemanager/statement/en/upload/515/gn132019.pdf>
- OFCA (Office of the Communications Authority). 2019b. "Offer of Spectrum Assignments in the 26 GHz and 28 GHz Bands for Provision of 5G Services." Press Release, March 27, 2019. https://www.ofca.gov.hk/en/media_focus/press_releases/index_id_1891.html
- Ofcom (Office of Communications). 2005. *Spectrum Framework Review: Implementation Plan – Interim Statement*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/38162/statement.pdf
- Ofcom (Office of Communications). 2019. *Enabling Wireless Innovation through Local Licensing: Shared Access to Spectrum Supporting Mobile Technology*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0033/157884/enabling-wireless-innovation-through-local-licensing.pdf
- Ofcom (Office of Communications). 2020a. *Improving Spectrum Access for Wi-Fi: Spectrum use in the 5 and 6 GHz Bands*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0038/189848/consultation-spectrum-access-wifi.pdf
- Ofcom (Office of Communications). 2020b. *Supporting Innovation in the 100-200 GHz Range: Proposals to Increase Access to Extremely High Frequency (EHF) Spectrum*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0034/189871/100-ghz-consultation.pdf
- PTS (Post and Telecom Authority). 2018. *Decision on Permission to Use Radio Transmitters in the 700 MHz Band*. https://pts.se/globalassets/startpage/dokument/legala-dokument/beslut/2018/radio/700-tilldelningsbeslut/tilldelningsbeslut-700-mhz-14-december-2018389611-0_tmp.pdf

- RU (Regulatory Authority for Electronic Communications and Postal Services). 2020. *Call for Tenders for Granting Individual Licenses for the Use of Frequencies*. https://www.teleoff.gov.sk/data/files/49605_call-for-tender.pdf
- Tele2. 2018. "Tele2 and Telenor Secure New Frequencies and Consolidate Joint Plan for 5G Network in Sweden." Press Release. December 10, 2018. <https://www.tele2.com/media/press-releases/2018/tele2-and-telenor-secure-new-frequencies-and-consolidate-joint-plan-for-5g-network-in-sweden>
- URSEC (Unidad Reguladora de Servicios de Comunicaciones). 2019. *Resolution No. 034/2019*. https://www.gub.uy/unidad-reguladora-servicios-comunicaciones/sites/unidad-reguladora-servicios-comunicaciones/files/2019-05/034%20.%20ANTEL%20Tecnolog%C3%AD%205G_0.pdf
- Wi-Fi Alliance. 2020. *20 Years of Wi-Fi*. April 17. <https://www.wi-fi.org/discover-wi-fi/20-years-of-wi-fi>

Глава 7. Реагирование регуляторных органов на развитие технологий



7.1 Введение

В процессе цифровизации общества и экономики непрерывно создаются рекордные объемы данных. Движущей силой цифровизации является расширение масштабов и повышение скорости соединений между людьми и вещами. Волоконные линии до жилого помещения (FTTx) и высокоскоростные сети подвижной связи дают возможность участвовать в цифровой деятельности, а социальные сети и создаваемый пользователями контент являются источником мотивации для этого. В то же время все больше предметов становятся "умными", то есть подключаются к интернету для приема и отправки данных. Стремительный рост объема данных привел к появлению новых технологий, помогающих сортировать данные и извлекать выгоду из обобщения и анализа больших массивов данных. Для описания этих технологий часто используются такие обобщающие понятия, как искусственный интеллект (ИИ) и большие данные.

Развитие новых технологий требует от регуляторных органов ИКТ пересмотра инструментов, которые они используют для содействия добросовестной конкуренции в секторе ИКТ и защиты прав потребителей. Развитие новых технологий также порождает проблемы правового, этического и макроэкономического характера. Центральные банки, ведомства по защите прав потребителей, комиссии по вопросам конкуренции и регуляторные органы ИКТ спешно пытаются оценить последствия для своих сфер ответственности. Эти последствия состоят в том, что функции регуляторных органов конкретных секторов (сектор ИКТ, водоснабжение, электроэнергетика и банковские услуги), а также регуляторных органов, занимающихся конкретными вопросами (ведомство по защите прав потребителей или комиссия по вопросам конкуренции), возможно, понадобится изменить, а в некоторых случаях, возможно, придется создавать более узкоспециализированные регуляторные органы.

На рисунке 7.1 показано, как функциональные регуляторные органы, сфера ответственности которых охватывает все секторы экономики, дополняют деятельность отраслевого регуляторного органа ИКТ.

Рисунок 7.1. Экосистема цифрового регулирования



В этой главе рассматривается общая тенденция к пересмотру функций различных регуляторных органов в ответ на появление облачных вычислений, ИИ, технологии блокчейн, больших данных и интернета вещей (IoT). Желаемые конечные результаты – добросовестная конкуренция, защита прав потребителей и экономическое развитие – остаются неизменными, однако способы их достижения изменяются со временем и отличаются друг от друга в разных странах. Цель этой главы – предложить базовую модель определения соответствующего подхода к регулированию в ответ на возникновение новых технологий. В следующем разделе рассматриваются отдельные технологии в контексте цепочки создания стоимости в интернете и эволюции бизнес-моделей в секторе ИКТ. В последнем разделе рассматриваются динамика изменения регуляторной среды и варианты распределения регуляторных полномочий между отраслевыми и/или функциональными регуляторными органами.

7.2 Эволюция технологий

Общей чертой технологий блокчейн, ИИ, больших данных, облачных хранилищ и IoT является то, что все они так или иначе предполагают работу с данными и способствуют созданию новых бизнес-моделей, которые могут смещать создание стоимости как внутри сегментов цепочки создания стоимости, так и между ними. Устройства IoT получают данные (зондирование и сбор), облачные технологии обеспечивают хранение и обработку данных, технологии больших данных формируют новые данные путем обобщения крупных массивов данных, ИИ использует данные, в том числе большие данные, для обучения, а блокчейн представляет собой механизм надежного сбора хронологических данных о транзакциях распределенным способом (см. рисунок 7.2).

Рисунок 7.2. Связи между технологиями, рассматриваемыми в этой главе



Разница между этими технологиями заключается в том, что на IoT распространяются нормы регулирования сектора ИКТ, а на остальные технологии в настоящее время – нет. Хотя приложения, созданные на основе этих технологий, могут относиться к сфере ответственности регуляторных органов ИКТ или регуляторных органов, занимающихся конкретными вопросами, например защитой данных или защитой прав потребителей, а также структур, отвечающих за кибербезопасность, на сами технологии сфера ответственности этих органов не распространяется. Например, в криптовалютах используется технология блокчейн, однако в регуляторном плане ответственность лежит на центральных банках.

Облачные вычисления

Облачные вычисления превращают инфраструктуру ИТ и программное обеспечение в услуги, предоставляемые с помощью общедоступного интернета, включая серверы, хранилища, сети, программное обеспечение и анализ данных. Облачные вычисления позволяют компаниям увеличивать и уменьшать масштабы доступных им возможностей в области вычислений и создания сетей в течение нескольких минут. В сфере облачных вычислений действуют поставщики, предлагающие хранение в качестве услуги, такие как Dropbox и iCloud, а также компании, специализирующиеся на передаче файлов, например WeTransfer. Облачную инфраструктуру используют все потоковые сервисы, такие как Netflix и YouTube, а также приложения для социальных сетей, такие как TikTok и Facebook.

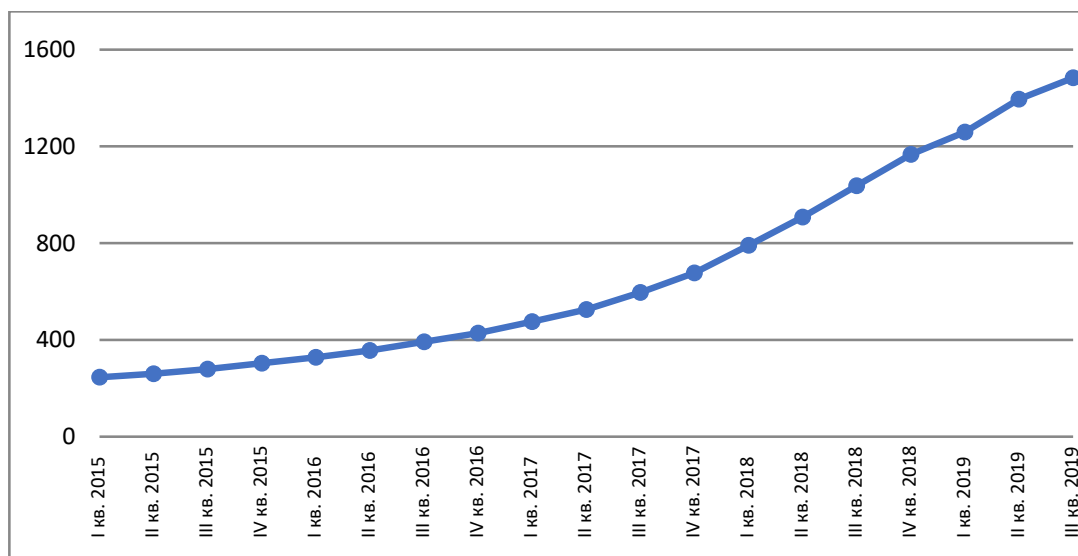
Согласно определению Международного союза электросвязи (ITU 2018b), облачные вычисления – это "парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу".

В некотором смысле вычислительная обработка данных прошла полный круг. Началом ее стали централизованные вычисления с использованием универсальных ЭВМ и "немых" терминалов, на смену которым пришли персонализированные вычисления при помощи персональных компьютеров (ПК) и ноутбуков, а в настоящее время произошел возврат к централизованной инфраструктуре (облачные вычисления) с использованием "умных" терминалов и устройств, в том числе смартфонов и планшетов. Облачные вычисления являются частью цепочки создания стоимости в интернете, а регуляторные аспекты связаны преимущественно с защитой данных и защитой прав потребителей в различных юрисдикциях.

Интернет вещей

IoT – это собирательное понятие, охватывающее технологии, которые позволяют объектам взаимодействовать между собой. Ofcom определяет IoT как соединение через интернет вычислительных устройств, встроенных в предметы быта, что позволяет им передавать и получать данные¹. IoT включает технологии связи на малом расстоянии, такие как пассивная радиочастотная идентификация (RFID) и связь ближнего действия (NFC), а также технологии, обеспечивающие связь на больших расстояниях, например межмашинное взаимодействие (M2M). Для идентификации и аутентификации в сетях подвижной связи M2M использует стандартные карты модуля идентификации абонента (SIM-карты). На рисунке 7.3 показано, сколько SIM-карт сейчас используется в мире для установления соединений в сфере IoT. По оценке компании Ericsson, содержащейся в ее отчете Mobility Report (Ericsson 2019), к 2025 году число устройств, подключенных к IoT, достигнет 25 миллиардов.

Рисунок 7.3. Лицензированные сотовые соединения IoT в мире (млн.)



Источник: GSMA Intelligence.

Цепочка создания стоимости IoT короче цепочки создания стоимости в интернете и состоит из трех-четырех звеньев (BEREC 2016).

- **Поставщик услуг IoT** – компания, которая включает IoT в свои продукты или услуги, например производитель автомобилей или поставщик электроэнергии.
- **Поставщиком услуг установления соединения для IoT** может являться оператор подвижной связи или поставщик услуг интернета (ПУИ), чье интернет-соединение используется при помощи Wi-Fi устройств, таких как Alexa от Amazon или Apple Watch.
- **Пользователь IoT** приобретает продукт или услугу со встроенным IoT. Продукты и услуги можно комбинировать или приобретать по отдельности. Производитель автомобилей может предоставлять бесплатную услугу слежения на определенный период времени или на весь срок службы автомобиля, а может взимать за нее отдельную плату.

¹ Определение понятия "интернет вещей": <https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/internet-of-things>. В Рекомендации МСЭ-T Y.2060 приводится обзор интернета вещей (IoT) и его более подробное определение: интернет вещей (IoT) определяется как "глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий. ПРИМЕЧАНИЕ 1. – Благодаря задействованию возможностей идентификации, сбора, обработки и передачи данных, в IoT обеспечивается наиболее эффективное использование вещей для предоставления услуг для всех типов приложений при одновременном выполнении требований безопасности и неприкосновенности частной жизни. ПРИМЕЧАНИЕ 2. – В широком смысле IoT можно воспринимать как концепцию, имеющую технологические и социальные последствия" (<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>).

К использованию IoT предъявляется ряд регуляторных требований.

- Использование спектра для IoT нуждается в регулировании. Помимо использования SIM-карт устройства IoT могут обмениваться данными на разных частотах с использованием технологий Wi-Fi, NFC или RFID. Например, NFC может использовать частоты в диапазоне от 300 МГц до 3 ГГц. RFID может использоваться в низкочастотном диапазоне 125–134 кГц или 13 МГц (ITU 2016).
- Вопросы, касающиеся конкуренции, возникают вследствие "привязки" клиентов из-за установки в устройства SIM-карт определенного оператора. Затраты на обеспечение переносимости номеров в части изменения поставщиков подвижной связи для устройств IoT могут оказаться непомерно высокими. BEREC (2016) считает, что существующие нормы в отношении переносимости номеров могут быть неподходящими и что необходима разработка новых гибких подходов.
- Защита данных имеет первостепенное значение для IoT. Кому принадлежат созданные данные и каковы юридические обязательства владельца данных в отношении использования и хранения данных, а также ответственности за их утечку?
- Для внедрения IoT с использованием SIM-карт может потребоваться решение проблемы роуминга. Устройствам IoT (например, автомобилям со встроенными устройствами отслеживания) может потребоваться постоянный роуминг в нескольких юрисдикциях. Вопрос заключается в том, применяются ли правила, касающиеся роуминга, к устройствам IoT. Например, если речь идет о Европейском союзе (ЕС), должен ли распространяться на устройства IoT принцип "в роуминге как дома"?
- BEREC (2016) утверждает, что внезапный многократный рост числа соединений в роуминге может привести к проблемам с доступом.

Проблемы, связанные с адресацией и нумерацией, могут быть решены путем введения в оборот eSIM-карт, которые идентифицируют устройства по международному идентификатору абонентов подвижной связи (IMSI) и позволяют переключаться между поставщиками в режиме онлайн. GSMA разработала стандарт для eSIM².

eSIM откроет новые возможности в оптовом сегменте, в том числе для компаний, чей бизнес не связан с установлением соединений. Частные сети, например, на горнодобывающих предприятиях или в портах, могут иметь собственные eSIM, что позволит повысить уровень безопасности конкретных приложений и контролировать использование ими данных. Гостиничные сети и больницы могли бы предоставлять своим клиентам или пациентам eSIM с установленным лимитом передачи данных. Поставщики услуг IoT могут предлагать свои продукты с включенными данными, а клиенты могут без труда пополнять счет в онлайн-режиме или менять поставщика на время отпуска или при переезде в другой город.

Большие данные

Большие данные можно в целом определить как извлечение ценности из объединения крупных массивов данных. Большие данные – это сочетание различных источников данных и данных с различными характеристиками. В материале UNSTATS (2015) описаны характеристики данных с точки зрения объема, скорости, разнообразия, количества переменных, достоверности, избирательности, структуры и частоты (в привязке к событиям или непрерывно во времени). Большие данные часто описываются с использованием следующих характеристик (ITU 2014).

- **Объем:** крупные массивы данных могут поступать из большого количества источников, таких как записи об адресатах вызова (CDR) звонков с мобильных телефонов и интеллектуальных устройств (IoT).
- **Скорость:** это понятие относится к скорости генерации данных. Информация о прошедшем проверке годовом финансовом отчете обновляется через 12 месяцев. Фиксация сведений о продажах определенного товара в супермаркетах может происходить много тысяч раз в день.
- **Разнообразие:** данные поступают в различных форматах и видах. Они могут представлять собой структурированные данные фондовых бирж или неструктурированные данные, полученные из текстовых документов, электронных писем, видеофайлов, аудиозаписей и т. д.

² Встроенная SIM-карта или встроенная универсальная карта с интегральной схемой (eUICC). <https://www.gsma.com/iot/embedded-sim/>

- **Достоверность:** под достоверностью подразумевается качество данных, при этом надежность некоторых данных выше, а других – ниже. Примером достоверности данных является разница между опросами общественного мнения и результатами выборов: достоверность последних выше.
- **Ценность:** данные обладают "внутренней ценностью", которая раскрывается только после ее выявления и использования.

Таблица 7.1. Источники больших данных

Виды данных	Примеры
Административные данные	Административные данные – это данные, сбором которых занимается государство, например сведения о налоговых платежах, свидетельствах о рождении, номерах социального страхования и взносах в фонды социального страхования
Данные обследований	В течение года государство проводит ряд обследований, некоторые из них – в рамках циклов продолжительностью пять или десять лет. В качестве примеров можно привести переписи населения, обследования рабочей силы, обследования в сфере здравоохранения и многоцелевые обследования домашних хозяйств
Данные, предоставляемые с высокой периодичностью	Частный сектор осуществляет сбор широкого спектра данных, предоставляемых с высокой периодичностью. К ним относятся: • CDR от операторов подвижной связи • покупки в супермаркетах и онлайнные покупки • банковские операции и транзакции с использованием кредитных карт • операции на фондовых и товарных биржах • дорожные датчики и детекторы транспортного потока • метеостанции • отслеживающие устройства GPS • поиск в интернете, активность в социальных сетях и просмотр страниц
Неструктурированные данные	Примерами неструктурированных данных являются текстовые документы, видеофайлы, рисунки Блоги и сообщения, а также другой авторский и неавторский контент в онлайнной среде
Геопространственные данные со спутников	Инфракрасные изображения, например, для оценки численности населения

Большие данные могут использоваться для оценки показателей ИКТ в рамках мониторинга достижения целевых показателей развития в секторе ИКТ. Также их могут использовать операторы сетей подвижной связи (MNO) для сокращения оттока клиентов, оптимизации сетей и повышения эффективности поддержки клиентов.

- К офисным инструментам сокращения оттока клиентов относятся прогнозирование оттока и персонализированные пакеты пополнения баланса и поощрений. Привлечение нового клиента дороже удержания существующего. Большие данные могут помочь в выявлении клиентов, готовых уйти, и разработать продукты/услуги, отвечающие их конкретным потребностям, за счет сочетания информации об использовании клиентом услуг, жалобах, операциях, социальных сетях и сегментации клиентов (Deloitte 2015).
- Оптимизация сети: операционные расходы – один из значимых компонентов затрат операторов. Модернизация до уровня 5G может потребовать также увеличения количества базовых станций, и управление сетью усложнится. В структуре затрат компании MTN в Нигерии почти 52% приходится на обслуживание сети и инфраструктуры. Аналитику больших данных можно использовать для повышения качества функционирования сетей путем сравнения данных в режиме реального времени с ретроспективными данными (MapR 2020).
- Операторы подвижной связи по всему миру используют чат-боты для поддержки клиентов. Чат-боты могут повысить качество обслуживания клиентов.

Поскольку большие данные представляют собой сочетание различных массивов данных, возрастает вероятность того, что полученные данные могут идентифицировать отдельных лиц. Кроме того, с различными массивами данных могут сопрягаться различные уровни согласия и обязательств для владельцев данных, в силу чего возрастает потребность в строгих законах о защите данных.

Блокчейн

Блокчейн представляет собой технологию выстраивания записей, именуемых блоками, в определенную последовательность с использованием криптографии. Каждая запись содержит набор информационных материалов, включая отметку времени действия, список участников операции и два уникальных идентификационных кода, называемых хеш-кодом. Запись содержит хеш предыдущей записи, а также хеш текущей записи, формируя таким образом цепочку (см. рисунок 7.4). Это вид распределенного реестра, который состоит из записанных в цифровой форме данных, организованных в виде последовательно растущей цепочки блоков, каждый из которых криптографически связан и защищен от несанкционированного доступа и изменения (ITU 2019a). Этот распределенный процесс верификации делает блокчейны устойчивыми и практически полностью исключает возможность несанкционированного доступа, поскольку единой точки отказа не существует. Более того, по мере добавления в цепочку следующих блоков внести изменения становится все сложнее.

Существует важное различие между частными и публичными блокчейнами. Публичный блокчейн также называют открытым или общедоступным; он позволяет любому присоединиться к сети в качестве узлового компьютера и сохранить локальную копию реестра (Michels 2018). В отличие от него в частном блокчейне (с эксклюзивным доступом) обработка данных доступна только для ограниченной группы узловых компьютеров.

Технология блокчейн не подлежит никакому регулированию, как не подлежат регулированию защищенный протокол передачи гипертекста (HTTPS) или 3D-печать. Блокчейн – это технология, которая может использоваться для приложений, применяющихся в широком спектре секторов и имеющих различные свойства и функциональные возможности. В зависимости от сектора и особенностей использования технологии блокчейн могут потребоваться нормативные меры реагирования.

Рисунок 7.4. Блокчейн



Так, например, биткоин представляет собой децентрализованную цифровую валюту, использующую технологию блокчейн. Его использование создает проблемы с точки зрения предотвращения отмывания денег и мошенничества. Поскольку реестр распределен по компьютерным сетям по всему миру, остановка финансовых операций и/или их проверка только в пределах одной юрисдикции представляется затруднительной. В связи с этим важную роль играет сотрудничество между различными юрисдикциями.

Биткоин стал первым примером использования технологии блокчейн в сфере криптовалют. С тех пор было запущено в обращение много других криптовалют, однако тестируются и не относящиеся к валюте приложения. В отчете МСЭ (ITU 2019b) о распределенных реестрах было обобщено более 50 вариантов использования технологии блокчейн, включая приложения в секторе ИКТ. К последним примерам использования технологии блокчейн в секторе ИКТ относятся:

- Регуляторный орган электросвязи Индии (TRAI 2018) требует использования технологии блокчейн в сфере электросвязи при создании реестра "не беспокоить", предназначенного для предотвращения спама. В этом нормативном акте TRAI ссылается на технологию распределенного реестра (DLT), а блокчейн является одним из видов DLT;

- Управление определением идентичности и данными: технология блокчейн может использоваться для поддержания доверия и безопасности среди миллиардов датчиков, которые будут подключены к сети (например, "умные" холодильники, маршрутизаторы Wi-Fi, "умные" часы и т. д.);
- Ofcom проводит тестирование технологии блокчейн для управления стационарными телефонными номерами в Соединенном Королевстве³. Тестирование проводится в целях совершенствования процесса переносимости номеров. Управление владением номером и маршрутизацию голосовых звонков можно осуществлять путем фиксации сторон переноса номера и изменения времени в записи (или блоке);
- Альянс ID2020⁴ направляет усилия на разработку новой глобальной модели проектирования, финансирования и внедрения решений и технологий цифровой идентичности. В этих целях проводится изучение технологии блокчейн, а также биометрии⁵;
- компания Deloitte выпустила отчет (Deloitte 2016), в котором перечислены основанные на технологии блокчейн бизнес-возможности для операторов подвижной связи и ПУИ. Одним из вариантов применения является хранение данных о качестве работы сети на уровне сот в блокчейне для анализа эффективности работы сети.

Хотя применительно к каждому приложению на основе технологии блокчейн у регуляторных органов возникают различные поводы для беспокойства, некоторые вопросы, такие как защита данных, касаются большинства приложений на основе этой технологии. Публичные блокчейны позволяют каждому видеть всю историю операций, что может иметь последствия для защиты данных в зависимости от того, какая информация содержится в блоках. В связи с частными блокчейнами возникают вопросы, касающиеся владения данными и обязанностей владельцев данных⁶.

Для некоторых приложений может потребоваться отраслевое регулирование. Центральные банки несут ответственность за криптовалюты, и им будет необходимо обеспечить соблюдение положений о противодействии отмыванию денег.

Примером необходимости вмешательства со стороны регуляторного органа ИКТ может быть ситуация, связанная со злоупотреблением оператором своим положением на рынке, когда он, пользуясь своим влиянием на рынке, устанавливает высокие цены на услуги, оказываемые с использованием сочетания цифровых ID, eSIM и счетов мобильных денег на основе технологии блокчейн. Акцент необходимо сделать на злоупотреблении положением на рынке. В существующем законодательстве и подзаконных актах уже присутствует запрет на злоупотребление положением на рынке для доминирующих операторов. В этом случае инструменты для вмешательства на рынке уже существуют, и их не нужно изобретать заново.

Искусственный интеллект

Согласно определению Общества Интернета (Internet Society 2017), ИИ – это "искусственно созданный интеллект, напоминающий интеллект человека, который способен к обучению, рассуждению, планированию, восприятию или обработке естественного языка". Он относится к системам, созданным для имитации человеческих способностей к пониманию и решению проблем. Существует множество вариантов применения ИИ, включая профилактическое техническое обслуживание автомобилей и чат-боты для поддержки клиентов.

МСЭ (ITU 2018a) отмечает, что ИИ включает пять "технологий": компьютерное зрение, обработку естественного языка, глубокое обучение, робототехнику и другие системы автоматизации. Ограничения на развертывание ИИ связаны с получением достаточно больших массивов данных, способностью объяснять и обобщать результаты, полученные от систем ИИ, и риском систематической ошибки (ITU 2018a).

Инструменты ИИ – это то, что позволяет обрабатывать большие данные. Таким образом, регуляторные требования к ИИ и к большим данным тесно взаимосвязаны. Однако может потребоваться дополнительное регулирование в связи с риском систематической ошибки, которая может быть обусловлена используемыми

³ Ofcom, How Blockchain Technology Could Help to Manage U.K. Telephone Numbers. <https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/blockchain-technology-uk-telephone-numbers>

⁴ <https://id2020.org/alliance>

⁵ ID2020: Digital Identity with Blockchain and Biometrics. <https://www.accenture.com/us-en/insight-blockchain-id2020>

⁶ Более подробные сведения о регламентарных последствиях использования конкретных приложений на основе технологии блокчейн содержатся в отчете МСЭ (ITU 2019b).

данными и алгоритмами (McKinsey 2018). Могут потребоваться дополнительные шаги для устранения рисков систематической ошибки, выходящих за рамки данных и алгоритмов.

Существует определенный риск, что при отборе собранных данных была допущена ошибка выборки или что они отражают социальные предубеждения, таким образом закрепляя их в системе. Известным примером является алгоритм коррекционного профилирования правонарушителей для определения альтернативных наказаний (COMPAS) в США, который прогнозировал, что среди чернокожих правонарушителей вероятность повторного совершения правонарушений на 77% выше по сравнению с белыми при сходстве всех прочих факторов⁷. Зная о существующей в обществе предвзятости, этого можно было бы избежать, исключив расу как одну из переменных, используемых в алгоритме обучения. Но еще более важно, каким образом была обнаружена эта систематическая ошибка. Для этого потребовалась организация, которая была обеспокоена результатами, и механизм запроса исходных данных (запрос был подан на основании норм о свободе информации). Со временем, по мере усложнения алгоритмов, обнаруживать систематические ошибки будет все труднее.

Регуляторным органам необходимо рассмотреть способы решения проблемы "черного ящика", когда алгоритмы принимают решения или дают рекомендации, а затронутые ими люди не имеют возможности понять, на чем основываются эти решения и рекомендации (Deloitte 2018b). Для решения этих проблем в ЕС в рамках официального информационного документа были сформулированы семь ключевых требований к регулированию ИИ, в число которых вошли недопущение дискриминации и справедливость (European Commission 2020).

Статья 22 Общего регламента по защите данных (GDPR) Европейского союза дает потребителю "право не подпадать под действие такого решения, основанного исключительно на автоматизированной обработке, включая профилирование, которое порождает правовые последствия в отношении него или подобным образом существенно воздействует на него"⁸. Это означает, что каждый потребитель имеет право знать, какие данные и соображения лежали в основе принятия решения, если это было автоматизированное решение. Например, если потребителю было отказано в выдаче кредита на основании автоматизированного профилирования, он может запросить у банка обоснование решения.

Однако применение средств защиты данных и ИИ создает целый ряд проблем. В ЕС GDPR предписывает компаниям, осуществляющим обработку данных, использовать минимальный набор данных, необходимых для принятия решения. ЕС пытается установить ограничения на объем используемых данных и ограничить вмешательство в частную жизнь. Это сложнее, чем кажется, поскольку ЕС не определил, какие именно данные составляют необходимый минимум. В то же время в других юрисдикциях такое ограничение отсутствует, в связи с чем компании могут использовать столько данных, сколько сочтут нужным, что может поставить компании из ЕС в невыгодное положение и ограничить инновационную деятельность в сфере ИИ.

Аналогичным образом, каждый гражданин ЕС имеет право ознакомиться с исходными данными до профилирования, а также с полученными после профилирования результатами (статья 15 GDPR). Недобросовестные компании могут получить доступ к результатам профилирования и попытаться раскрыть алгоритмы, использованные проводившей исходную работу компанией. Эти проблемы указывают на необходимость проделать большую работу по усовершенствованию традиционных инструментов регулирования в целях решения сложных проблем, связанных с использованием таких технологий, как ИИ, и их влиянием на такие аспекты, как защита данных.

В общем смысле основной вопрос для ЕС и регуляторных органов заключается в том, может ли существующая система защиты данных формировать доверие между поставщиками и потребителями и поддерживать его. Более строгие правила могут создать невыгодные конкурентные условия на одном уровне, однако формирующееся доверие может помочь в достижении конкурентных преимуществ на другом уровне.

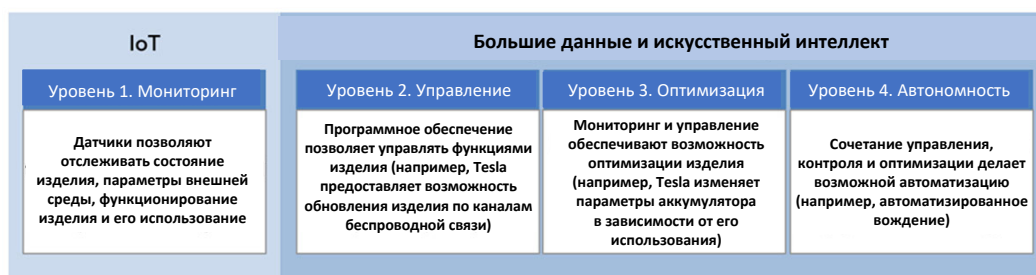
⁷ How We Analyzed the COMPAS Recidivism Algorithm. <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>

⁸ <https://gdpr-info.eu/art-22-gdpr/>

"Умные" функциональные возможности и защита данных

Такие технологии, как IoT, ИИ и большие данные, позволяют развивать новые возможности для продуктов и услуг. На рисунке 7.5 датчики IoT отслеживают использование изделия, направляя полученные данные производителю для дальнейшей обработки в целях обновления или усовершенствования изделия. Производители могут в известной мере управлять характеристиками изделия. Например, компания Tesla может изменить емкость аккумуляторной батареи автомобиля путем обновления программного обеспечения, как это было сделано для водителей, пострадавших от урагана "Ирма" в 2017 году (Liptak 2017). Сочетание управления и мониторинга означает возможность улучшения или оптимизации производительности изделия. Мониторинг, управление и оптимизация обеспечивают автоматизацию, которая зависит от степени обучаемости искусственного интеллекта.

Рисунок 7.5. Подход, ориентированный на наращивание функциональных возможностей



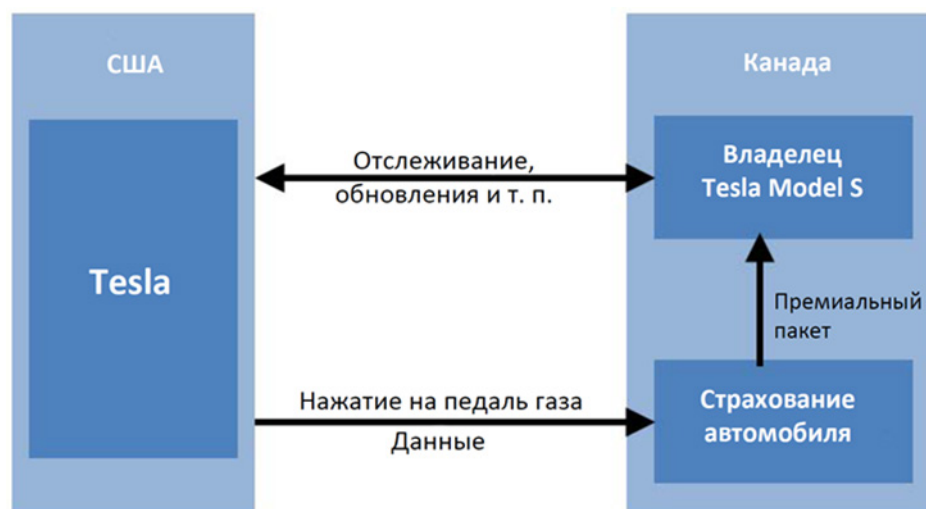
Источник: подготовлено на основе Porter 2014.

"Умные" функциональные возможности продуктов и услуг формируют новые модели сотрудничества, в рамках которых придется искать решение ряда различных, иногда противоречащих друг другу задач, заключающихся в защите неприкосновенности частной жизни отдельных лиц при одновременном использовании преимуществ трансграничного и межотраслевого обмена знаниями.

Уже осуществляются инициативы, направленные на развитие сотрудничества во всех звеньях цепочки создания стоимости. Поставщики услуг электросвязи и финансовых услуг сотрудничают в вопросах регулирования сферы мобильных денег. Также примером может служить недавнее объявление корпораций Google и Apple о будущей совместной деятельности в области разработки технологии отслеживания контактов на основе Bluetooth с открытым исходным кодом в связи с пандемией COVID-19, которая потребует сотрудничества между органами здравоохранения, регуляторными органами ИКТ, ведомствами по защите данных и правительствами.

Перемещение данных из одной юрисдикции в другую влечет последствия для защиты этих данных и обмена ими. Возьмем, например, такую автомобильную компанию, как Tesla, которая продает свои автомобили только онлайн, минуя традиционную сеть автомобильных дилеров. Как только автомобиль доставлен покупателю, Tesla может отслеживать состояние автомобиля, а автомобиль может либо активировать удаленный вызов Tesla для планирования ремонта, либо направить уведомление владельцу. Нетрудно представить сценарий, при котором данные об использовании могут собираться в целях предоставления владельцам индивидуально подобранных продуктов. Внимательная и спокойная манера управления автомобилем может быть вознаграждена большими скидками на автострахование. Резкое нажатие водителем на педаль газа может привести к увеличению страховых взносов из-за повышенного риска аварии (см. рисунок 7.6).

Рисунок 7.6. Пример, иллюстрирующий продажу Tesla за границу и использование данных третьими лицами



В рамках этого сценария последствия для защиты данных и обеспечения неприкосновенности частной жизни, возникающие в целом ряде различных сегментов цепочки создания стоимости, требуют сотрудничества между различными регуляторными органами. Каким образом следует защитить данные, если они собираются с использованием сетей подвижной связи (находящихся под надзором регуляторных органов ИКТ), совместно используются страховыми компаниями (находящимися под надзором регуляторного органа финансовых услуг) и производителями автомобилей (находящимися под контролем регуляторных органов сферы транспорта и безопасности)? Какими средствами правовой защиты обладают потребители, если они не хотят, чтобы данные об использовании ими автомобиля передавались третьим лицам, например страховым компаниям? Сложность ситуации многократно возрастает в том случае, если гражданин Канады заказывает автомобиль Tesla онлайн в Соединенных Штатах.

Защита данных как объединяющий фактор

Применение технологий ИИ, больших данных и IoT обуславливает для регуляторных органов необходимость рассмотрения пяти вопросов (Deloitte 2018b).

- Кому принадлежат собираемые данные?
- Каковы обязательства владельца данных в отношении хранения и защиты этих данных?
- Могут ли организации, занимающиеся сбором данных, устанавливать дифференцированные цены для пользователей, согласных с тем, что их данные могут быть использованы, и для тех, кто не дал своего согласия на это?
- Имеют ли граждане право не подвергаться оценке с использованием алгоритмов?
- Могут ли граждане запрашивать доступ к данным, которые использовались для принятия решения или вынесения рекомендаций, которые их затрагивают?

По сути, в вопросе о защите данных речь идет о неприкосновенности частной жизни⁹. Во многих странах право на неприкосновенность частной жизни считается одним из основных прав человека. Что еще более важно, фактическое или предполагаемое отсутствие конфиденциальности приводит к тому, что потребители отказываются от приобретения новых устройств (например, "умных" носимых устройств, таких как "умные" часы) и в целом склонны избегать рисков. Компания Accenture (Accenture 2016) установила, что 47% потребителей выражали обеспокоенность в отношении конфиденциальности и безопасности, в связи с чем отказывались от приобретения "умных" устройств. Уверенность потребителей в том, что их персональные данные принадлежат им и они могут контролировать их использование, является необходимым условием формирования доверия потребителей к операциям в онлайн-овой

⁹ Анализ нормативно-правовых аспектов защиты данных см. в главе 5 "Защита данных и доверие".

среде. Когда дело касается защиты данных, необходимо в первую очередь придерживаться следующих важнейших принципов, сформулированных в какой-либо форме.

- Определение персональной информации должно быть составлено таким образом, чтобы к ней относилась любая информация об идентифицируемом живом физическом лице.
- Организации¹⁰ должны нести ответственность за собираемую ими персональную информацию.
- Организации обязаны указать, в каких целях они будут использовать персональную информацию, и подтвердить оправданность такого использования.
- Организации должны использовать только необходимую для них персональную информацию, а не ту, которую они захотят.
- Потребители¹¹ должны знать, какие организации собирают их персональную информацию и когда это происходит, и должны давать свое согласие на последующие действия организаций с этими данными.
- Организации должны принять разумные меры для обеспечения безопасности персональной информации, а в случае нарушения безопасности они должны информировать об этом потребителей и принять меры для ограничения ущерба.
- Организации должны делать все возможное, чтобы персональная информация, право на использование которой им было предоставлено, была хорошего качества.
- Определенные виды персональной информации, например биометрическая информация и персональные данные детей, являются конфиденциальными и требуют принятия дополнительных мер защиты.

В состав экосистемы защиты данных входят законы, учреждения и отраслевые и потребительские форумы. В таблице 7.2 представлена рамочная основа оценки экосистемы защиты данных в стране. Любые вопросы, на которые дан отрицательный ответ, дают возможность улучшить эту рамочную основу.

Как особо отмечено в контрольном списке вопросов, касающихся защиты данных, наличие соответствующего законодательства является необходимым, но недостаточным условием. Осуществление законодательства и нормативных положений по защите данных требует финансирования как для ведения информационно-разъяснительной работы, так и для обеспечения соблюдения законодательства в области защиты данных. Для развивающихся стран это представляет серьезную проблему. Экономические и социальные преимущества, которые могут принести новые технологии, основаны на уверенности потребителей в том, что их данные защищены и что они в определенной мере контролируют уровень их защиты.

¹⁰ Сбор данных могут осуществлять организации и физические лица. С юридической точки зрения организации/частные лица, занимающиеся сбором данных, являются контролерами данных. Понятие "контролер данных" используется в GDPR ЕС, в котором оно определяется как "физическое лицо, компания или другой орган, который определяет цели и способы обработки персональных данных (самостоятельно или совместно с другими лицами/компаниями/органами)" (<https://www.atinternet.com/en/glossary/data-controller/>).

¹¹ С юридической точки зрения потребитель является "субъектом данных". Понятие "субъект данных" используется в GDPR ЕС, в котором оно определяется как "любое физическое лицо, которое можно прямо или косвенно идентифицировать посредством идентификатора, такого как имя, идентификационный номер, данные о местоположении, или с использованием факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица. Другими словами, субъект данных – это конечный пользователь, персональные данные которого могут быть собраны" (<https://www.atinternet.com/en/glossary/data-subject/>).

Таблица 7.2. Экосистема защиты данных

Контрольный список вопросов, касающихся защиты данных			Да	Нет
Существует ли в вашей стране закон о защите данных?				
Закон о защите данных	Персональные данные	Включает ли определение персональной информации все аспекты? Включены ли персональные данные организаций? Включены ли персональные данные умерших?		
	Подотчетность	Понятно ли, кто является контролерами данных и за что они несут ответственность?		
	Цель	Согласуются ли списки приемлемых целей с таковыми в других странах?		
	Минимальность	Обязаны ли организации (или контролеры данных) использовать только необходимую им персональную информацию?		
	Уведомление/открытость	Информируют ли потребителей (субъектов данных) об использовании их персональных данных и предоставляется ли им возможность отказаться от такого использования? Какова процедура уведомления в случае нарушения безопасности?		
	Безопасность	Относится ли безопасность к стандартным требованиям и существует ли объяснение повторяющегося цикла безопасности?		
	Качество	Должна ли у организаций (контролеров данных) существовать стратегия обеспечения высокого качества данных?		
	Конфиденциальные персональные данные	Принимаются ли повышенные меры предосторожности при обращении с конфиденциальными персональными данными?		
	Орган по обеспечению защиты данных	Существует ли специальный независимый орган, которому поручено обеспечивать защиту данных, и обладает ли он достаточным уровнем финансирования и потенциалом?		
	Международное сотрудничество	Предусмотрена ли в законе необходимость сотрудничества с международными органами по защите данных?		
	Прямой маркетинг	Регламентирует ли закон прямой маркетинг, не останавливая его полностью?		
	Кодексы поведения	Существуют ли механизмы для работы с компаниями отрасли и заинтересованными группами гражданского общества, позволяющие им осуществлять саморегулирование при необходимости?		
Позволяют ли нормы закона о защите данных регулировать способы использования данных в рамках развивающихся технологий?				
Обладает ли регуляторный орган достаточным опытом и уровнем финансирования для ведения разъяснительной работы и обеспечения соблюдения закона о защите данных?				
Обладает ли регуляторный орган достаточными юрисдикционными полномочиями и возможностями в области международного сотрудничества для работы в нескольких странах с различными регуляторными органами?				
Существует ли механизм подачи запросов на основании положений о свободе информации?				

7.3 Развитие цепочки создания стоимости в интернете

Облачные вычисления, ИИ, аналитика больших данных и технология блокчейн — все это части цепочки создания стоимости в интернете. В 2010 году компания Kearney¹² провела анализ цепочки создания стоимости в интернете, а в 2016 году это исследование было обновлено по заказу GSMA¹³. В рамках этого исследования было выделено пять сегментов производственно-сбытовой цепочки в интернете (GSMA 2016a). Для этого Справочника цепочка создания стоимости в интернете была расширена за счет включения спроса на цифровые услуги, включая доступ в интернет. В настоящее время цепочка создания стоимости в интернете рассматривается не как традиционный набор последовательных компонентов, а как самоусиливающийся цикл (см. рисунок 7.7).

Рисунок 7.7. Цикл создания стоимости в интернете



К этим шести компонентам относятся:

- **права на контент.** Охватывают исключительные права на контент, созданный профессиональными поставщиками контента. Сюда также входит пользовательский контент, доступ к которому осуществляется через социальные сети, в том числе YouTube, Twitter, Instagram, Vimeo и Facebook;
- **онлайн-услуги.** Охватывают широкий спектр услуг, предоставляемых через интернет, включая электронную розничную торговлю, развлечения (игры, азартные игры, видео, музыку, публикации), услуги поиска и справочно-информационные услуги (Википедия, Google, Yahoo), социальные сети и облачные услуги;
- **вспомогательные технологии.** Включают основные услуги, обеспечивающие бесперебойное функционирование интернета, такие как дизайн и хостинг веб-сайтов, платежные платформы (кредитные карты, PayPal, MPESA), платформы, обеспечивающие услуги на базе межмашинного (M2M) взаимодействия, рекламные площадки (рекламные биржи и брокеры);
- **установление соединений.** Сегмент установления соединений можно подразделить на первую, среднюю, последнюю и невидимую мили. Первая миля относится к международным соединениям, то есть к тому, каким образом страна подключается к остальному миру с использованием интернета. Средняя миля охватывает установление соединений на национальном уровне, включая волоконные сети и центры обмена данными. Последняя миля представляет собой беспроводной или проводной

¹² Internet value chain economics. <https://www.kearney.com/communications-media-technology/article?/a/internet-value-chain-economics>

¹³ https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf

канал связи для обеспечения доступа конечного пользователя. Невидимая миля охватывает регуляторные и законодательные аспекты, оказывающие влияние на сектор ИКТ;

- **пользовательский интерфейс.** К устройствам, которые конечные пользователи используют для доступа в интернет, относятся смартфоны и обычные мобильные телефоны, ПК, ноутбуки и планшетные компьютеры, а также цифровые телевизоры или цифровые абонентские приставки. Операционное программное обеспечение (ПО) для этих устройств также относится к этому сегменту, как и приложения, работающие поверх операционного ПО;
- **использование цифровых услуг.** Спрос на цифровые услуги, помимо располагаемого дохода и возможности установления соединения, зависит от навыков пользователя, привлекательности контента и функциональности;

Ранее поток данных шел от владельцев контента к конечному пользователю через общедоступный интернет. Сегодня пользователи создают контент, используя приложения социальных сетей и другие способы загрузки данных, тем самым внося свой вклад в потребляемый контент.

Цепочка создания стоимости в интернете объединяет в рамках одной платформы различные, ранее не связанные между собой отрасли, причем не только внутри страны, но и во всем мире. Можно привести несколько примеров.

- Телефония начиналась с голосовых вызовов, затем к ним добавились текстовые сообщения, а сегодня можно осуществлять видеозвонки через общедоступный интернет.
- Приобретение товаров начиналось "у ворот фермы", затем переместилось на местные рынки, а сегодня происходит на онлайн-торговых площадках.
- Шоу и спектакли сначала шли на сцене, затем их стало возможно увидеть на телевидении и DVD, а сегодня они доступны в виде контента по запросу.
- Степень автоматизации регистрации данных неуклонно растет с развитием мобильных приложений и онлайн-сервисов.

Традиционно у телевизионного и кинематографического контента существовал собственный канал доставки. Сегодня интернет представляет собой единую платформу предоставления контента. Бизнес-модель вещания остается прежней, основанной на подписках или рекламе, в то время как способ доставки все в большей степени смещается на IP-платформу. Такое смещение предоставляет преимущества потребителям, которые теперь могут решать, что, когда и где смотреть, вместо того чтобы планировать свое время отдыха в зависимости от программы передач телерадиовещательных компаний.

Облачные вычисления, большие данные, блокчейн и ИИ предоставляют возможность создания стоимости на основе самоусиливающегося цикла создания стоимости в интернете. Эти технологии могут создавать профили пользователей на основании потребляемого и создаваемого ими контента, позволяя онлайн-сервисам предлагать индивидуально подобранные услуги. Способность предоставлять целевой контент, услуги и рекламу открывает возможности для персонализированного опыта использования, а также новых услуг и новых бизнес-моделей. Это применимо также к сегменту установления соединений в цепочке создания стоимости, в частности для операторов фиксированной и подвижной связи, рассмотрению деятельности которых посвящен следующий раздел.

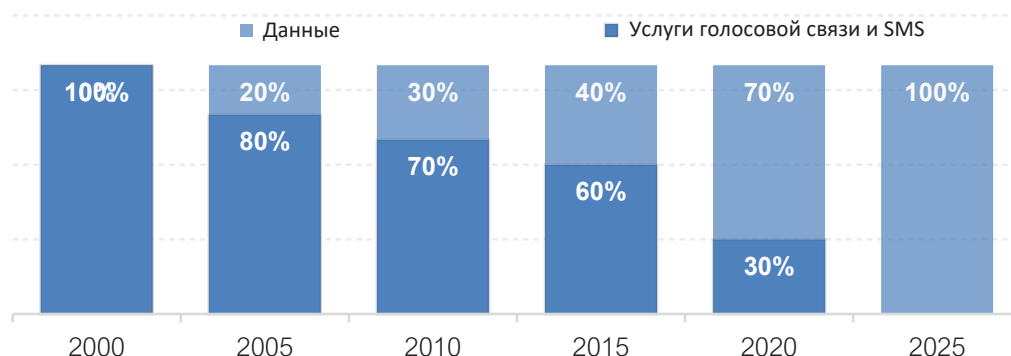
7.4 Эволюция бизнес-моделей в секторе ИКТ

Растущая цифровизация нашей работы и жизни влияет и на наше общение. Вместо традиционных голосовых вызовов и отправки SMS-сообщений длиной в 160 символов люди могут общаться более удобным для них образом, с полноценным видео или в группах с использованием интернет-приложений. Услуги, которые ранее предоставляли операторы сетей подвижной связи (MNO), теперь сталкиваются с конкуренцией со стороны общедоступного интернета. Голосовым вызовам и SMS приходится конкурировать с приложениями over-the-top (OTT), такими как Skype, WhatsApp и Facebook Messenger. Криптовалюты, основанные на технологии блокчейн, могут конкурировать с мобильными деньгами. Национальным поставщикам связи необходимо адаптировать свои бизнес-модели к этим новым услугам; аналогичным образом, регуляторным органам придется пересмотреть круг своих обязанностей.

MNO являются поставщиками услуг подвижного доступа в интернет, а передача данных представляет собой основной источник их доходов. Бизнес-модель подвижной связи будет следовать бизнес-модели

операторов фиксированной связи, которые начинали как поставщики услуг голосовой связи, но теперь зарабатывают деньги преимущественно за счет предоставления услуг передачи данных как розничным, так и оптовым клиентам. За последние двадцать лет большая часть инвестиций MNO была вложена в развитие сетей передачи данных. Переход от услуг голосовой связи и SMS-сообщений к бизнес-модели, ориентированной на данные, неизбежен (см. таблицу 7.3). Рано или поздно MNO окончательно превратятся в поставщиков услуг подвижного доступа в интернет, разграничивая свои продукты по скорости и качеству услуг и конкурируя с другими формами доступа, такими как общедоступные сети Wi-Fi и возможность подключения в местах работы, учебы, а также дома. MNO будут взимать плату не за услуги голосовой связи и SMS, а только за пропускную способность и/или потребление данных. Бизнес-модель поставщика услуг подвижного доступа в интернет можно также описать как ориентированную на данные или цифровую бизнес-модель. Этот переход показан на рисунке 7.8.

Рисунок 7.8. Наглядные тенденции развития бизнес-моделей цифровой подвижной связи



Источник: Esselaar and Stork 2019.

Помимо давления со стороны конкурентов, тенденция, представленная на рисунке 7.8, зависит также от уровня проникновения смартфонов и покрытия сетями 3G+. Переход на бизнес-модель цифровой подвижной связи потребует больше времени в странах с недостаточным покрытием сетями 3G, 4G и общедоступными/частными сетями Wi-Fi, а также низким уровнем проникновения смартфонов. Недостаточное покрытие сетями 3G+ является одной из основных причин того, что некоторым операторам подвижной связи трудно получить от передачи данных доходы, достаточные для компенсации снижения доходов от предоставления услуг голосовой связи и SMS.

Таблица 7.3. Развитие цифровой бизнес-модели неизбежно

	Аналоговая подвижная связь	Цифровая подвижная связь
Бизнес-модель	Услуги	Обеспечение возможностей установления соединений
Система измерений	Минуты и SMS	Пропускная способность или скорость передачи
Влияние на затраты	Значение имеют удаленность, продолжительность и местоположение	Затраты не зависят от времени, удаленности и местоположения
Выставление счетов	Выставление счетов за доступ к услугам и их использование: детализированные системы выставления счетов за услуги голосовой связи и SMS, которые могут различаться в зависимости от их типа (внутрисетевой/межсетевой или в период максимальной нагрузки/обычное время)	Простой счет за услуги доступа
Мониторинг трафика	Подробный мониторинг трафика в рамках системы выставления счетов	Мониторинг использования ограничен использованием данных
Абоненты тарифных планов с последующей оплатой	Подробная проверка для снижения риска или потери доходов и сокращения расходов, связанных с завершением вызовов и предоставлением субсидий на мобильные телефоны	• Риск, связанный с последующей оплатой, ограничен доходом за один расчетный период • Отсутствие риска внешних издержек • Нет необходимости дифференцировать по ценам планы на основе предоплаты и планы с последующей оплатой • Тарифный план с последующей оплатой можно продлить без проведения значительной проверки
Сетевая инфраструктура	GSM 1G и 2G	2,5G, 3G, 4G, 5G

Источник: Esselaar and Stork 2019.

В основе цифровой бизнес-модели лежит принцип "знай своего клиента". На самом деле, борьба не связана с поглощением одного продукта другим, например заменой доходов от услуг голосовой связи и SMS-сообщений доходами от передачи данных; борьба идет за лидерство в сохранении информации о пользователях. В течение многих лет лидирующие позиции занимали MNO: они знали о местонахождении своих клиентов в пространстве и времени, а также то, с кем и когда они общаются. Хотя эта информация по-прежнему доступна для MNO, социальные сети и онлайн-покупки представляют собой источник более эффективной и подробной информации. Информация о клиенте, которой обладают Amazon и Facebook, будет, вероятно, экономически более значимой, нежели информация MNO о том же клиенте. Выход на этот рынок – это решение, обусловленное интересами бизнеса, а не продиктованное регуляторным органом.

Рентабельность по EBITDA в цепочке создания стоимости в интернете показывает, что предоставление доступа конечным пользователям по-прежнему представляет собой прибыльный бизнес. Еще большее значение по сравнению с размером каждого сегмента с точки зрения дохода имеет рентабельность крупных игроков в каждом из сегментов цепочки создания стоимости. В таблице 7.4 приведена прибыль до вычета процентов, налогов, износа и амортизации (рентабельность по EBITDA) для отдельных игроков каждого из сегментов цепочки создания стоимости. В среднем в сегменте установления соединений рентабельность по EBITDA выше, чем в других сегментах цепочки создания стоимости. Сложно приводить аргументы в пользу того, что MNO находятся в более неблагоприятных условиях по сравнению с остальными сегментами. Различия в рентабельности по EBITDA между сегментами показывают также, что в каждом сегменте существует собственное ценностное предложение, инвестиционные критерии и доходность. Netflix, к примеру, намного прибыльнее, чем Disney.

Таблица 7.4. Рентабельность по EBITDA во всей цепочке создания стоимости на основе проверенной финансовой отчетности (проценты)

Сегмент	Компания	2016 год	2017 год	2018 год
Права на контент	Netflix	60	61	59
	Warner Media	–	–	18
	Disney	30	30	29
	Fox Corporation	–	–	22
Онлайновые услуги	Amazon	9	9	12
	Alphabet	33	30	26
	Facebook	53	57	52
Вспомогательные технологии	Cisco	30	30	31
	Akamai	41	37	40
Установление соединений	Airtel Group	35	38	37
	Etisalat	50	50	49
	Maroc Telecom Group	48	49	50
	MTN Group	35	33	35
	Ooredoo	41	42	41
	Sonatel	49	47	45
	Safaricom	42	48	48
	Vodacom Group	38	38	38
	В среднем по сегменту установление соединений	42	43	43
Пользовательский интерфейс	Apple	33	31	31
	Samsung	24	31	35

Источник: Esselaar and Stork 2019.

При переходе МНО к модели, полностью ориентированной на данные, они могут ожидать, что размер их прибыли снизится до уровня других сегментов цепочки создания стоимости. Переход к модели, ориентированной на данные, также означает меньшую потребность в узкоспециализированном регулировании для сектора ИКТ. За исключением радиочастотного спектра, регулирование в области электросвязи со временем станет в меньшей степени ориентировано на конкретный сектор.

7.5 Резюме

Эволюция бизнес-моделей и технический прогресс означают, что может возникнуть необходимость в изменении регуляторных инструментов и институциональных механизмов регулирования, а осуществление регуляторного надзора может быть возложено на вновь созданные или какие-либо иные организации (см. рисунок 7.9). Если отраслевое министерство являлось адекватным надзорным органом для монополий фиксированной связи, то с момента выхода на рынок ПУИ и МНО возникла потребность в отраслевых регуляторных органах. Переход к среде, полностью основанной на цифровых технологиях и IP, означает необходимость модернизации законодательства, политики и нормативных актов в интересах сохранения добросовестной конкуренции. Это приводит к последствиям для национальных регуляторных органов, в том числе регуляторных органов в области ИКТ и радиовещания, комиссий по

вопросам конкуренции и ведомств по защите прав потребителей. Большие данные, ИИ и IoT стимулируют потребность в пересмотре нормативно-правовой среды, поскольку эти технологии способны объединять, анализировать и использовать разрозненные источники данных, предоставляя ценную информацию, пригодную для применения не только в рамках одного сектора, но и на межсекторальном уровне, и в рамках не только одной юрисдикции, а многих. Для решения проблем, возникающих в результате глобализации персональных данных, особенно в отношении защиты персональных данных и разрешения споров с участием потребителей, все чаще возникает потребность в новых узкоспециализированных регуляторных учреждениях.

Рисунок 7.9. Изменение регуляторных подходов с течением времени



Любое приложение, в основе которого лежат рассматриваемые в этой главе технологии, подлежит горизонтальному регулированию со стороны ведомств, отвечающих за защиту прав потребителей, защиту данных, конкуренцию, киберпреступность и т. д. Факторами, определяющими обоснованность надзора со стороны отраслевых регуляторных органов ИКТ, являются функциональность приложений и их использование в той или иной отрасли. Приоритетным должно быть наличие надежной горизонтальной регуляторной экосистемы. Для этого может потребоваться обновление законодательства и создание новых ведомств.

Учитывая трансграничный характер цепочки создания стоимости в интернете, в частности, применительно к онлайн-услугам, ключевыми факторами, содействующими цифровизации экономики и общества, а также получению обусловленных ими преимуществ экономического роста и социального развития, являются сотрудничество и согласованность между различными юрисдикциями.

Справочные материалы

- Accenture. 2016. *Igniting Growth in Consumer Technology*. https://www.accenture.com/t20151231t013104_w_us-en/_acnmedia/pdf-3/accenture-igniting-growth-consumer-technology.pdf
- BEREC. 2016. *BEREC Report on Enabling the Internet of Things*. BoR (16) 39. https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-%20the-internet-of-things
- Deloitte. 2015. *Opportunities in Telecom Sector: Arising from Big Data*. <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-opportunities-in-telecom-sector-noexp.pdf>
- Deloitte. 2016. *Blockchain @ Telco: How Blockchain Can Impact the Telecommunications Industry and its Relevance to the C-Suite*. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf
- Deloitte. 2018a. "Regulating the Future of Mobility: Balancing Innovation and the Public Good in Autonomous Vehicles, Shared Mobility, and Beyond". *Deloitte Insights*, December 21, 2018. <https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/regulating-transportation-new-mobility-ecosystem.html>
- Deloitte. 2018b. "The Future of Regulation: Principles for Regulating Emerging Technologies". *Deloitte Insights*, June 19, 2018. <https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html>
- Deloitte. 2018c. *The Regulator's New Toolkit: Technologies and Tactics for Tomorrow's Regulator*. https://www2.deloitte.com/content/dam/insights/us/articles/4539_Regulator_4-0/DI_Regulator-4-0.pdf
- Deloitte. 2018d. *Government Trends 2020: What are the Most Transformational Trends in Government Today?* *Deloitte Insights*, June 24, 2019. <https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html>
- Ericsson. 2019. *Ericsson Mobility Report*. <https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf>
- Esselaar, S. and C. Stork. 2019. "Evolving Business Models are Driven by OTT Applications". Paper presented at the ITU Study Group on OTT, Geneva, September 2019. <https://researchictolutions.com/home/wp-content/uploads/2019/11/RIS-evolving-business-models.pdf>
- European Commission. 2020. *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*. COM(2020) 65 final. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
- Internet Society. 2017. *Paths to Our Digital Future*. <https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>
- ITU (International Telecommunication Union). 2014. "The Role of Big Data for ICT Monitoring and for Development", In *Measuring the Information Society Report 2014*, Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Statistics/Documents/bigdata/MIS2014_Chapter5.pdf
- ITU (International Telecommunication Union). 2016. *Trends in Telecommunication Reform: Regulatory incentives to Achieve Digital Opportunities*. Geneva: International Telecommunication Union. <https://www.itu.int/pub/D-PREF-TTR.17-2016>
- ITU (International Telecommunication Union). 2017. *Global ICT Regulatory Outlook 2017*. Geneva: International Telecommunication Union. Geneva: International Telecommunication Union. <https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Outlook/2017.aspx>
- ITU (International Telecommunication Union). 2018a. *Assessing the Economic Impact of Artificial Intelligence*. ITU Trends: Issue Paper No.1. Geneva: International Telecommunication Union. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-ISSUEPAPER-2018-1-PDF-E.pdf

- ITU (International Telecommunication Union). 2018b. *Cloud Computing Standardization Roadmap*. ITU-T Y.3500-series. Geneva: International Telecommunication Union. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.Sup49-201811-I!!PDF-E&type=items
- ITU (International Telecommunication Union). 2019a. *Distributed Ledger Technology Terms and Definitions*. Technical Specification FG DLT D1.1. Geneva: International Telecommunication Union. <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>
- ITU (International Telecommunication Union). 2019b. *Distributed Ledger Technology: Regulatory Framework*. Technical Paper HSTP.DLT-RF. Geneva: International Telecommunication Union. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-DLT-2019-RF-PDF-E.pdf
- Liptak, Andrew. 2017. "Tesla Extended the Range of Some Florida Vehicles for Drivers to Escape Hurricane Irma". *The Verge*, September 10, 2017. <https://www.theverge.com/2017/9/10/16283330/tesla-hurricane-irma-update-florida-extend-range-model-s-x-60-60d>
- MapR. 2020. *MapR Guide to Big Data in Telecommunications*. <https://mapr.com/whitepapers/data-convergence-in-telecommunications/assets/data-convergence-in-telecommunications.pdf> (по состоянию на 24 апреля 2020 года).
- McKinsey. 2018. *Notes from the AI Frontier: Insights from Hundreds of Use Cases*. <https://www.mckinsey.com/~media/mckinsey/featured%20insights/artificial%20intelligence/notes%20from%20the%20ai%20frontier%20applications%20and%20value%20of%20deep%20learning/notes-from-the-ai-frontier-insights-from-hundreds-of-use-cases-discussion-paper.ashx>
- Michels, Johan David. 2018. "Blockchain and Telecoms". *InterMEDIA*, (46) 4. <https://ssrn.com/abstract=3324482>
- Porter, M. and James E. Heppelmann. 2014. "How Smart, Connected Products Are Transforming Competition". *Harvard Business Review*, November 2014. <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition>
- TRAI (Telecom Regulatory Authority of India). 2018. "Information Note to the Press". Press Release No. 58/2018. <https://www.trai.gov.in/sites/default/files/PRNo.5829052018.pdf>
- UNSTATS. 2015. *Deliverable 2: Revision and Further Development of the Classification of Big Data*. United Nations Global Working Group on Big Data for Official Statistics Task Team on Cross-Cutting Issues. [https://unstats.un.org/unsd/trade/events/2015/abudhabi/gwg/GWG%202015%20-%20item%202%20\(iv\)%20-%20Big%20Data%20Classification.pdf](https://unstats.un.org/unsd/trade/events/2015/abudhabi/gwg/GWG%202015%20-%20item%202%20(iv)%20-%20Big%20Data%20Classification.pdf)

Глава 8. Техническое регулирование



Настоящая глава, посвященная техническому регулированию, состоит из двух частей: в первой рассматривается качество обслуживания (QoS), а во второй – вопросы нумерации, наименования, адресации и идентификации (ННАИ). В части о QoS описывается роль регуляторного органа в информировании пользователей, сдерживании операторов, имеющих сильные конкурентные позиции, обеспечении эффективного использования ограниченных ресурсов и оценке национальной инфраструктуры. Рассматривается деятельность регуляторных органов, связанная с контролем QoS, в том числе выбор показателей, определение измерений, установление целевых значений, выполнение измерений, их проверка и публикация их результатов, стимулирование повышения качества и обзор достигнутых результатов. Во второй части объясняется важность ННАИ, рассматриваются ресурсы ННАИ, описанные в Рекомендациях МСЭ-Т, и кратко излагаются главные цели управления ННАИ. Рассматриваются наступление цифровой эпохи и влияние новых технологий на ННАИ, а также приводится описание инструментов, имеющих в распоряжении регуляторного органа.

8.1 Часть 1. Качество обслуживания

Введение

Что такое качество обслуживания?

Люди, где бы они ни находились, зависят от услуг ИКТ. Если эти услуги недостаточно хороши, то для того чтобы вести беседы, передавать и принимать сообщения, узнавать новости, переводить деньги, играть, управлять машинами и контролировать их, торговать и покупать, участвовать во встречах, учиться, развлекаться и т. д., требуется личный контакт. Спектр услуг непрерывно растет.

Что именно означает оценка "достаточно хороши", зависит от многих факторов, например чувств и ожиданий пользователей, которые сами по себе различаются в зависимости от используемых приложений и обстоятельств. Достаточно хорошие услуги, пусть даже они не вызывают восхищения, как правило, не должны раздражать. Согласно определению, приведенному в Рекомендации МСЭ-Т Р.10/G.100, оценка пользователем качества услуг (QoE) – это "степень удовлетворенности или неудовлетворенности пользователя приложением или услугой" (ITU-T 2017).

Оценка качества определяет степень удовлетворенности или раздражения при определенных обстоятельствах. С расширением спектра услуг растет разнообразие оценок качества; например, в настоящее время существуют стандарты оценки качества потоковой передачи мультимедиа по технологии over-the-top (OTT) на телевизоры и смартфоны, а также стандарты разработки тестов для оценки качества цифровых финансовых услуг (ITU-T 2020b; МСЭ-T 2020c).

Понятие качества обслуживания (QoS) ограничивает внимание некоторыми факторами, от которых зависит оценка качества услуги пользователем; оно определяется как "совокупность характеристик услуг электросвязи, которые отражают ее способность удовлетворять сформулированные и подразумеваемые потребности пользователя" (ITU-T 2017).

QoE и QoS относятся как к информационным, так и к коммуникационным технологиям. Например, пользователей интерактивных систем интересует быстрота получения ответа от системы, а не то, как вырабатываются ответы, и отдельные части систем могут находиться в облаке, а не в пользовательских терминалах (раньше это называлось отношениями клиент–сервер с тонкими клиентами): важны как скорость передачи, так и скорость обработки информации.

На протяжении многих лет качество обслуживания и другие подобные термины использовались по-разному. В некоторых документах (например, спецификациях WiMAX) качество обслуживания относится к методам управления определенными типами трафика, такими как голосовой или видеотрафик; в других документах для этой цели используются термины "класс обслуживания" и "тип услуг", а термин "категория обслуживания" (grade of service) относится конкретно к успешному установлению соединения. Когда QoS используется только для описания методов управления трафиком, для оценки того, насколько хорошо или плохо услуги ИКТ, необходимо использовать QoE.

QoS, как оно рассматривается здесь, тесно связано с QoE и лишь косвенно – с методами управления трафиком. Однако понятие QoE включает в себя аспекты характеристики пользователя, которые QoS, как оно часто понимается, упускает из вида.

Понятию QoE здесь уделяется особое внимание, поскольку оно менее известно, чем QoS. Тем не менее QoS остается актуальным для оценки того, используют ли люди услуги ИКТ, почему они их используют и каким образом.

Что должен делать регуляторный орган?

Операторы сами проводят множество оценок QoS в ходе своей обычной технической деятельности и в ответах на жалобы клиентов. Если у них имеются конкуренты, то они в целях сохранения своей доли рынка ищут наилучшее сочетание качества и цены и обязательно контролируют QoS. Конечно, в отсутствие конкуренции и принуждения они могут этого не делать. Однако даже при наличии конкуренции некоторые группы населения могут обслуживаться плохо, а общенациональные потребности не удовлетворяться.

В общем случае регуляторный орган должен преследовать следующие цели.

- **Информирование пользователей.** Любые проверки жалоб операторов должны выполняться другими сторонами. При любых сравнениях качества между операторами должны использоваться сопоставимые измерения, которые не могут быть выполнены одним оператором. Эти проверки и сравнения, опубликованные надлежащим образом, помогут восстановить информационный баланс между клиентами и операторами.
- **Сдерживание операторов, имеющих сильные конкурентные позиции.** Такие операторы могут понизить качество услуг в целях повышения своих доходов, особенно если они обладают значительным влиянием на рынке или назначены для обеспечения универсального обслуживания. Это справедливо как для оптовых, так и для розничных услуг; например, оператор, контролирующий коммутаторы международного шлюза в стране, может диктовать условия соглашений об уровне обслуживания при межсетевом взаимодействии.
- **Обеспечение эффективного использования ограниченных ресурсов.** Люди имеют право знать, насколько хорошо используется общественная собственность, такая как радиочастотный спектр, и соблюдаются ли права доступа к такой собственности, например к земельным ресурсам. Это "ограниченные ресурсы" – их можно использовать более или менее эффективно, но их количество не растет. Правильное использование таких ресурсов может способствовать полноценному обслуживанию различных сообществ по всей стране.

- **Оценка национальной инфраструктуры.** Должна быть построена удовлетворительная инфраструктура для оказания поддержки в чрезвычайных ситуациях, инвестиционной деятельности, развития человеческого потенциала и предоставления государственных услуг. Ни один оператор не несет за это ответственности, а вот регуляторный орган может увидеть общую картину. Конкурентный рынок не в состоянии заполнить пробелы в инфраструктуре без дополнительной помощи и даже может привести к снижению качества, поскольку все операторы пытаются сократить расходы.

Эти цели могут ограничить сферу участия регуляторного органа, но не определяют его масштаб. В разных местах и в разное время качество услуг может значительно различаться. Существенно различаются и сами услуги; их оценка не всегда сводится лишь к подсчету процента успешно завершенных вызовов. Возможно, регуляторному органу придется тщательно выбрать области участия или найти способы побудить к проведению оценок других, работая с операторами или используя метод краудсорсинга.

Степень участия регуляторного органа зависит от нескольких факторов, таких как зрелость рынка, финансовые ограничения, политические установки и институциональные механизмы. Даже если регуляторный орган не проводит измерения QoS, не осуществляет их проверку и не публикует их результаты, существуют способы, которыми он может выполнять определенный мониторинг совместно с операторами.

Нормы QoS могут существовать на бумаге, но игнорироваться на практике. Регуляторные органы могут не получать результатов измерений и не обеспечивать соблюдения требований. В этих случаях операторы могут достигать установленных целевых значений, но не чувствовать необходимости в сообщении результатов¹. Особенно часто от этого страдают небольшие страны, где работают дочерние компании крупных операторов.

Что представляют собой параметры и целевые значения?

QoS оценивается путем проведения измерений и проверки того, являются ли их результаты удовлетворительными. Результаты измерений относятся к следующим категориям.

- **Параметры.** Это количественные величины, которые измеряются для оценки качества того или иного аспекта услуг. В других документах они могут называться "показатели", "характеристики", "меры" или "детерминанты". Примерами могут служить "коэффициент успешного установления вызовов" (или "доля успешных попыток установления вызовов") и "среднее время разрешения жалоб" (или "среднее время, затрачиваемое на разрешение жалоб").
- **Целевые значения.** Это значения параметров, при которых данный аспект услуги считается "удовлетворительным"; они могут быть предназначены для немедленного достижения или для достижения за определенный период времени. В других документах они могут называться "целевые показатели", "контрольные показатели" или "пороговые значения". Примерами могут служить "97%" (для коэффициента, такого как коэффициент успешного установления вызовов) или "6 часов" (для показателя времени, например среднего времени разрешения жалоб).

Международные стандарты QoS, разработанные Международным союзом электросвязи (МСЭ), Европейским институтом стандартизации электросвязи (ETSI), Проектом партнерства третьего поколения (3GPP) или другими организациями, обычно определяют параметры и описывают методы их измерения, но не устанавливают целевых значений. Во многих странах также определяются параметры, но целевые значения не устанавливаются.

Среди региональных организаций Управление электросвязи стран Восточно-Карибского региона (ECTEL) и Восточноафриканская организация связи (EACO) предложили необычное определение параметров для своих государств-членов. Параметры определяются для услуг передачи голоса и данных, а в EACO — для цифровых финансовых услуг с использованием определенных неструктурированных данных дополнительных услуг (USSD), службы коротких сообщений (SMS) и сообщений защищенного протокола передачи гипертекста (HTTPS) (EACO 2017).

МСЭ подготовил руководство по регулированию качества обслуживания, предназначенное главным образом для регуляторных органов (ITU-D 2017). В нем содержится множество примеров параметров, принятых в разных странах мира, а также обсуждаются некоторые другие актуальные темы. Сокращенное

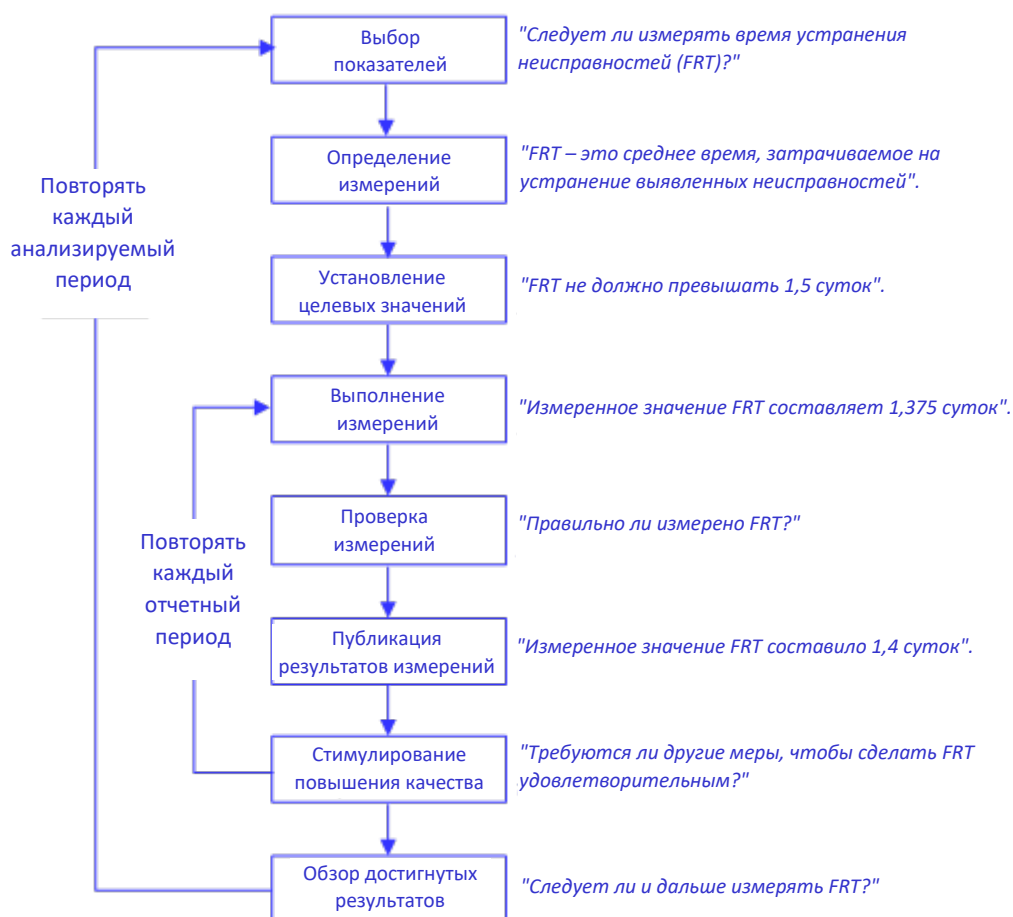
¹ Оба недостатка проиллюстрированы в тематическом разделе "Опыт ECTEL в области регулирования качества обслуживания" *Платформы цифрового регулирования*.

описание некоторых из этих тем можно найти в Добавлении 9 к Рекомендациям МСЭ-Т серии E.800 (МСЭ-Т 2013а).

Что включает контроль качества обслуживания?

На рисунке 8.1 показана деятельность регуляторных органов, связанная с контролем QoS, в виде сокращенного варианта обширной блок-схемы.

Рисунок 8.1. Деятельность в рамках контроля QoS



Источник: по материалам ITU-D 2006.

Внешний цикл, повторяемый каждый анализируемый период, включает следующие действия.

- **Выбор параметров.** Выбранные для измерения параметры должны напрямую относиться к наиболее важным для пользователей аспектам их восприятия.
- **Определение измерений.** Измерения должны определяться таким образом, чтобы разных операторов можно было сравнивать по параметрами, имеющим существенное значение для пользователей.
- **Установление целевых значений.** Любые целевые значения параметров следует устанавливать с учетом тех улучшений качества, которые можно разумно ожидать.
- **Обзор достигнутых результатов.** Обзор достигнутых результатов проводится в конце анализируемого периода, чтобы определить, выполнены ли задачи по контролю QoS.

Внутренний цикл, повторяемый каждый отчетный период, включает следующие виды деятельности.

- **Выполнение измерений.** Измерения проводятся операторами, регуляторным органом или и операторами и регуляторными органами. Если измерения проводятся операторами, те регистрируют их и сообщают результаты регуляторному органу в конце отчетного периода.
- **Проверка измерений.** Регуляторный орган может осуществлять проверку измерений. Если измерения проводятся операторами, регуляторный орган часто полагается на самосертификацию операторов (когда руководство компаний-операторов удостоверяет правильность измерений) и периодические или ежегодные проверки, возможно, в сочетании с тестированием в условиях движения на автомобиле или ходьбы или тестированием с использованием метода краудсорсинга.
- **Публикация результатов измерений.** Результаты измерений публикуются операторами, регуляторным органом или и операторами и регуляторным органом. Затем они могут публиковаться журналистами в онлайн-новых и традиционных изданиях.
- **Стимулирование повышения качества.** Повышение качества можно стимулировать различными способами, которые варьируются от предложения планов повышения качества до наложения штрафов. В некоторых случаях достаточным стимулом может стать дурная слава, вызванная публикацией результатов измерений.

Могут наблюдаться всплески активности, не соответствующие отчетным периодам, с постоянной продолжительностью и частотой повторений, особенно во внутреннем цикле. Например, регуляторные органы могут проводить измерения в определенных местах, которыми пренебрегли при расширении сети или с которыми связано множество жалоб, при этом им, возможно, придется отказаться от проведения измерений в других местах.

Для повышения качества услуг, не связанных непосредственно с обслуживанием клиентов, часто требуется совершенствование сетей. Следовательно, его оценку нужно проводить только в таких временных рамках, в которых можно было бы добиться улучшений; все остальное может привести к излишней нагрузке на операторов, которые должны будут проводить измерения и сообщать их результаты, и на регуляторные органы, проводящие проверки или публикующие результаты. Это означает, что между оценками QoS должно пройти не менее трех месяцев. Соответственно регуляторные органы часто требуют от операторов ежеквартальной отчетности. Однако сами они могут проводить измерения раз в год для выяснения обстоятельств в определенных местах или проверки отчетов операторов.

Эти виды деятельности подробнее рассматриваются в Руководстве МСЭ по регулированию качества обслуживания (ITU-D 2017), а также в Рекомендации МСЭ-Т E.805 (МСЭ-Т 2019a). В следующих разделах они рассматриваются по отдельности в порядке их проведения.

Выбор параметров

Регуляторные органы могут получить первоначальное представление о том, как им следует организовать контроль QoS, из сообщений в прессе, от встреч с общественностью, из контактов с организациями потребителей, жалоб, поступающих операторам, и бесед с операторами. Может помочь анализ сообщений в социальных сетях, но он осложнен из-за потенциальных преувеличений или дезинформации.

Кроме того, регуляторные органы могут проводить опросы потребителей – очные, по телефону или в интернете, для чего вовсе не требуется больших расходов или трудозатрат. Могут принести пользу даже ответы на общие вопросы, такие как "Насколько вы удовлетворены качеством получаемых услуг?". Простым примером служат ответы клиентов на девять вопросов о трех услугах, предоставляемых тремя операторами на двух островах (CICRA 2019).

Особенно тщательный метод заключается в том, чтобы просить людей вести записи в дневнике о своей деятельности, связанной с ИКТ. Ведение дневника придает относительную важность деятельности, которая может повлиять на приоритеты в отношении контроля QoS. Результаты могут быть достаточно подробными: в одном случае упоминалось до 30 различных видов деятельности в области ИКТ для разных возрастов, социальных групп и полов (Ofcom 2016).

Выбор параметров должен соответствовать следующим критериям.

- **Актуальность для пользователей.** Контроль QoS больше касается оценки пользователями качества услуг, чем технических характеристик сети. Операторам при проектировании сетей может потребоваться проверка эксплуатационных параметров последних, однако регуляторным органам, которые не занимаются проектированием сетей, это не нужно. Например, регуляторные органы не требуют от операторов сообщать параметры передачи обслуживания (хэндовера) при беспроводной связи; они могут быть важны для проектировщиков сетей, но не имеют прямого отношения к пользователям, которым достаточно знать долю успешных соединений. При контроле QoS регуляторные органы стараются оценить QoS, достигаемое операторами, в сравнении с QoE, желательным для пользователей². Таким образом, параметры QoS, контролируемые регуляторными органами, должны иметь прямое отношение к оценке пользователями качества услуг.
- **Важность для общества.** Некоторые параметры могут не представлять непосредственного интереса для отдельных пользователей, но быть важными для общества в целом. В частности национальная инфраструктура должна быть удовлетворительной для оказания поддержки в чрезвычайных ситуациях, инвестиционной деятельности, развития человеческого потенциала и предоставления государственных услуг. Оценка национальной инфраструктуры позволит, например, оценить пропускную способность соединений на важнейших сетевых маршрутах, чтобы гарантировать, что в случае бедствия может быть выполнено достаточное количество вызовов. Потребность в таких параметрах должна быть рассмотрена рабочей группой по планированию электросвязи в чрезвычайных ситуациях.
- **Общие характеристики услуг.** Разные регуляторные органы по-разному группируют услуги в целях контроля QoS; например, они могут объединять услуги фиксированной широкополосной связи с услугами подвижной широкополосной связи или разделять их (в этом случае услуги подвижной широкополосной связи часто игнорируются). Группирование отражает конкретные ситуации в разных странах, но затрудняет сравнение между странами. Однако некоторые параметры могут быть общими для разных услуг, особенно те, что связаны с обслуживанием клиентов.
- **Независимость от технологии.** Параметры не должны зависеть от технологии, если только пользователи не считают ее характеристикой контролируемых услуг. Например, голосовые вызовы остаются голосовыми независимо от того, являются ли базовые сети фиксированными или подвижными, так что параметры телефонии для фиксированных и подвижных услуг (а также для традиционных и OTT-услуг) могут быть общими. Это согласуется с усиливающимся вытеснением фиксированных услуг подвижными, когда требования пользователей к услугам телефонной связи и их ожидания в отношении таких услуг в основном не зависят от сетевых технологий.

В то же время параметры предоставления услуг могут быть общими для услуг проводной и беспроводной связи, нуждающихся в фиксированном доступе (поскольку они усложняются главным образом необходимостью посещения помещений клиентов), но игнорироваться для услуг, требующих подвижного доступа.

- **Минимальность требований.** Контроль QoS может быть обременительным как для регуляторных органов, так и для операторов. Расходы на него следует сопоставлять с получаемыми от него выгодами. Существует много параметров, которые могут контролироваться: в Рекомендации МСЭ-Т E.803 (ITU-T 2011) перечислены 88 параметров системы обслуживания абонентов. Однако жалобы абонентов и опросы указывают на отсутствие необходимости в большинстве из них. Например, в Соединенном Королевстве 75–95% жалоб на то, что услуги "не работают должным образом" (часто из-за прерывания обслуживания, некачественной доставки или неточной рекламы), и на ошибки при выставлении счетов приходятся на четыре услуги (фиксированная широкополосная связь, фиксированная телефонная связь, подвижная широкополосная и телефонная связь, а также абонентское телевидение) (Ofcom 2019).

Если параметры выбраны, они, как правило, остаются даже тогда, когда в них больше нет необходимости. Например, в разных странах все еще сообщают время установления голосового вызова, хотя оно редко бывает большим. Если параметры устарели или надобность в них отпала, следует отказаться от их измерения. Так поступили, например, в Бразилии³.

² Соответствующие виды оценки описаны в тематическом разделе "Взаимосвязь между качеством обслуживания и оценкой пользователем качества услуги" *Платформы цифрового регулирования*.

³ В результате в таблице из тематического раздела "Подход Anatel к контролю качества услуг подвижной связи" *Платформы цифрового регулирования* зачеркнуты 8 из 14 позиций.

Дополнительные рекомендации по выбору измеряемых параметров можно найти в Рекомендации МСЭ-Т E.802 (МСЭ-Т 2007). В ней с нескольких точек зрения обсуждаются отношения между различными аспектами качества и параметрами, которые могут рассматриваться как мера этих аспектов.

Определение измерений

Операторы, вероятно, уже разработали и реализовали планы регулярного контроля QoS. Обсуждение этого вопроса с ними и со сторонними организациями, осуществляющими контроль QoS по договорам, может способствовать лучшему пониманию полезности измерения определенных параметров, повышению целесообразности проведения и проверки измерений и установлению более реалистичных целевых значений.

Следующие руководящие указания касаются деталей процесса проведения измерений.

- **Соответствие использованию.** Измерения следует проводить в то время и в тех местах, которые в максимальной степени согласуются с восприятием (оценкой) пользователем качества услуг. В частности, следует использовать данные о фактической деятельности пользователей, а не данные из инструментов планирования. Аналогичным образом при измерениях следует использовать данные, полученные из мест расположения потенциальных пользователей, а не от базовых станций, когда они тестируют такое действие, как установление соединения, которое может дать сбой еще до установления связи с базовыми станциями.
- **Осведомленность о времени и месте.** В разное время года и разное время суток – даже в течение одного рабочего дня – могут иметь место значительные колебания качества. Это может служить признаком того, что у услуги еще недостаточно пользователей для эффективного статистического мультиплексирования – при небольшом количестве пользователей трудно оправдать распределение дополнительной полосы, поэтому колебания спроса приходится на значительную долю распределенной полосы частот.

Значительные различия в качестве также могут наблюдаться между соседними районами с разными показателями плотности населения, землепользованием, интенсивностью дорожного движения и окружающей средой. Например, быстрое перемещение на автомобиле или нахождение внутри помещения может привести к ослаблению сигнала на 15 дБм (Marina et al. 2015).

Если различия в качестве обслуживания в разное время и разных местах велики, то необходимы результаты отдельных измерений. Регуляторный орган совместно с операторами должен определить, результаты каких именно измерений необходимы (обычно после разделения измерений на измерения в помещении, в движении в автомобиле и при ходьбе). В любом случае регуляторный орган должен получать результаты измерений с указанием времени и места их проведения.

- **Сравнимость между операторами.** Измерения, выполненные разными операторами и регуляторным органом, могут быть полностью сравнимы друг с другом только в том случае, если способы их выполнения одинаковы во всех отношениях, имеющих важное значение для пользователей. Этого бывает трудно достичь: разные операторы не только проводят измерения в разное время и в разных местах, но и используют разные методы и оборудование. Простое перечисление параметров (как во многих нормативных документах и лицензиях) редко позволяет точно определить методы измерения – стандарты могут содержать множество вариантов, а поставщики оборудования – использовать одни и те же названия для разных счетчиков сетевых элементов.
- **Репрезентативность.** Часто результаты измерений составляются из выборочных значений, как правило, путем вычисления среднего значения. В этом случае всегда имеет место ошибка выборки. Она уменьшается, если взята достаточно большая выборка, чтобы обеспечить уверенность в том, что результат измерения, полученный на ее основе, близок к значению, соответствующему оценке качества услуг пользователем⁴. В идеале выборка должна быть достаточно велика, чтобы разные результаты измерений отражали заметно различающуюся оценку пользователем качества услуг. Регуляторные органы часто игнорируют этот момент в отчетах об измерениях в условиях движения и при ходьбе, приводя результаты для небольших районов без указания количества измерений, выполненных в каждом из них.

⁴ Связь между уровнем доверия и размерами выборки объясняется в тематическом разделе "Базовая статистика для оценки качества обслуживания" *Платформы цифрового регулирования*. Другая информация по оценке и ранжированию операторов содержится в Рекомендации МСЭ-Т E.840 (МСЭ-Т 2018).

- **Восприятие пользователями.** Разницу между результатами измерений, при которых не наблюдается ощутимых различий в восприятии (оценке) пользователями качества услуг, можно считать "едва заметной", то есть не превышающей порогового значения. Это пороговое значение не зависит от результатов измерения: часто при заданной разнице в результатах измерения различия в восприятии пользователями качества услуг выявить легче, когда результаты измерения малы (то есть разница между значениями 2% и 3% заметнее, чем между значениями 97% и 98%).

При усреднении не всегда суммируются все полезные результаты; например, среднее время ремонта может быть выведено из большого количества кратковременных и немногих длительных ремонтов. Поэтому наиболее подходящим параметром иногда служит не среднее значение по выборке, а максимум – в квантиле, который представляет собой долю (например, 80, 90, 95 или 99%-ную) наименьших значений в выборке. Взятые вместе, среднее значение и максимальное значение в подходящем квантиле могут дать всестороннюю характеристику выборки; если публикуется только одно из них, то это обычно среднее значение, которое понятнее пользователям⁵.

Установление целевых значений

Как отмечается в Рекомендации МСЭ-Т E.805 (МСЭ-Т 2019а), целевые значения параметров нужны не всегда. Популярность голосовых услуг ОТТ показывает, что многие пользователи готовы пожертвовать качеством ради экономии – высокому качеству при высоких ценах они предпочитают низкие цены при низком качестве. Требования QoS не должны мешать пользователям выбирать определенные уровни качества услуг или операторам предлагать услуги определенного качества независимо от того, традиционные это услуги или услуги ОТТ.

Регуляторные органы могут давать рекомендации по уровням качества (как пользователям, так и операторам), не устанавливая целевых значений. Однако при отсутствии практического выбора между уровнями качества целевые значения могут способствовать защите потребителей. Это может иметь место по следующим причинам:

- наличие монополии (а иногда даже олигополии со слабой конкуренцией), вероятно, с предоставлением "универсального обслуживания";
- при наличии конкуренции переход от одного поставщика к другому затруднен из-за высоких затрат и падения уровня качества без соответствующего снижения цен.

Полезные рекомендации по установлению целевых значений приведены в Рекомендации МСЭ-Т E.802 (МСЭ-Т 2007). Зачастую бывает трудно установить реалистичные, но достаточно жесткие целевые значения. Их следует вводить только после измерения степени их достижимости; такие значения можно все более ужесточать после каждого анализируемого периода, в течение которого они достигались.

К целевым значениям, установленным в других странах, следует относиться с осторожностью из-за иных условий и вероятности того, что регуляторные органы могут игнорировать собственные правила.

Выполнение измерений

Как описано в Рекомендации МСЭ-Т E.802 (МСЭ-Т 2007), измерения могут быть субъективными или объективными⁶. Здесь основное внимание уделяется объективным измерениям, поскольку субъективные измерения для репрезентативных выборок пользователей дороги и сложны в разработке.

Измерения для реальной сети можно проводить в сети или на местах. Ниже приведена их дальнейшая классификация.

- **Системные показания.** Их собирают в сети от сетевых узлов и вспомогательных систем. Может потребоваться посещение линейно-кабельных сооружений, но чаще производится централизованный сбор данных в сети и вспомогательных системах (хотя это возможно с использованием клиентского оборудования при тестировании, если оно работает и открыто для вмешательства оператора).

⁵ Описание средних значений и квантилей содержится в тематическом разделе "Базовая статистика для оценки качества обслуживания" *Платформы цифрового регулирования*. Дополнительные описания, сопровождаемые подробными сведениями о нескольких полезных дистрибутивах, можно найти в технической спецификации ЕТСИ (ETSI 2019).

⁶ Цели субъективных и объективных оценок качества описаны в тематическом разделе "Взаимосвязь между качеством обслуживания и оценкой пользователем качества услуг" *Платформы цифрового регулирования*.

Данные могут собираться оператором и направляться в регуляторный орган; в качестве альтернативы регуляторный орган может самостоятельно получать их непосредственно с сервера, подключенного к сети оператора. Однако эти данные не всегда полностью отражают оценку пользователем качества услуг; например, подсчет сетевым элементом попыток беспроводного вызова не учитывает неудачные попытки, поскольку они не достигают базовой станции.

- **Выездные испытания.** Они проводятся в полевых условиях в соответствии с планом для определенного времени и места. Испытательное оборудование должно использовать проводное или беспроводное подключение к сетям подобное тому, какое понадобится потребителю. Выездные испытания фиксированного доступа нередко проводятся в помещениях или на линейно-кабельных сооружениях операторов во избежание необходимости получения доступа в жилые дома и учреждения; выездные испытания подвижного доступа часто представляют собой тестирование в условиях движения в автомобиле или ходьбы, которое проводится в транспортных средствах или общественных местах (например, в магазинах и торговых центрах) с использованием множества мобильных телефонов или специального испытательного оборудования и допущений о возможности распространения результатов на жилые дома и учреждения. Хотя тестирование в условиях движения обычно осуществляется людьми, оснащенными соответствующим оборудованием, когда требуется наблюдение за определенными местами, аналогичное тестирование может проводиться удаленно с помощью автономных зондов.

Тестирование в условиях движения в автомобиле или ходьбы связано с большими расходами. Для обеспечения доверия к нему нужны сотни тестов, которые необходимо повторять везде, где требуются отдельные результаты. Для снижения затрат регуляторный орган или операторы могут выбрать агента, который будет проводить испытания для всех операторов. В простейшем случае агента выбирает регуляторный орган, возмещая расходы в форме обычных сборов с операторов (или, например, пропорционально количеству испытаний на оператора). При альтернативном варианте агента выбирают операторы; регуляторный орган может оказать помощь и уменьшить возможность задержки, созывая собрания операторов и предлагая способы распределения расходов. В любом случае агент должен быть готов к проведению испытаний для всех операторов на равных условиях, чтобы все они могли получить одинаковую экономию от масштаба и объема измерений.

- **Краудтестирование.** Оно проводится на местах методом краудсорсинга. Измерения, которые выполняются с помощью терминалов пользователей или распределенного среди пользователей испытательного оборудования, в совокупности отражают оценку пользователем качества услуг. Такое тестирование не эквивалентно для разных операторов: оно проводится в любое время и во всех местах, где присутствуют пользователи, и может быть или не быть инициировано пользователями. Для краудтестирования фиксированного доступа требуются персональные компьютеры или испытательное оборудование, а для краудтестирования подвижного доступа – смартфоны (если только тестирование не основано лишь на передаче текстовых сообщений пользователям и от них). Хотя тесты могут быть инициированы пользователями, результаты с большей вероятностью будут отражать общую ситуацию, если они будут запущены автоматически, а не в зависимости от сиюминутных ощущений каждого пользователя.

Полезное описание этих методов содержится в примерах из франкоговорящих стран Африки (Fratel 2019; Fratel 2020). В них также упоминается оценка качества на основе сообщений о покрытии (обычно отображаемом на картах). Если сообщения о покрытии основаны только на географической и демографической информации, то такие оценки не заменяют измерений. Однако они могут повлиять на решение о том, где именно следует проводить измерения.

В прошлом измерения для фиксированного доступа обычно представляли собой сбор системных показаний, а измерения для подвижного доступа часто проводились в процессе автомобильного или пешего движения; теперь же альтернативу им составляет краудсорсинг. Эти методы оценки QoS в подвижных сетях обсуждаются в Рекомендации МСЭ-Т E.806 (МСЭ-Т 2019b). В ней даются рекомендации по выбору активных и пассивных измерений, измерению определенных параметров, характеристикам систем контроля (за исключением краудсорсинга), обработке данных и формированию выборок. Ее дополняет Рекомендация МСЭ-Т E.812 (ITU-T 2020a). В ней содержатся дополнительные рекомендации по некоторым из перечисленных тем (и по характеристикам тестовых серверов для краудсорсинга⁷).

⁷ Соответствующее обсуждение содержится в тематическом разделе "Методы краудсорсинга в оценке качества обслуживания" *Платформы цифрового регулирования*.

Проверка измерений

Когда измерения проводятся разными операторами в разное время и в разных местах, результаты не могут быть строго сравнимы между собой. Можно сократить расходы и достичь сравнимости результатов, проводя измерения для всех операторов одновременно. Однако операторы могут оказаться не готовы к тому, что их тесты в условиях движения в автомобиле или ходьбы проводятся общим агентом. В этих случаях результаты должны проверяться регуляторным органом.

С этой целью каждый оператор должен хранить записи измерений, возможно, в течение года после их получения. Записи должны включать подробности наблюдений и расчетов, а также любые сообщения о неисправностях или жалобы на обслуживание, от которых зависели результаты измерений. Они представляются регуляторному органу для сравнения с другими измерениями, выполненными этим регуляторным органом или другими операторами. Такое сравнение позволяет определить:

- что результаты измерений, вероятно, справедливы;
- что измерения нуждаются в более точных определениях, так как разные операторы интерпретируют их по-разному.

Если операторы используют краудсорсинг, у них могут быть разные сборщики данных, которые собирают данные и обрабатывают их для получения результатов измерений. Чтобы проверить, насколько сопоставимы результаты измерений для разных операторов, регуляторный орган должен подробно изучить процесс сбора и обработки данных каждого оператора и при необходимости потребовать внесения изменений.

При краудсорсинге каждый отдельный пользователь в каждый момент времени тестирует только одну сеть. Однако пользователей может быть столько, что может быть проведено достаточно тестов каждой услуги. Если требуются дополнительные тесты, регуляторный орган может организовать вызовы на множество смартфонов (по одному для каждой сети) в определенное время и в определенном месте.

Даже если краудсорсинг не является основным методом измерения QoS, он может быть полезен при проверке, позволяя сравнить результаты измерений, сообщенные операторами, с результатами, полученными методом краудсорсинга.

Публикация результатов измерений

Публикация информации по QoS имеет важное значение, если потребителям необходимо делать осознанный выбор. Публикация может осуществляться регуляторным органом или операторами. Дешевле и лучше будет, если это будет делать одна организация; более того, у регуляторного органа больше возможностей для предоставления объективных сравнительных данных, чем у операторов. Однако операторы часто располагают большими ресурсами, чем регуляторный орган, поэтому им следует самостоятельно публиковать свою информацию по QoS, одобренную регуляторным органом, в форматах, согласованных с регуляторным органом.

При предоставлении информации пользователям необходимо соблюдать баланс — пользователей не следует перегружать, но они должны иметь достаточно информации для принятия решений. В частности:

- результаты измерений могут отображаться в виде рейтингов, таблиц, гистограмм или звездных карт (возможно, с использованием цветов светофора или других пометок, показывающих, удовлетворительны ли эти результаты⁸). Они могут сопровождаться пояснениями причин неудовлетворительных результатов измерений, сделанными операторами или регуляторным органом;
- в результатах измерений должны по возможности использоваться одинаковые соглашения по числовым параметрам. Так, на хорошее качество во всех или почти во всех случаях должны указывать только высокие или только низкие значения; например, наряду с коэффициентом сброшенных вызовов должен измеряться коэффициент безуспешного, а не успешного установления вызовов. Поскольку пользователи считают, что малые числа оценивать легче, чем большие, желательно, чтобы на хорошее качество указывали низкие значения, по крайней мере для параметров, которые

⁸ Большая часть этих возможностей проиллюстрирована в тематическом разделе "Примеры способов представления качества услуг регуляторными органами" *Платформы цифрового регулирования*.

измеряются процентами. Однако при средней экспертной оценке (MOS) хорошими считаются высокие значения;

- результаты измерений следует записывать не более чем с двумя значащими цифрами. Дополнительные разряды редко отражают различия в качестве, оцениваемом пользователями;
- результаты измерений могут быть представлены уровнями, каждый из которых содержит указания на следующий, более детальный. Пользователей по всей вероятности интересует не вся информация о QoS, а определенные ее части; например, одного может интересовать качество речи на главных дорогах, а другого – доступность широкополосной связи в удаленных местах⁹. Разным людям требуется представление информации с разными уровнями детализации. Например, лица, определяющие политику или формирующие общественное мнение, поставщики услуг и крупные предприятия могут отдавать предпочтение веб-страницам и газетным комментариям, а частные потребители и малые предприятия – листовкам, вкладышам в счета, каналам социальных сетей, радио- и телевизионной рекламе, бесплатным сообщениям по телефону и собраниям;
- результаты измерений должны быть представлены объективно. Например, результаты, полученные оператором, вынужденным использовать сеть другого оператора, могут быть снабжены пояснениями, если они ухудшены из-за недостатков этой сети.

Стимулирование повышения качества

Как указано в Рекомендации МСЭ-Т E.805 (МСЭ-Т 2019а), в случае необходимости в повышении качества могут потребоваться инвестиции, а наложение штрафов может оказаться контрпродуктивным. Например, регуляторный орган Чада, заметив, что налагавшиеся на протяжении нескольких лет штрафы не возымели эффекта, заменил их требованием в течение шести месяцев инвестировать суммы, эквивалентные сумме штрафов, в совершенствование сетей (ARCEP 2020).

Составление и реализация планов по стимулированию повышения качества поможет операторам и регуляторному органу совместно решать соответствующие задачи по разработке и изменению параметров и целевых значений, сохраняя их актуальность. Предоставление пользователям сравнительной информации по операторам позволит стимулировать повышение качества за счет конкуренции, особенно при упрощенной смене операторов.

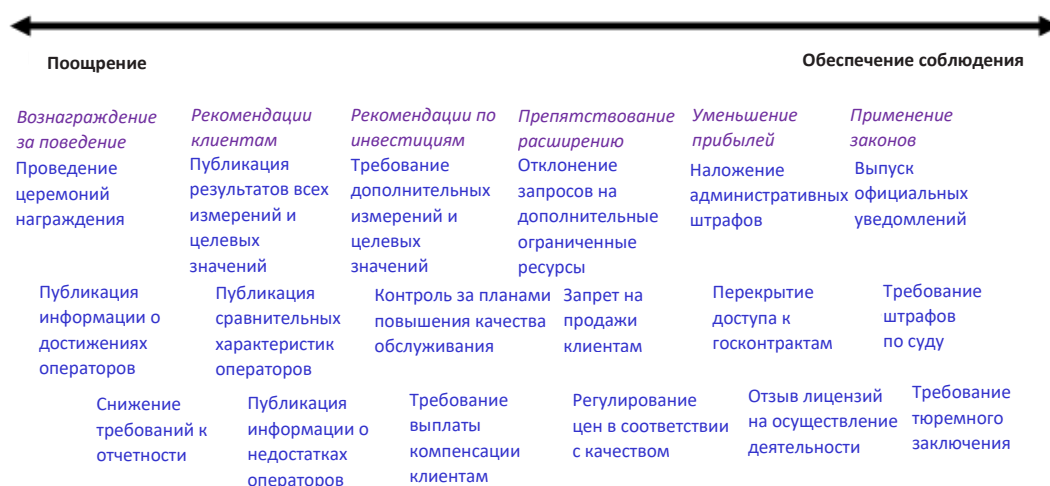
Повышению качества может способствовать как хорошая, так и плохая реклама. Например, регуляторный орган может публиковать информацию о достижениях операторов, которые работают значительно лучше других (или превышают целевые показатели), и награждать их такими званиями, как "лучший оператор широкополосной связи года" (или по крайней мере анализируемого периода). Сегодня немногие регуляторные органы делают нечто подобное; на самом деле многие даже не называют и не стыдят операторов, не отвечающих требованиям, и не публикуют показатели отдельных операторов.

Существует широкий круг доступных методов повышения качества¹⁰, как показано на рисунке 8.2. Их применение должно иметь аргументированное обоснование; иначе в конечном счете это может привести к пренебрежению верховенством закона (со стороны граждан или властей). Эти методы можно ранжировать по тому, в какой мере операторы стараются повысить качество обслуживания без повышения цен. Они также должны быть пропорциональными и адаптивными, как описано в Рекомендации МСЭ-Т E.805 (МСЭ-Т 2019а). Например, штрафы должны зависеть от продолжительности и серьезности нарушения нормативных актов и лицензий.

⁹ Спектр информации, предоставляемой в Бразилии, приведен в тематическом разделе "Подход Anatel к контролю качества услуг подвижной связи" *Платформы цифрового регулирования*.

¹⁰ Несколько таких методов упоминается в тематическом разделе "Примеры способов предоставления качества услуг регуляторными органами" *Платформы цифрового регулирования*.

Рисунок 8.2. Методы стимулирования повышения качества



Источник: по материалам ITU-D 2006.

Расходы на измерения QoS являются наиболее тяжелым бременем для мелких операторов, поскольку количество измерений, необходимых для получения достаточно точных результатов, не зависит от размера оператора. Таким образом, для регуляторных органов имеет смысл освободить операторов от выполнения измерений QoS в тех местах, где их клиенты составляют небольшую долю населения (например, менее 5%), как поступили в Бразилии (Anatel 2020). Тем не менее операторы, особенно те, которые стремятся увеличить свою долю рынка, могут предпочесть проводить такие измерения из-за полезной рекламы, создаваемой высокими результатами испытаний.

Если мелкие операторы не освобождены от выполнения измерений QoS для регуляторного органа, они все же могут быть освобождены от необходимости полностью соблюдать все требования. В частности, они могут быть освобождены от штрафов, даже если от них по-прежнему требуется выполнение плана повышения качества. Это согласуется с мнением, что меры по обеспечению соблюдения требований должны быть пропорциональными и адаптивными, как указано в Рекомендации МСЭ-Т E.805 (МСЭ-Т 2019a).

Обзор достигнутых результатов

При рассмотрении контроля QoS с точки зрения его целей следует учитывать изменения конъюнктуры рынка в течение анализируемого периода, а также изменения в QoS. Например:

- параметры, которые больше не важны, можно отбросить;
- если конкуренция становится достаточно сильной, целевые значения и освобождения от контроля QoS для мелких операторов можно отменить;
- если смартфоны становятся широко доступными, в контроле QoS большую роль может играть краудсорсинг;
- если для улучшения хороших результатов требуется больше времени, чем для улучшения плохих, продолжительность отчетных периодов можно увеличить.

Структуру контроля QoS, как правило, трудно изменить, если она указана в лицензиях, которые необходимо согласовать с несколькими операторами, или в нормативных актах, которые, прежде чем они вступят в силу, должны пройти через несколько государственных органов. Таких процессов иногда можно избежать для требований контроля QoS, согласующихся с государственной политикой и не вызывающих споров; например, такие требования могут быть указаны в планах или в открытых письмах операторам. Однако исключение таких процессов обычно ограничивает полномочия регуляторного органа – некоторые способы поощрения повышения QoS теряют свою правовую основу, так что принуждение приходится заменять убеждением.

8.2 Часть 2. Нумерация, наименование, адресация и идентификация (ННАИ)

Почему важны нумерация, наименование и адресация?

Телефонные номера были придуманы более века назад как способ однозначной идентификации адресатов телефонных вызовов. Затем их стали использовать для идентификации источников телефонных вызовов при идентификации линии вызывающего абонента (CLI). Они могут нести в себе информацию о тарифах и дополнительном контенте. В настоящее время они чаще всего используются в качестве уникальных идентификаторов при денежных переводах, передаче сообщений по технологии over-the-top (OTT), для устройств интернета вещей (IoT) и т. д. Фактически понятие "адресат" было расширено и теперь относится к людям и вещам в целом.

Дисковые номеронабиратели (dials), которые первоначально применялись для ввода номеров, давно исчезли (хотя английское слово dialling по-прежнему используется для обозначения ввода телефонного номера). Теперь сообщения часто отправляют, касаясь экрана или произнося команды; при этом отправители сообщений обычно не видят и не называют телефонные номера, но они могут по-прежнему присутствовать в списках контактов.

С 1960-х годов ресурсы нумерации, наименования, адресации и идентификации (ННАИ) претерпели эволюцию в целях удовлетворения новых требований и учета технических инноваций. Цифровая эпоха не стала исключением. Фактически развитие областей применения ресурсов ННАИ в цифровую эру не могло бы происходить без начальных эволюционных этапов.

Что такое ресурсы ННАИ?

Термин "ресурсы ННАИ" служит общим обозначением ресурсов, описанных в Рекомендациях МСЭ-Т и используемых для предоставления услуг электросвязи. В данном разделе рассматриваются три из перечисленных выше ресурсов из-за их полезности в цифровую эпоху:

- телефонные номера (Рекомендация МСЭ-Т E.164 "Международный план нумерации электросвязи общего пользования") (МСЭ-Т 2010);
- международные идентификаторы абонентов подвижной связи (Рекомендация МСЭ-Т E.212 "План международной идентификации для сетей общего пользования и абонентов") (МСЭ-Т 2016);
- идентификационные номера эмитентов (Рекомендация МСЭ-Т E.118 "Международная расчетная карточка за электросвязь") (МСЭ-Т 2006a).

Телефонные номера изначально использовались в сети для определения вызываемого абонента и маршрутизации вызова по сети между двумя фиксированными точками. Каждая из этих фиксированных точек известна оператору, и на основе этих данных оператор может взимать плату с клиента. При введении мобильности потребовалась разработка других механизмов, позволяющих определять возможность установления соединения и взимать плату. Международные идентификаторы абонентов подвижной связи (IMSI) служат средством, с помощью которого пользователю могут предоставляться услуги за пределами национальной сети, выбранной им для совершения и приема вызовов. Идентификационный номер эмитента (IIN) используется для идентификации платежей за вызовы в сценарии подвижной связи. В следующих разделах основное внимание уделяется телефонным номерам, так как это наиболее заметный ресурс.

Управление ННАИ

Ответственность за управление ННАИ обычно несет администратор плана нумерации. Таким администратором может быть назначенное министерство или регуляторный орган. Круг ответственности этого органа является национальным вопросом. В некоторых случаях эту роль может взять на себя официальный национальный орган или агенты, действующие от его имени (как в некоторых странах Североамериканского плана нумерации). Осуществляя управление ННАИ, регуляторный орган может решать следующие задачи.

- **Уникальная идентификация пользователей и устройств.** Регуляторный орган, ответственный за ресурсы ННАИ, может гарантировать уникальное применение номеров как на национальном, так и на международном уровне. Другому органу может быть разрешено выдавать номера, предоставленные ему регуляторным органом, но исходным источником все равно остается регуляторный орган.
- **Оказание помощи в использовании номеров.** В идеале операторы предпочли бы иметь короткие номера со значениями, соответствующими их услугам. Регуляторный орган может сохранять номера короткими, одинаковыми по длине и простыми для понимания. Особенно важны номера служб экстренной помощи и других социально значимых служб (таких как телефон доверия); регуляторный орган может обеспечить их независимость от операторов и доступность во всех национальных сетях.
- **Исключение дефицита номеров в будущем.** Пространство нумерации – ограниченный ресурс¹¹. Если операторы будут сохранять номера, не возвращая в употребление те из них, которые больше не используются, то этот ресурс может оказаться растроченным впустую. Хотя имеющееся количество номеров может показаться достаточным, со временем их может потребоваться больше. В результате номера придется заменять более длинными, что будет сопряжено с расходами и неудобствами в процессе замены и последующими трудностями привыкания к более длинным номерам. Регуляторный орган может предотвратить потери и заранее спланировать нумерацию так, чтобы избежать дефицита, обычно без необходимости изменять уже присвоенные номера.
- **Развитие упорядоченных рынков в области связи.** Операторы могут затруднить предоставление номеров, особенно если они обладают значительным влиянием на рынке или распоряжались номерами до назначения регуляторного органа. Например, они могут накапливать неиспользуемые номера, широко рассредоточивать используемые номера по множеству блоков или продолжать присваивать старые короткие номера вместо новых, более длинных. Регуляторный орган может взять выдачу и использование номеров на себя, чтобы гарантировать их доступность для новых участников рынка и возможность для абонентов пользоваться услугами этих новых участников без необходимости изменять свои номера.

Хотя операторы и поставщики услуг присваивают абонентам индивидуальные номера, им самим номера выделяются блоками администратором плана нумерации. Администратор плана нумерации – это организация, ответственная за присвоение номеров. Первоначально эту роль играл традиционный оператор, но с введением регулирования и конкуренции она перешла к соответствующему министерству, независимому регуляторному органу или агенту (как в случае некоторых участников Североамериканского плана нумерации). Размер блока зависит от использования номеров этого блока.

Привязка людей к телефонному номеру и нежелание менять телефонные номера, чтобы воспользоваться альтернативной услугой, на ранних этапах конкуренции воспринимались как препятствие для использования альтернативных услуг. Введение переносимости номеров, возможности для потребителей менять поставщиков услуг, сохраняя свои телефонные номера, во многом помогло устранить этот барьер. В разных странах управление переносимостью номеров и механизмы ее реализации различны. В Добавлении 2 к Рекомендации МСЭ-Т E.164¹² (МСЭ-Т 2010), которое постоянно обновляется 2-й Исследовательской комиссией (ИК2) МСЭ-Т, отвечающей за эксплуатационные аспекты, включая ННАИ, определена стандартная терминология для обеспечения общего понимания различных аспектов переносимости номеров в рамках схемы нумерации по Рекомендации МСЭ-Т E.164. Определены форматы нумерации и адресации, операции по обслуживанию вызовов, архитектура сети и методы маршрутизации, которые составят альтернативные способы реализации. Также предлагается ряд примеров административных и эксплуатационных процессов, требуемых для успешной реализации переносимости номеров.

Глобальные ресурсы ННАИ

Ресурсы ННАИ, использовавшиеся для поддержки предоставления услуг до 1990-х годов, были ориентированы на национальную среду. Определенные на тот момент ресурсы распределялись и присваивались операторам косвенно Международным союзом электросвязи (МСЭ), то есть МСЭ распределял ресурсы между государствами-членами на основе правил, согласованных этими

¹¹ Предел составляет 15 цифр и указан в Рекомендации МСЭ-Т E.164.

¹² В Добавлении 2 к Рекомендации МСЭ-Т E.164 определена стандартная терминология для обеспечения общего понимания различных аспектов переносимости номеров в рамках схемы нумерации по Рекомендации МСЭ-Т E.164. Определены форматы нумерации и адресации, операции по обслуживанию вызовов, архитектура сети и методы маршрутизации, которые составят альтернативные способы реализации. Также предлагается ряд примеров административных и эксплуатационных процессов, требуемых для успешной реализации переносимости номеров.

государствами. Как следствие, правила, регулирующие эти ресурсы, были национальным делом. Однако в 1990-е годы это положение изменилось с введением международных (или присваиваемых напрямую) ресурсов.

Напрямую присваиваемые ресурсы ННАИ описаны в Рекомендациях МСЭ-Т. Первоначально они использовались для таких услуг, как бесплатный международный вызов, услуги с разделением дохода и услуги с оплатой по повышенному тарифу, но для потребителей, носящих глобальный характер, таких как крупные гостиничные сети, телефоны доверия и т. д. Таким глобальным службам присваивались собственные коды страны, и по сей день они напрямую администрируются МСЭ для поставщиков услуг и операторов. Например, международной службе бесплатного вызова (IFS) (Рекомендация МСЭ-Т E.152) (МСЭ-Т 2006b) присвоен код страны +800. Использование напрямую присваиваемых ресурсов продолжает развиваться.

Наступление цифровой эпохи

Ресурсы ННАИ сохраняют свою актуальность, несмотря на развитие самой природы электросвязи. Традиционная модель связи с использованием технологии передачи голоса (с коммутацией каналов) сменилась моделью с использованием других типов связи, помимо голосовой (с коммутацией пакетов). Изменение модели связи также подразумевает изменения в использовании ресурсов ННАИ.

Среда, в которой существуют такие ресурсы ННАИ, изменилась, отражая изменения в понимании самого термина "электросвязь". Эта среда становится все более сложной и разнообразной. В некоторых национальных системах электросвязью управляет государство; другие полностью основаны на конкуренции, когда имеется несколько поставщиков услуг и независимый регуляторный орган, или находятся в процессе перехода к такой среде. Различается даже сам подход к установлению правил, регулирующих использование ресурсов ННАИ: в одних странах государственные органы проводят проверку организаций, желающих предоставлять услуги электросвязи, и выделяют им ресурсы ННАИ, а в других требуют от таких операторов только согласия соблюдать правила. Первый случай называется режимом лицензирования, а второй – режимом общего санкционирования.

Использование ресурсов ННАИ в цифровую эпоху продолжает развиваться в контексте преобразования национальных систем, изменения самих услуг электросвязи и появления новых технологий. Эволюция использования ресурсов ННАИ в цифровую эпоху происходит с использованием предыдущих эволюционных шагов.

Влияние новых технологий

Появление новых технологий повлекло за собой создание новых услуг и возможностей, которые, в свою очередь, предъявляют новые требования к доступности и применению ресурсов ННАИ не только в целях удовлетворения новых потребностей, но и в целях использования новыми поставщиками. Такое изменение также повлияло на изменение среды, в которой существуют ресурсы ННАИ, и на способ общения потребителей.

Тенденции, возникшие в последние годы и продолжающие определять развитие ресурсов ННАИ, основаны на более широком применении информационных технологий во всех аспектах жизни людей. Таким образом более широкое использование информационных технологий отражается в постоянной потребности в ресурсах ННАИ. Между тем в сфере электросвязи преобладающее использование полностью голосовых услуг сменилось преобладающим использованием услуг передачи данных, связанных с цифровыми услугами.

Одним из видов таких услуг являются услуги over-the-top (OTT). Эти услуги появились как альтернатива традиционной голосовой связи. Некоторые службы OTT обеспечивают прямую связь по телефонному номеру в рамках услуг OTT. Это допускается условиями, с которыми соглашается потребитель (который часто их даже не читает) при первоначальной подписке на услуги OTT. Некоторые поставщики услуг OTT используют буквенные символы, так что телефонный номер для прямой связи в рамках услуг OTT не требуется.

Решение о том, как использовать телефонный номер, часто принимают не участвующие в вызове пользователи, а программное обеспечение услуг OTT в соответствии с условиями, с которыми пользователь согласился, воспользовавшись услугой. Это может привести к тому, что вызывающий абонент набирает

номер телефона, а вызываемый абонент принимает вызов через службу OTT. Этот и другие аналогичные вопросы обсуждаются в ИК2 МСЭ-T.

В службе OTT телефонные номера используются в качестве идентификаторов, а не телефонных номеров, и такие идентификаторы в приложении часто преобразуются в IP-адреса. Одна из проблем, возникающих при использовании телефонных номеров в качестве идентификаторов, заключается в том, что телефонный номер может быть переприсвоен новому абоненту, который затем регистрируется в той же службе OTT. В этом случае возникает возможность того, что новый абонент получит доступ к данным прежнего абонента.

Характеристики услуг связи развиваются, и последствия этого выходят за рамки использования ресурсов ННАИ с точки зрения коммерческих соглашений. Связь в рамках цифровых услуг, такая как межмашинное взаимодействие (M2M) и IoT, характеризуется соединениями с очень малой продолжительностью и очень короткой задержкой, а также, возможно, с большей частотой повторений по сравнению с голосовыми вызовами между людьми. Цифровые услуги используются и в качестве альтернативы традиционным услугам электросвязи. Приложения OTT легко доступны и гораздо дешевле для потребителей, хотя иногда и в ущерб качеству.

Цифровые услуги связи сказываются на доходах, которые могли бы получить операторы от оплаты каждого голосового телефонного вызова. Многие операторы меняют коммерческие соглашения по традиционным услугам голосовой связи, стремясь получать дополнительные доходы от вызовов, кроме собственно платы за услуги связи. Например, одно из новых коммерческих предложений заключается в том, что поставщики услуг межмашинного взаимодействия (M2M)/IoT предлагают предприятиям не просто услуги связи, а комплексное управленческое решение. Другой пример – попытка поставщиков традиционных услуг голосовой связи в целях конкурирования с услугами OTT воспрепятствовать внедрению процедур OTT, перейдя с оплаты за соединение на ежемесячную абонентскую плату.

Тенденция к взаимодействию старого и нового мира услуг связи для потребителей вызвала множество дискуссий. В частности обсуждаются вопросы, в какой степени такое взаимодействие может способствовать мошенничеству с применением обходных схем или может рассматриваться как развитие электросвязи. В некоторых странах услуги голосовой связи на основе OTT считаются действиями в обход сети независимо от того, связаны ли они с традиционной реализацией услуг голосовой связи или нет. Что касается ННАИ, то каково бы ни было отношение к такому взаимодействию, для его существования необходимо наличие соответствующих коммерческих соглашений и нормативно-правовой базы. Такое взаимодействие представляет собой развитие контекста, в котором используются ресурсы ННАИ. Для вызовов, исходящих от новых услуг, применяются уже используемые телефонные номера, для вызовов, адресуемых новым услугам, необходимо, чтобы новые операторы имели возможность распределять ресурсы ННАИ, которая имеется во многих юрисдикциях.

Какие инструменты может использовать регуляторный орган?

Регуляторный орган решает свои задачи, поддерживая и изменяя по мере необходимости три основных инструмента. С помощью этих инструментов он может эффективно и действенно управлять нумерацией.

- **Реестр нумерации.** В нем записано, какие блоки номеров распределены каким операторам и какие блоки доступны. Это может быть электронная таблица, содержащая список операторов, которым присвоены определенные блоки номеров (хотя простая система управления базами данных может предоставить лучшие методы анализа и пользовательские интерфейсы). Ведение реестра номеров предусматривает повседневную работу по предоставлению блоков номеров операторам и периодической проверке реестра на соответствие записям, хранящимся у операторов. В реестр номеров часто вносятся изменения, когда регуляторный орган предоставляет блоки номеров операторам, подающим заявки на них. Изменения также вносятся, когда регуляторный орган отзывает присвоенные ранее блоки номеров.
- **Правила нумерации.** Это правила и процедуры, в соответствии с которыми регуляторный орган выполняет свою роль, а также правила, которые регуляторный орган может предписать операторам. Основное внимание уделяется таким задачам регуляторного органа, как содействие конкуренции и защита прав потребителей, а также тому, какие правила могут применяться для управления использованием ресурсов ННАИ. Например, может быть указано, при каких условиях с операторов может взиматься плата за ресурсы ННАИ. Изменение правил нумерации происходит относительно

редко при пересмотре правил и процедур. Обычно изменения вносятся только после консультаций с общественностью.

- **План нумерации.** В плане нумерации указано, какие номера могут предоставляться для использования и каким способом. Это может быть таблица со списком услуг или зон набора местных номеров, которые могут быть связаны с определенными первыми цифрами и длиной номеров, а также с другими элементами, такими как национальные номера. Регуляторным органам рекомендуется публиковать национальный план нумерации и предоставлять ссылку или структуру другим государствам-членам, направляя эту информацию в МСЭ в соответствии с Рекомендацией МСЭ-Т E.129 (МСЭ-Т 2013а). Для сохранения актуальности плана нумерации следует реагировать на возникающие потребности и наблюдать за тенденциями, связанными с применениями ресурсов ННАИ, которые необходимо отразить в плане нумерации. Такой подход позволяет регуляторным органам решать задачи развития конкуренции и обеспечения достаточного количества национальных номеров без помех для использования уже присвоенных номеров. Изменение плана нумерации происходит относительно редко (возможно, когда номера впервые предоставляются операторам). Опять же, изменения могут вноситься только после консультаций с общественностью, особенно если они влекут за собой отзыв номеров, которые уже предоставлены и используются. Изменения в плане нумерации могут иметь разрушительные последствия, особенно в случае изменения уже используемых телефонных номеров, и должны рассматриваться регуляторным органом как крайняя мера. Другие меры, такие как начисление платы за использование номеров, могут помочь регуляторному органу избежать изменения номеров.

Новые виды использования несут с собой новые проблемы

Использование электросвязи для управления технологиями, например в транспортных средствах, может служить ярким примером тенденций, оказывающих влияние на ННАИ. Однако эти сохраняющиеся тенденции порождают новые проблемы, связанные с использованием ННАИ. Один из примеров – производители автомобилей, использующие возможность удаленного мониторинга и, при необходимости, управления рабочими характеристиками автомобиля. Эта возможность требует удаленного доступа для сбора данных. Также используется автомобильная система экстренных вызовов, то есть возможность в случае чрезвычайной ситуации установить связь из автомобиля, а иногда и с ним. Для этого требуется система голосовой связи между автомобилем и пунктом доступа к службам общественной безопасности (PSAP). В обоих случаях используются ресурсы ННАИ.

Еще одна проблема, связанная с автомобильной системой экстренных вызовов, – это проблема маршрутизации. Сомнительно, чтобы постоянное использование ресурсов ННАИ страны производителя автомобиля в третьей стране всегда облегчало доступ к PSAP.

В некоторых случаях при использовании автомобильной системы экстренных вызовов, например голосового вызова eCall в Европейском союзе, вызовы можно инициировать как из автомобиля, так и из центра экстренной помощи. Однако главное, что может потребоваться, – это возможность инициировать голосовой вызов eCall из автомобиля только для закрытых групп пользователей. Конечно, для других пока еще не реализованных услуг IoT может потребоваться трансляция вызовов анонимным группам (например, всем пользователям, находящимся в пределах 1 км). Номера M2M могут быть предназначены в первую очередь для передачи данных (например, в домашних системах сигнализации). Для вызовов OTT использование ННАИ должно регулироваться теми же правилами, что и использование других аналогичных номеров, когда регуляторный орган решил разрешить использование таких номеров для услуг OTT, или могут применяться особые правила, когда регуляторный орган предпочитает использовать определенный диапазон номеров, выделенный для услуг OTT.

Однако в отличие от услуг подвижной связи, когда использование ресурсов ННАИ за пределами географической юрисдикции может быть временным, использование таких ресурсов ННАИ, связанных с транспортным средством, может быть постоянным, если автомобиль экспортируется в третью страну. Чтобы гарантировать возможность использования ресурсов ННАИ в таких случаях, национальные регуляторные органы ставят в известность об этих проблемах и соответствующим образом адаптируют правила.

Экспортируемые транспортные средства – лишь один из возможных примеров. К другим возможным примерам можно отнести управление транспортными контейнерами или устройствами M2M/IoT, которым для связи требуется беспроводное соединение, таким как системы сигнализации. Существуют две проблемы для стран происхождения, чьи ресурсы ННАИ могут экспортироваться на постоянной основе.

Во-первых, необходимо обеспечить, чтобы при постоянном использовании ресурсов ННАИ за границей оставалось достаточное количество этих ресурсов для внутреннего пользования. Во-вторых, следует обеспечить, чтобы использование ресурсов за границей соответствовало национальным нормативным документам зарубежных стран.

В тех странах, где по прошествии определенного периода времени требуется прекращение постоянного использования ресурсов ННАИ страны происхождения в пределах их юрисдикции, возникают другие проблемы. Одна из таких проблем – требование замены ресурсов ННАИ страны происхождения национальными ресурсами ННАИ. Еще одна – возврат исходных ресурсов ННАИ в страну происхождения. Если замена ресурсов ННАИ возможна, то решения для их возврата в страну происхождения в настоящее время нет.

Средства управления ресурсами ННАИ также развиваются и способствуют изменению использования таких ресурсов. Развитие устройств подвижной связи, которым первоначально требовался физический модуль идентификации абонента (SIM-карта), привело к тому, что теперь можно использовать электронную, или виртуальную, версию SIM-карты. Но здесь имеются свои проблемы. Например, производителю автомобилей, экспортируемых на зарубежный рынок, в которых используются физические SIM-карты, придется понести расходы на замену этих SIM-карт, если этого требует национальное законодательство. Появилась возможность обновлять электронные SIM-карты (eSIM) по каналам беспроводной связи (OTA), но это сопряжено с дополнительными расходами. В то же время регуляторные органы могут рассматривать внедрение eSIM и использование технологии OTA как средство стимулирования конкуренции на тех рынках, где в противном случае возникли бы препятствия для конкуренции ввиду необходимости физической замены SIM-карт. С этим могут столкнуться предприятия, использующие интеллектуальные счетчики для своих клиентов и ресурсы ННАИ в области подвижной связи, если такие предприятия захотят сменить поставщика услуг связи.

Международные ресурсы ННАИ

Один из способов избежать некоторых из этих новых проблем – отказаться от использования национальных ресурсов ННАИ. В последние несколько лет растет число как традиционных, так и новых операторов и поставщиков услуг, которые хотели бы, чтобы ресурсы ННАИ напрямую распределял МСЭ. Хотя такое глобальное распределение ресурсов ННАИ решает некоторые проблемы использования национальных ресурсов за границей на постоянной основе, прямое их присвоение создает ряд своих проблем. Основная проблема, связанная с международными номерами для операторов и поставщиков услуг, заключается в том, чтобы добиться признания напрямую присвоенных ресурсов ННАИ с кодом страны в целях обеспечения маршрутизации и тарификации. Для регуляторных органов использование международных ресурсов в национальном контексте поднимает вопрос обеспечения соблюдения национальных нормативных документов. Гарантировать, что использование таких международных ресурсов будет соответствовать национальным нормативным актам и, например, не даст никаких конкурентных преимуществ, весьма затруднительно, поскольку использование этих ресурсов регулируется не национальными правилами, а Рекомендациями МСЭ-Т. Тем не менее разрешение на использование международных ресурсов в национальном контексте позволит избежать истощения национальных ресурсов ННАИ, а следовательно, обеспечить наличие национальных ресурсов в будущем. Для организации, имеющей международный ресурс ННАИ, который можно использовать в нескольких юрисдикциях, преимущество заключается, например, в том, что нужно администрировать только один диапазон номеров, а не огромное множество таких ресурсов. Правила, регулирующие использование подобных ресурсов, закреплены в Рекомендациях МСЭ-Т, утвержденных государствами-членами.

Будущие проблемы, связанные с ННАИ

Развитие ННАИ для использования в новых видах услуг продолжает события, начавшиеся более 60 лет назад. С появлением новых услуг и технологий существующие ресурсы ННАИ сохраняют свою роль. Это связано с их гибкостью и эволюцией, начавшейся в 1960-е годы, как с точки зрения использования ресурсов ННАИ, так и с точки зрения нормативно-правовой среды, в которой существуют ресурсы ННАИ. Это означает, что наступление цифровой эпохи не несет с собой резких перемен в использовании ресурсов ННАИ, а скорее является продолжением эволюции. То, как определяются, управляются и развиваются ресурсы ННАИ, обеспечило прочную основу для их дальнейшего использования в эпоху цифровых технологий.

Что может сделать регуляторный орган для решения этих проблем, связанных с ННАИ?

Например, для того чтобы оказать людям помощь в использовании номеров, регуляторный орган может:

- упростить их запоминание и набор за счет перехода к более единообразной длине номеров, не зависящей от изменений;
- сохранять простые значения номеров, так чтобы услуги различались большей частью тарифами и пунктами назначения (понятно, с учетом типа платного контента);
- помочь людям, зависящим от нескольких операторов или меняющим операторов, вынудив всех операторов использовать одни и те же короткие коды для общих сетевых услуг (таких как проверка баланса и отправка сообщений о неисправностях);
- позволить одинаково записывать и набирать номера по всей стране, отменив малоиспользуемые форматы местных номеров (например, если вызовы совершаются главным образом из подвижных сетей);
- ввести сокращенные коды для социально значимых служб (таких как телефоны доверия для детей), если существуют организации, способные предложить звонящим надлежащую поддержку;
- поощрять использование стандартных способов записи номеров (см. Рекомендацию МСЭ-Т E.123) (ITU-T 2001);
- обеспечить переносимость номеров между операторами.

Кроме того, во избежание нехватки номеров в будущем регуляторный орган может:

- гибко предоставлять национальные ресурсы ННАИ для использования в соответствии с возникающими потребностями;
- возвращать неиспользованные номера в пулы номеров для будущего распределения;
- предоставлять номера группами, кратными конкретным размерам блоков (например, 1000), и близко друг к другу, чтобы для неизвестных применений в будущем оставались большие пустые пространства;
- вести запись всех предоставленных блоков номеров и время от времени (возможно, ежегодно) сверять ее с информацией, хранимой операторами;
- время от времени (возможно, ежегодно) сравнивать прогнозы будущего спроса на номера с количеством имеющихся в наличии номеров и заранее составлять планы во избежание их нехватки.

Спрос на ресурсы ННАИ для поддержки новых и новейших услуг и технологий вряд ли снизится в краткосрочной и среднесрочной перспективе. При управлении ресурсами ННАИ, вероятно, придется столкнуться с еще более сложными проблемами. Это проблемы наличия достаточного количества ресурсов и возможности адаптировать правила, регулирующие присвоение ресурсов ННАИ, для удовлетворения потребностей рынка (в рамках ответственности за содействие конкуренции), но таким образом, чтобы обеспечить защиту прав потребителей и соблюдение национального законодательства.

Правила, регулирующие использование национальных ресурсов ННАИ, эволюционировали в соответствии с возникавшими требованиями. Хотя во многих юрисдикциях эти требования одинаковы, способ реализации (и администрирования) использования ресурсов ННАИ отражает разные национальные условия. Это остается справедливым и в цифровую эпоху.

Справочные документы

- Anatel. 2020. *Qualidade – Telefonia Móvel*. <https://www.anatel.gov.br/dados/controle-de-qualidade/controle-telefonia-movel>
- ARCEP. 2020. *Évaluation QoS et QoE et analyse comparative des réseaux mobiles au Tchad*. <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/qos/202003/Documents/1.%20QoS%20and%20QoE%20assessment%20and%20comparative%20analysis%20of%20mobile%20networks%20in%20Chad.pdf>
- CICRA. 2019. *Telecoms Customer Satisfaction in the Channel Islands 2018*. <https://www.gcra.gg/media/597877/t1370gj-telecoms-customer-satisfaction-report.pdf>
- EACO. 2017. *EACO Guidelines on Consumer Experience and Protection in Digital Financial Services*. <http://www.eaco.int/admin/docs/publications/GUIDELINE%20FOR%20CONSUMER%20QoE.pdf>
- ETSI. 2019. *Speech and Multimedia Transmission Quality (STQ); QoS Aspects for Popular Services in Mobile Networks; Part 6: Post Processing and Statistical Methods*. ETSI TS 102 250-6 V1.3.1 (2019-11). https://www.etsi.org/deliver/etsi_ts/102200_102299/10225006/01.03.01_60/ts_10225006v010301p.pdf
- Fratel. 2019. *Mesurer la performance des réseaux mobiles: couverture, qualité de service et cartes*. <https://www.fratel.org/documents/2019/10/Document-Fratel-couverture-et-qualité-de-service-mobiles.pdf>
- Fratel. 2020. *Measuring Mobile Network Performance: Coverage, Quality of Service and Maps*. <https://www.fratel.org/documents/2020/05/document-Fratel-ENG-web.pdf>
- ITU-D. 2006. *ICT Quality of Service Regulation: Practices and Proposals*. https://www.itu.int/ITU-D/treg/Events/Seminars/2006/QoS-consumer/documents/QOS_Bkgpaper.pdf
- ITU-D. 2017. *Quality of service regulation manual*. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.QOS_REG01-2017-PDF-E.pdf
- ITU-T. 1996. *Home Country Direct*. Recommendation ITU-T E.153. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=3856>
- ITU-T. 2001. *Notation for National and International Telephone Numbers, E-Mail Addresses and Web Addresses*. Recommendation ITU-T E.123. <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=E.123>
- МСЭ-Т. 2006a. *Международная расчетная карточка за электросвязь*. Рекомендация МСЭ-Т E.118. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8728>
- МСЭ-Т. 2006b. *Международная служба бесплатного вызова*. Рекомендация МСЭ-Т E.152. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8729>
- МСЭ-Т. 2007. *Принципы и методики определения и применения параметров QoS*. Рекомендация МСЭ-Т E.802. <https://www.itu.int/rec/T-REC-E.802-200702-I>
- МСЭ-Т. 2010. *Международный план нумерации электросвязи общего пользования*. Рекомендация МСЭ-Т E.164. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10688>
- ITU-T. 2011. *Quality of Service Parameters for Supporting Service Aspects*. ITU-T Recommendation E.803. <https://www.itu.int/rec/T-REC-E.803/en>
- МСЭ-Т. 2013a. *Представление национальных планов нумерации*. Рекомендация МСЭ-Т E.129. <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=E.129>
- ITU-T. 2013b. *Supplement 9 to ITU-T E.800-series Recommendations (Guidelines on Regulatory Aspects of QoS)*. ITU-T Recommendations Series E.800 Supplement 9. <https://www.itu.int/rec/T-REC-E.800SerSup9/en>
- МСЭ-Т. 2016. *План международной идентификации для сетей общего пользования и абонентов*. Рекомендация МСЭ-Т E.212. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12831>
- ITU-T. 2017. *Vocabulary for Performance, Quality of Service and Quality of Experience*. ITU-T Recommendation P.10/G.100. <https://www.itu.int/rec/T-REC-P.10/en>

- МСЭ-Т. 2018. *Статистическая основа для оценки и ранжирования контрольных показателей сквозных рабочих характеристик сети*. Рекомендация МСЭ-Т E.840. <https://www.itu.int/rec/T-REC-E.840/en>
- МСЭ-Т. 2019а. *Стратегии создания нормативно-правовой базы обеспечения качества*. Рекомендация МСЭ-Т E.805. <https://www.itu.int/rec/T-REC-E.805/en>
- МСЭ-Т. 2019б. *Мероприятия по измерению, системы мониторинга и методики формирования выборок для контроля качества обслуживания в сетях подвижной связи*. Рекомендация МСЭ-Т E.806. <https://www.itu.int/rec/T-REC-E.806/en>
- ITU-T. 2020а. *Crowdsourcing Approach for the Assessment of End-to-End QoS in Fixed and Mobile Broadband Networks*. ITU-T Recommendation E.812. <https://www.itu.int/rec/T-REC-E.812/en>
- ITU-T. 2020б. *Video Quality Assessment of Streaming Services over Reliable Transport for Resolutions up to 4K*. ITU-T Recommendation P.1204. <https://www.itu.int/rec/T-REC-P.1204/en>
- МСЭ-Т. 2020с. *Методика тестирования QoE цифровых финансовых услуг*. Рекомендация МСЭ-Т P.1502. <https://www.itu.int/rec/T-REC-P.1502/en>
- Marina, M. K., V. Radu, and K. Balampekios. 2015. "Impact of Indoor-Outdoor Context on Crowdsourcing based Mobile Coverage Analysis". AllThingsCellular '15: Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges, August 2015: 45-50. <http://doi.org/10.1145/2785971.2785976>
- Ofcom. 2016. *Digital Day 2016: Media and Communications Diary: Aged 6+ in the UK*. <http://www.digitaldayresearch.co.uk/media/1086/aged-6plus-in-the-uk.pdf>
- Ofcom. 2019. *Comparing Service Quality Research 2018: Reasons to Complain*. https://www.ofcom.org.uk/_data/assets/pdf_file/0028/145819/reason-to-complain-research-2018-chart-pack.pdf

Глава 9. Связь в чрезвычайных ситуациях



9.1 Введение

Электросвязь и информационно-коммуникационные технологии (электросвязь/ИКТ) имеют решающее значение для управления операциями в случае бедствий и для снижения риска, поскольку они используются в целях мониторинга основных опасностей и предоставления жизненно важной информации всем заинтересованным сторонам, включая наиболее уязвимые сообщества. Эффективное управление риском бедствий зависит от уровня готовности, а также от связи и обмена информацией на всех уровнях власти, внутри сообществ и между государственными и частными организациями. В этом смысле национальные планы электросвязи в чрезвычайных ситуациях (NETP) могут содержать стратегию, которая делает возможной и гарантирует доступность связи на всех четырех этапах управления рисками бедствий – смягчение последствий, обеспечение готовности, реагирование и восстановление. Реализация NETP позволяет стране минимизировать экономические потери, смягчить негативное воздействие бедствий на благосостояние населения и, прежде всего, сократить человеческие жертвы (ITU-D 2020a).

Почему важны электросвязь/ИКТ в чрезвычайных ситуациях?

Электросвязь/ИКТ приобретают все более важное значение для всех нас и выходят на первый план в борьбе с бедствиями благодаря широким возможностям, которые они открывают. Во-первых, электросвязь/ИКТ помогают осуществлять мониторинг окружающей среды и основных опасных явлений, а также анализировать информацию и данные о потенциальных бедствиях. На этапах смягчения последствий и обеспечения готовности электросвязь/ИКТ используются для реализации стратегий, технологий и процессов, позволяющих уменьшить количество жертв и материальный ущерб в случае возможных бедствий. Кроме того, они играют ключевую роль в оповещении и предупреждении населения, чтобы люди знали, как действовать в чрезвычайной ситуации. Во-вторых, на этапах реагирования и восстановления, то есть во время и после бедствия, электросвязь/ИКТ и службы радиовещания могут обеспечить функционально совместимые и непрерывные каналы связи для служб реагирования, передающих жизненно важную информацию в целях координации усилий по реагированию (ITU-D 2020a). Электросвязь/ИКТ также помогают оценить ущерб и потребности пострадавших районов и населения, определить места, где нуждаются в помощи по восстановлению, отслеживать процесс восстановления и координировать восстановительные работы, а также установить связь между пострадавшими и их друзьями и родственниками.

В случае чрезвычайной ситуации, такой как пандемия COVID-19, электросвязь/ИКТ помогают оценить воздействие вируса и ограничить его распространение, способствуя сохранению связи между людьми при их физическом дистанцировании, например, при помощи социальных сетей или новостных бюллетеней, удаленной работы, дистанционного обучения и других средств.

Используя возможности новых технологий, системы управления в чрезвычайных ситуациях становятся все более интеллектуальными, безопасными и эффективными. Особенно важными для управления операциями в случае бедствий могут оказаться машинное обучение и широкое моделирование с использованием больших данных, датчики и исполнительные механизмы в устройствах робототехники и интернета вещей (IoT) или искусственный интеллект (ИИ) и блокчейн. Эти технологии позволяют считывать, обрабатывать и передавать данные, связанные с чрезвычайными ситуациями, и оказывают персоналу служб управления в чрезвычайных ситуациях помощь в процессе принятия решений во время кризисов.

В связи с этим важно, чтобы органы, разрабатывающие планы управления в чрезвычайных ситуациях, рассматривали мультитехнологический подход, то есть учитывали все возможные зрелые и новые доступные технологии, облегчающие своевременное поступление жизненно важной информации во все учреждения и ко всем гражданам, которые участвуют в этом процессе.

Какие бывают виды опасностей?

Существуют разные виды бедствий, которые могут быть вызваны целым рядом опасных явлений, в том числе метеорологических (таких как ураганы, наводнения, штормы, засухи, оползни и т. д.), геологических (таких как землетрясения, извержения вулканов) и биологических, включая эпидемии и пандемии, или опасностей, вызванных космическими явлениями (см. рисунок 9.1).

Бедствия, вызываемые опасными природными явлениями (стихийные бедствия) могут происходить независимо от деятельности человека, поэтому можно смягчить их последствия, но их невозможно избежать.

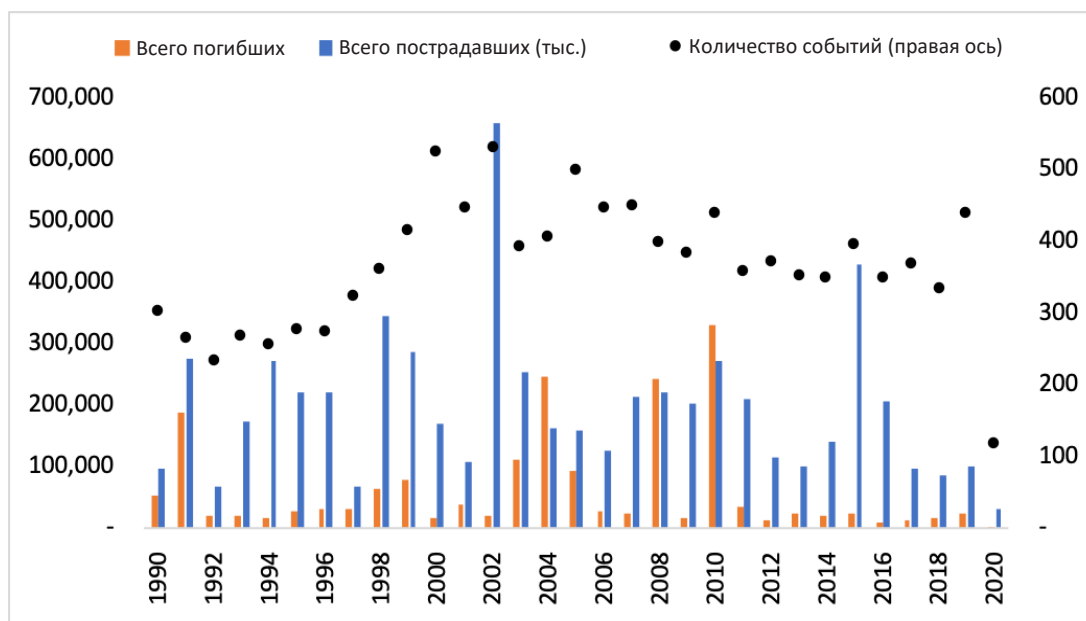
Рисунок 9.1. Виды стихийных бедствий

Геофизические	Гидрологические	Метеорологические	Климатологические	Биологические	Космические
Землетрясение	Наводнение	Бури	Засуха	Падёж скота	Влияние
Движения масс (сухих)	Оползни	Экстремальная температура	Прорыв ледникового озера	Эпидемия	Космическая погода
Вулканическая активность	Действие волн	Туман	Лесные пожары	Нашествие насекомых-вредителей	

Источник: Guha-Sapir et al. 2016.

За последние три десятилетия количество стихийных бедствий и степень их опасности колебались от года к году, как показано на рисунке 9.2. В некоторые годы отмечалось большое количество бедствий со значительными человеческими жертвами или числом пострадавших. Это относится к 2002 и 2015 годам, когда произошли соответственно 532 и 440 стихийных бедствий, от которых в 2002 году пострадало более 650 млн. человек, а в 2015 году – почти 270 млн. человек и которые привели к гибели почти 330 тыс. человек.

В то же время в некоторые годы, как можно было убедиться, корреляции между количеством событий и числом пострадавших или погибших может и не быть. Так, в 2000 году произошло более 500 стихийных бедствий, но было зарегистрировано лишь немногим более 16 тыс. смертей.

Рисунок 9.2. Частота стихийных бедствий в мире, 1990–2020 годы³

Примечание. — а. До 2 июля 2020 года.

Источник: МСЭ, на основе базы данных по чрезвычайным ситуациям (EM-DAT). <https://www.emdat.be>

Эти цифры показывают, насколько разными могут быть последствия различных стихийных бедствий для населения и в какой степени они могут колебаться от года к году. Ниже приведены примеры стихийных бедствий, происшедших за последние два десятилетия.

- В 2010 году в результате землетрясения на Гаити погибло 222 570 человек (66,7% от общего числа умерших в тот год), в то время как доля пострадавших от этого толчка (3,4 млн. человек) составляла всего 1,3% от общего числа пострадавших от стихийных бедствий за тот же год. С другой стороны, два наводнения, которые произошли в Китае в том же 2010 году (разливы рек) и в Пакистане (ливневое наводнение), унесли соответственно жизни 3676 человек (1,1% от общего числа смертей в тот год), но затронули почти 150 млн. человек, то есть 56,1% от всех пострадавших в 2010 году.
- В 2015 году от засухи, вызванной нерегулярным выпадением осадков в ряде штатов¹ Индии, пострадали 330 млн. человек (77,1% от общей численности населения пострадавших районов в тот год), но при этом смертных случаев зарегистрировано не было.
- В 2020 году пандемия COVID-19 затронула почти все страны мира. Число умерших и заболевших оценить пока трудно, но, вероятно, она окажет значительное влияние на мировое население и помимо человеческих жертв приведет к серьезным экономическим последствиям.

Стихийные бедствия разного вида могут иметь разные последствия для населения. Тем не менее их объединяет одна общая особенность — электросвязь/ИКТ играют важную роль на этапах смягчения последствий, обеспечения готовности, реагирования и восстановления процесса управления рисками бедствий. С одной стороны, даже когда стихийные бедствия, такие как наводнение и засуха, не оказывают значительного воздействия на инфраструктуру электросвязи, электросвязь/ИКТ играют ключевую роль в предупреждении или оповещении населения о приближающихся неблагоприятных погодных условиях или в координации усилий по реагированию, таких как поисково-спасательные операции или раздача продуктов питания и перемещение населения в убежища. С другой стороны, во время таких стихийных бедствий, как землетрясение, которые могут нанести серьезный ущерб инфраструктуре электросвязи/ИКТ и привести к многочисленным жертвам, пострадавшие районы могут использовать электросвязь/ИКТ, среди прочего, для передачи жизненно важной информации службам быстрого реагирования и государственным организациям, отвечающим за координацию операций по реагированию, а также при оценке ущерба или определении мест, нуждающихся в помощи по восстановлению. Наконец, при

¹ Тамилнад, Раджастхан, Джаркханд, Ассам, Андхра-Прадеш, Химачал-Прадеш, Нагаленд, Махараштра, Бихар, Мадхья-Прадеш, Чхаттисгарх, Телангана, Джаркханд и Одиша.

таких событиях, как продолжающаяся всемирная пандемия, возможности электросвязи/ИКТ также могут использоваться для облегчения социального взаимодействия, удаленной работы, обучения через онлайн-платформы и любой другой повседневной деятельности с сохранением физического дистанцирования во избежание дальнейшего распространения заболевания.

Точно так же необходимо учитывать все возможные технологии, способствующие своевременной доставке жизненно важной информации в ходе разработки NETP (то есть применять мультитехнологический подход), уместно использовать подход, основанный на учете нескольких опасностей, при разработке или планировании систем электросвязи/ИКТ для управления в чрезвычайных ситуациях, принимая во внимание все возможные виды бедствий, которые могут произойти.

Что должен делать регуляторный орган?

Регуляторные органы в области электросвязи/ИКТ выполняют важные обязанности на всех четырех этапах управления рисками бедствий. Принимая за отправную точку национальный закон или свод законов, определяющих общую долгосрочную политику в области электросвязи/ИКТ для нужд управления рисками бедствий, регуляторные органы должны издать соответствующие правила и нормативные положения для применения этих национальных законов. Такие правила и положения должны содержать подробное описание обязанностей, протоколов и стратегий, которые должна выполнять каждая заинтересованная сторона для эффективного и действенного использования услуг электросвязи/ИКТ в чрезвычайных ситуациях, их предоставления или обеспечения во время национальных бедствий. Учитывая, что эти правила и положения также распространяются на операторов электросвязи/ИКТ, важно, чтобы регуляторные органы сохраняли способность к пониманию проблем отрасли и проявляли гибкость при их решении (ITU-D 2020a).

Эти нормативные положения должны устанавливаться до наступления реальных стихийных бедствий на этапе обеспечения готовности к ним с указанием контактных данных и общих стандартных рабочих процедур, широко известных всем заинтересованным сторонам. На этапе реагирования нормативные акты должны упрощать процесс, чтобы услуги электросвязи/ИКТ были доступны как можно скорее. Поэтому регуляторным органам следует рассмотреть, например, вопросы об ускорении или упрощении выдачи временных лицензий или отказов, снижении любых барьеров для импорта/экспорта оборудования, обеспечении свободного доступа для специалистов, способных помочь в восстановлении сети, или выдаче временных разрешений на использование спектра и приостановке сборов за использование спектра/лицензии (ITU-D 2020a).

Важно учитывать, что регуляторные органы, помимо выполнения вышеупомянутых обязанностей, должны также активно содействовать или даже играть ведущую роль в разработке и реализации национального плана электросвязи в чрезвычайных ситуациях (NETP), включающего описание законов, нормативных документов, политики, а также обязанностей всех органов, связанных с услугами электросвязи/ИКТ, по управлению операциями при бедствиях. Этот план также должен быть согласован с административной структурой страны и моделью управления рисками бедствий и разработан на основе коллективного подхода с участием многих заинтересованных сторон (см. вставку 9.1).

Вставка 9.1. Этапы разработки национального плана электросвязи в чрезвычайных ситуациях

1. Проведение кабинетных исследований в целях сбора и анализа информации, касающейся существующего международного сотрудничества, заявлений правительства на высоком уровне, политики и нормативных актов в области электросвязи/ИКТ для управления операциями при бедствиях. Определение заинтересованных сторон и руководство процессом разработки и принятия NETP (ITU-D 2020a, разделы 3, 4 и 6).
2. Проведение кабинетных исследований бедствий, имевших место в прошлом, профилей опасности (ITU-D 2020a, раздел 2), существующих систем раннего предупреждения и оповещения, а также развернутых в настоящее время сетей и услуг электросвязи/ИКТ (ITU-D 2020a, раздел 5).
3. Проведение семинара-практикума в целях: а) представления общей необходимости в разработке NETP, стратегии и методики, включая вопросы развития потенциала и организации учений, а также поддержки людей с особыми потребностями (ITU-D 2020a, разделы 7 и 8); б) представления первоначальных результатов кабинетного исследования; и с) обсуждения полученных результатов и получения отзывов. На этот семинар-практикум приглашаются представители государственных организаций и частные заинтересованные стороны, связанные с управлением рисками бедствий и обеспечением связи.
4. Запрос вкладов и/или проведение частных встреч с каждой заинтересованной стороной для дальнейшего обсуждения конкретных разделов NETP, например инвентаризации сетей электросвязи/ИКТ с поставщиками услуг или конкретных нормативных положений с национальными регуляторными органами и т. д.
5. Разработка первого проекта NETP, включая стандартные рабочие процедуры, с использованием указанных выше вкладов и в соответствии с руководящими принципами, изложенным в настоящем документе.
6. Проведение второго семинара-практикума в целях представления проекта NETP, разработанного на этапе 5. Получение дополнительных отзывов и при необходимости внесение изменений в проект NETP.
7. Запрос экспертной оценки проекта NETP у специалистов в данной области. Также предложение государственным организациям и частным заинтересованным сторонам рассмотреть проект NETP и представить свои замечания.
8. Анализ замечаний по проекту NETP и внесение всех изменений, необходимых для завершения работы над NETP.
9. Периодический пересмотр и обновление NETP после каждого учения и операции с учетом извлеченных уроков или как минимум раз в три года, если учения и операции не проводятся.

Источник: ITU-D 2020a, пункт 2.4.

Что представляет собой процесс управления рисками бедствий?

Процесс управления рисками бедствий, принятый на международном уровне Управлением Организации Объединенных Наций по снижению риска бедствий (УСРБ ООН), состоит из следующих четырех этапов (ITU-D 2020a): смягчение последствий, обеспечение готовности, реагирование и восстановление, как описано ниже (см. рисунок 9.3).

Рисунок 9.3. Этапы управления рисками бедствий



Источник: ITU-D 2020a, рисунок 3.

- **Смягчение последствий.** На этом этапе предпринимаются действия, снижающие вероятность будущих бедствий или уменьшающие тяжесть их последствий. Этап смягчения последствий включает такие меры, как выявление существующих рисков, разработка оценок уязвимости, а также создание или обслуживание инфраструктуры электросвязи, необходимой для смягчения последствий возможных бедствий.
- **Обеспечение готовности.** Этот этап включает разработку и проверку планов спасения жизней и минимизации ущерба при бедствиях, обеспечение готовности людей и необходимых для реагирования на бедствия материальных средств, а также передачу предупреждений о надвигающихся стихийных бедствиях. На этом этапе осуществляется деятельность, включающая создание систем раннего предупреждения, обучение, выполнение рабочих процессов, а также разработку и реализацию планов и процедур, таких как NETP.
- **Реагирование.** Этот этап направлен на оказание экстренной помощи, стабилизацию ситуации после бедствия и снижение вероятности вторичного ущерба. Он включает, в частности, такие меры, как поисково-спасательные операции, эвакуация населения из пострадавших районов, открытие убежищ и раздача продуктов питания. На этом этапе электросвязь/ИКТ играют жизненно важную роль в обеспечении контактов между заинтересованными сторонами в процессе реагирования на чрезвычайные ситуации, особенно с учетом того, что различные организации осуществляют различную деятельность и процедуры разными способами на местном, национальном и международном уровнях.
- **Восстановление.** На этапе восстановления основное внимание уделяется оказанию необходимой помощи в целях возврата к исходным уровням безопасности и функционированию сообщества, имевшим место до бедствия. К деятельности на этом этапе относятся вывоз мусора, реконструкция инфраструктуры и восстановление работы государственного сектора. Такое восстановление и реконструкция должны охватывать инфраструктуру электросвязи/ИКТ вследствие той фундаментальной роли, которую этот сектор играет в рамках сообщества.

9.2 Этап смягчения последствий

На этом этапе роль электросвязи/ИКТ состоит в распространении информации о том, как смягчить последствия возможного бедствия, и в поддержке реализации стратегий, технологий и процессов, помогающих ослабить эти негативные последствия (ITU-D 2020a). В этом смысле регуляторный орган в области электросвязи/ИКТ играет ведущую роль в повышении устойчивости критически важной инфраструктуры электросвязи/ИКТ и в содействии принятию таких мер, как ведение периодически обновляемой базы данных, позволяющей создавать карты с указанием всех существующих сетей электросвязи/ИКТ или выполнять анализ уязвимости и рисков для всех сетей электросвязи/ИКТ. Кроме

того, нормативные акты, относящиеся к электросвязи/ИКТ, на этапе смягчения последствий должны учитывать следующие регуляторные меры (ITU-D 2020a):

- создание системы временного лицензирования как услуг электросвязи/ИКТ, так и радиочастот для оказания помощи при бедствиях;
- приостановка лицензионных сборов за временные услуги для оказания помощи при бедствиях;
- процесс отмены утверждения типа/одобрения оборудования электросвязи/ИКТ во время реагирования на бедствия;
- требование резервирования и обеспечения устойчивости сетей для операторов электросвязи/ИКТ, предоставляющих различные услуги, например услуги подвижной, фиксированной, наземной, спутниковой связи и радиовещания, включая наличие планов на случай непредвиденных обстоятельств;
- разрешение приоритетной маршрутизации вызовов;
- распределение частот для служб обеспечения общественной безопасности и оказания помощи при бедствиях (PPDR) и других служб в условиях чрезвычайных ситуаций (например, служб наземной и спутниковой связи);
- обеспечение регуляторной гибкости, например добровольное сообщение о бедствиях поставщиками услуг электросвязи/ИКТ, временное лицензирование;
- содействие тщательной оценке уязвимости сетей электросвязи/ИКТ на основе национальных оценок рисков или карт уязвимостей, разработанных соответствующей организацией;
- содействие заключению соглашений между операторами, а также между операторами и аварийными службами о совместном использовании инфраструктуры и приоритизации трафика, особенно в чрезвычайных ситуациях;
- устранение барьеров для приема и размещения людей и оборудования из других стран после бедствий.

На этапе смягчения последствий в стране должна иметься новейшая карта рисков и уязвимостей сетей электросвязи/ИКТ. Ее следует разработать на основе национальной оценки рисков или карт уязвимости для страны и для каждой опасности и каждого региона, который может подвергаться риску. Важно знать состояние систем электросвязи, в частности что необходимо операторам электросвязи для обеспечения непрерывной работы или восстановления сетей, и заранее принять соответствующие меры для поддержки способности операторов выполнять планы обеспечения непрерывности работы в случае бедствия (ITU-D 2020a).

По данным Всемирного банка, уровень воздействия разных видов опасностей на инфраструктуру электросвязи может быть различным. Например, землетрясения могут оказать сильное негативное воздействие на подводные и подземные кабели и среднее – на воздушные наземные кабели, центры обработки данных и передающие антенны беспроводной связи, как показано в таблице 9.1.

В то же время пандемия COVID-19 представляет собой бедствие, которое не наносит прямого ущерба физической инфраструктуре, но может вызывать косвенные последствия, такие как перегрузка сети из-за увеличения трафика данных как в проводных, так и в беспроводных сетях, поскольку ограничительные меры создают повышенный спрос на средства онлайн-общения. Следовательно, уровень воздействия этой опасности на инфраструктуру электросвязи в каждом отдельном случае может считаться низким или средним в зависимости от серьезности и продолжительности мер, принимаемых для борьбы с пандемией.

Таблица 9.1. Уровни воздействия опасностей на инфраструктуру электросвязи

Инфраструктура	Наводнения во внутренних и прибрежных районах	Землетрясения	Цунами	Повышение уровня моря	Высокие температуры	Дефицит воды	Сильные ветры и штормы
Подводный кабель (глубоководный)	L	H	M	L	L	L	L
Подводный кабель (прибрежный)	L	H	H	L	L	L	L
Станция выхода подводного кабеля	H	H	H	H	L	L	L
Наземные кабели (подземные)	M	H	L	L	L	L	L
Наземные кабели (воздушные)	L	M	L	L	L	L	M
Центры обработки данных	H	M	L	L	M	M	L
Передающие антенны беспроводной связи	L	M	L	L	L	L	H

Примечание. — H — высокий уровень; M — средний уровень; L — низкий уровень.

Источник: Hallegatte, Rentschler, and Rozenberg 2019, таблица 4.1.

Кроме того, на этом этапе необходимо учитывать дублирование инфраструктуры. Для повышения устойчивости сетей требуется устранить единые точки отказа, особенно в магистральных кабелях и критически важном оборудовании, таком как серверы аутентификации. Затраты можно уменьшить, если у конкурирующих между собой операторов имеются собственные отдельно маршрутизируемые и оборудованные сети, но в случае бедствия они согласны сделать их доступными друг для друга. Такие схемы требуют осторожности, поскольку могут ослабить конкуренцию, а маршруты, не пересекающиеся на одном уровне сети, легко могут совместно использовать более низкий уровень. Однако наличия отдельно маршрутизируемых сетей недостаточно: на самом деле из любой точки в любую другую точку должно вести два маршрута (за исключением проводного доступа к абоненту на последней миле). С этой целью каждая сеть, предоставляющая услуги подключения, должна обеспечивать две точки подключения к сетям, не имеющим собственных точек подключения.

Наконец, в процесс смягчения последствий также должно входить рассмотрение отказа от применения принудительных мер в области регулирования. Часто после удара стихии срочно требуются иностранные специалисты и импортное оборудование (включая заменяющее или специализированное оборудование). Поэтому до наступления бедствия важно иметь специальное законодательство, позволяющее во время катастроф ввозить в страну и своевременно устанавливать иностранное оборудование связи, а также принимать персонал, работающий со средствами ИКТ в чрезвычайных обстоятельствах. Некоторые из этих целей могут быть достигнуты путем принятия на национальном уровне *Конвенции Тампере о предоставлении телекоммуникационных ресурсов для смягчения последствий бедствий и осуществления операций по оказанию помощи* (МСЭ-D 1998). Этот международный договор направлен на содействие использованию ресурсов электросвязи на этапах реагирования и восстановления процесса управления рисками бедствий путем создания основы для международного сотрудничества между государствами, неправительственными и межправительственными организациями. Конвенция Тампере признает важность временного приостановления странами применения национального законодательства об импорте, лицензировании и использовании оборудования связи во время и после бедствий, чтобы облегчить использование средств электросвязи/ИКТ группами экстренного реагирования. Она также гарантирует юридическую неприкосновенность персонала, использующего средства ИКТ в чрезвычайных ситуациях при бедствиях. При этом Конвенция Тампере гарантирует уважение суверенитета страны, получающей помощь, предоставляя принимающему государству полный контроль над инициированием и прекращением помощи, а также право полностью или частично отклонять предлагаемую помощь (ITU-D 2020a).

9.3 Этап обеспечения готовности

На этом этапе управления рисками бедствий электросвязь/ИКТ необходимы для содействия распространению информации и предупреждений, чтобы население знало, какие действия оно должно предпринимать в чрезвычайной ситуации. Электросвязь/ИКТ также облегчают координацию действий и контакты между участниками процесса управления рисками бедствий на этом этапе. В частности, основными областями использования электросвязи/ИКТ на этом этапе являются обеспечение раннего предупреждения и оповещения, а также разработка или укрепление механизмов связи. На этапе обеспечения готовности важно развивать потенциал персонала, отвечающего за связь, путем обучения и проведения тренировочных занятий, а также разработать рабочие процессы, относящиеся к связи, путем составления письменных планов и процедур, таких как национальный план электросвязи в чрезвычайных ситуациях (ITU-D 2020a; ITU-D 2020b).

В частности, практические или тренировочные занятия должны охватывать как можно больше заинтересованных лиц из государственных, коммерческих и неправительственных организаций (НПО), поскольку они позволяют отрепетировать процедуры, выявить пробелы и проверить планы, вступающие в силу во время реальных операций реагирования на чрезвычайную ситуацию. Кроме того, на этом этапе необходимо учитывать необходимость широкого распространения предоставленной информации, поскольку она должна доводиться до сведения не только ключевых участников, но и широкой общественности. Например, можно ожидать, что поставщики услуг электросвязи сообщат своим клиентам о собственных услугах, но не обязательно обо всех доступных средствах связи. В связи с этим регуляторный орган должен потребовать, чтобы операторы электросвязи информировали о плане по электросвязи до и после бедствий не только своих сотрудников, но и потребителей. К такой информации относятся объяснения предупредительных сообщений, национальные номера телефонов экстренных служб, а также правила и условные обозначения, которые должны применяться в случае стихийных бедствий. Эта информация должна дойти до каждого дома, клуба, рабочего места, каждой школы и сельской общины, поэтому ее следует повторять для людей всех поколений и распространять через разные средства массовой информации (через устное слово, посредством плакатов, в газетах, по телевидению и радио, на веб-страницах и в социальных сетях).

Наряду с вышесказанным этап обеспечения готовности включает мониторинг и прогнозирование опасностей. Мониторинг условий окружающей среды с использованием специализированного оборудования давно является необходимой частью обеспечения готовности. В связи с этим важно учитывать, что со временем стоимость оборудования снижается, а его возможности расширяются, и сегодня в устройствах IoT имеется множество дешевых и портативных датчиков и исполнительных механизмов, которые могут питаться от солнечных панелей или долговечных батарей и взаимодействовать по беспроводным сетям большого радиуса действия. Они также хорошо подходят для применения в опасных и труднодоступных местах. Теперь имеется возможность использовать дешевые датчики, солнечные панели и беспроводные сети интернета вещей для прогнозирования опасностей, что позволяет узнать, когда опасность усугубляется, и помогает определить, следует ли выдавать предупреждения. Для распространения этих предупреждений можно использовать протокол общего оповещения (CAP), поскольку это хорошо отлаженный механизм раннего предупреждения и оповещения с использованием различных средств (WMO 2012).

9.4 Этап реагирования

Роль электросвязи/ИКТ на этом этапе жизненно важна для установления связи между участниками процесса, оказывающими экстренную помощь, а также для стабилизации ситуации после наступления бедствия и снижения вероятности вторичного ущерба.

После бедствия сети могут нуждаться в ремонте и дополнении другими элементами. Может потребоваться перевезти из относительно безопасных мест или даже импортировать запасное оборудование. Временные базовые станции подвижной (сотовой) связи, иногда с выдвижными мачтами, например "соты на колесах" (COW) и "соты на легких грузовиках" (COLT), имеют различные коммерческие применения и обычно широко используются при бедствиях (GSMA 2020). Если наземной связи недостаточно, то можно использовать спутниковые сети; в случаях когда базовые станции подвижной связи или спутниковая сеть недоступны, могут оказаться полезными беспилотные летательные аппараты (БПЛА) и станции на высотных платформах (HAPS), которые позволяют широко ретранслировать трафик и наблюдать за объектами с высоты (Li 2017).

На этом этапе электросвязь/ИКТ могут быть полезны и для оценки ущерба. Необходимо собирать, распространять и обрабатывать данные о последствиях бедствия для людей и имущества. Существующее измерительное оборудование может продолжать работать и передавать полезные сведения. Широкую картину могут дать самолеты, спутники и высотные БПЛА, предназначенные для аэрофотосъемки; дополнительную информацию могут обеспечить дроны – маловысотные БПЛА, оснащенные прожекторами и видеокамерами. Для того чтобы усилия по оказанию помощи были эффективными и действенными, особенно важно знать местоположение людей. С этой целью можно отслеживать, какие мобильные телефоны используют те или иные близлежащие базовые станции, чтобы оценить перемещения населения (Bengtsson et al. 2011). Необходимая для этого информация содержится в записях регистрации вызовов подвижной связи. В ходе поисково-спасательных работ людям и собакам могут помогать роботы, оснащенные датчиками, и дроны.

Сразу после серьезных бедствий многие национальные и международные организации собирают и анализируют информацию для планирования мер реагирования. Поэтому важно, чтобы страны разработали национальные планы управления в чрезвычайных ситуациях, а в случае электросвязи/ИКТ – национальные планы электросвязи в чрезвычайных ситуациях с использованием подхода, основанного на участии многих заинтересованных сторон, в которых учтены все национальные и международные учреждения и лица, участвующие в процессе управления в чрезвычайных ситуациях.

9.5 Этап восстановления

На этапе восстановления основное внимание уделяется такой деятельности, как вывоз мусора, восстановление работы государственных учреждений и реконструкция инфраструктуры, включая инфраструктуру электросвязи. На этом этапе сети и услуги электросвязи/ИКТ должны использоваться для содействия в оценке ущерба и потребностей пострадавших районов и населения, определении мест, нуждающихся в помощи в восстановлении, отслеживании и координации восстановительных работ (ITU-D 2020a).

После бедствия важно провести анализ извлеченных уроков для уменьшения негативных последствий в будущем. Полезны обзоры с анализом того, какие меры оказались эффективными, а какие требуют дальнейшего совершенствования на национальном и местном уровнях.

Вскоре после бедствия должна быть произведена реконструкция инфраструктуры электросвязи, при этом следует рассмотреть вопрос о создании более устойчивой инфраструктуры сетей электросвязи/ИКТ и в меру сил добавления возможности развертывания резервных сетей для подготовки к будущим бедствиям. Государственным учреждениям и организациям частного сектора также следует воспользоваться этой возможностью для восстановления соответствующей инфраструктуры электросвязи/ИКТ и в меру сил развертывания более устойчивых, эффективных и менее дорогостоящих технологий (ITU-D 2020a).

Операторы при реконструкции своих сетей могут воспользоваться этой возможностью, чтобы обеспечить удобный контроль и регулирование сетевых узлов и наблюдение за датчиками. В частности, можно установить датчики на линейно-кабельных сооружениях, чтобы сообщать такие параметры, как температура и влажность воздуха, и информировать работников о внеочередных приоритетах. В других секторах коммунальных услуг, помимо электросвязи, таких как электро- и водоснабжение, они также могут управлять исполнительными механизмами.

С другой стороны, регуляторный орган должен отслеживать усовершенствования, чтобы после восстановления инфраструктура становилась лучше, чем была. В частности, инфраструктура в целом (не обязательно сеть какого-то отдельного оператора) должна быть достаточно устойчивой, чтобы выдержать будущие бедствия, и должны быть созданы и отработаны механизмы координации.

Справочные документы

- Christian, E., 2012. "Introducing the Common Alerting Protocol (CAP)." https://etrp.wmo.int/pluginfile.php/16462/mod_resource/content/0/CAP-101-Notes.pdf
- GSMA, 2020. *Building a Resilient Industry: How Mobile Network Operators Prepare for and Respond to Natural Disasters*. London: GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/TWP5861_BuildingAResilientIndustry_v003.pdf
- Guha-Sapir, D., P. Hoyois, P. Wallemacq, and R. Below. 2016. *Annual Disaster Statistical Review 2016: The Numbers and Trends*. Brussels: CRED. http://emdat.be/sites/default/files/adsr_2016.pdf
- Hallegatte, Stephane, Jun Rentschler, and Julie Rozenberg. 2019. *Lifelines: The Resilient Infrastructure Opportunity*. Washington, DC: World Bank. <https://openknowledge.worldbank.org/handle/10986/31805>
- ITU-D. 2020a. *ITU Guidelines for National Emergency Telecommunication Plans*. Geneva: International Telecommunication Union. <https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2020/NETP-guidelines.pdf>
- ITU-D. 2020b. *Emergency Telecommunications Table-Top Simulation Guide*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Publications/2020/TTX_Guide.pdf
- МСЭ-D. 1998. *Конвенция Тампере о предоставлении телекоммуникационных ресурсов для смягчения последствий бедствий и осуществления операций по оказанию помощи*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf
- Li, A. 2017. "Alphabet Deployed Emergency LTE to Puerto Rico with Project Loon in Under a Month." 9TO5Google. October 20, 2017. <https://9to5google.com/2017/10/20/alphabet-x-project-loon-puerto-rico-live/>

Канцелярия Директора
Международный союз электросвязи (МСЭ)
Бюро развития электросвязи (БРЭ)
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: bdtdirector@itu.int
Тел.: +41 22 730 5035/5435
Факс: +41 22 730 5484

**Департамент цифровых сетей и
цифрового общества (DNS)**

Эл. почта: bdt-dns@itu.int
Тел.: +41 22 730 5421
Факс: +41 22 730 5484

**Департамент центра цифровых
знаний (DKH)**

Эл. почта: bdt-dkh@itu.int
Тел.: +41 22 730 5900
Факс: +41 22 730 5484

Канцелярия заместителя Директора и региональное присутствие
Департамент координации операций на местах (DDR)
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: bdtdeputydir@itu.int
Тел.: +41 22 730 5131
Факс: +41 22 730 5484

**Департамент партнерских отношений
в интересах цифрового развития (PDD)**

Эл. почта: bdt-pdd@itu.int
Тел.: +41 22 730 5447
Факс: +41 22 730 5484

Африка

Эфиопия

Региональное отделение МСЭ
Gambia Road
Leghar Ethio Telecom Bldg., 3rd floor
P.O. Box 60 005
Addis Ababa – Ethiopia

Эл. почта: itu-ro-africa@itu.int
Тел.: +251 11 551 4977
Тел.: +251 11 551 4855
Тел.: +251 11 551 8328
Факс: +251 11 551 7299

Камерун

Зональное отделение МСЭ
Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Эл. почта: itu-yaounde@itu.int
Тел.: + 237 22 22 9292
Тел.: + 237 22 22 9291
Факс: + 237 22 22 9297

Сенегал

Зональное отделение МСЭ
8, Route des Almadies
Immeuble Rokhaya, 3^e étage
Boîte postale 29471
Dakar – Yoff – Senegal

Эл. почта: itu-dakar@itu.int
Тел.: +221 33 859 7010
Тел.: +221 33 859 7021
Факс: +221 33 868 6386

Зимбабве

Зональное отделение МСЭ
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare – Zimbabwe

Эл. почта: itu-harare@itu.int
Тел.: +263 4 77 5939
Тел.: +263 4 77 5941
Факс: +263 4 77 1257

Северная и Южная Америка

Бразилия

Региональное отделение МСЭ
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães
Bloco E, 10^o andar, Ala Sul
(Anatel)
CEP 70070-940 Brasília – DF – Brazil

Эл. почта: itubrasilia@itu.int
Тел.: +55 61 2312 2730-1
Тел.: +55 61 2312 2733-5
Факс: +55 61 2312 2738

Барбадос

Зональное отделение МСЭ
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Эл. почта: itubridgetown@itu.int
Тел.: +1 246 431 0343
Факс: +1 246 437 7403

Чили

Зональное отделение МСЭ
Merced 753, Piso 4
Santiago de Chile – Chile

Эл. почта: itusantiago@itu.int
Тел.: +56 2 632 6134/6147
Факс: +56 2 632 6154

Гондурас

Зональное отделение МСЭ
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa – Honduras

Эл. почта: itutegucigalpa@itu.int
Тел.: +504 2235 5470
Факс: +504 2235 5471

Арабские государства

Египет

Региональное отделение МСЭ
Smart Village, Building B 147
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Эл. почта: itu-ro-arabstates@itu.int
Тел.: +202 3537 1777
Факс: +202 3537 1888

Азиатско-Тихоокеанский регион

Таиланд

Региональное отделение МСЭ
Thailand Post Training Center
5th floor
111, Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Эл. почта: ituasiapacificregion@itu.int
Тел.: +66 2 575 0055
Факс: +66 2 575 3507

Индонезия

Зональное отделение МСЭ
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110 – Indonesia

Эл. почта: ituasiapacificregion@itu.int
Тел.: +62 21 381 3572
Тел.: +62 21 380 2322/2324
Факс: +62 21 389 5521

СНГ

Российская Федерация

Региональное отделение МСЭ
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Эл. почта: itumoscow@itu.int
Тел.: +7 495 926 6070

Европа

Швейцария

Отделение для Европы МСЭ
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: euregion@itu.int
Тел.: +41 22 730 5467
Факс: +41 22 730 5484

Международный союз электросвязи
Бюро развития электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-31664-8



Опубликовано в Швейцарии
Женева, 2020 г.
Фотографии представлены: iStock