Кибербезопасность 5G

Исследовательский период 2022–2025 гг.

Вопрос 3/2

Защищенность сетей информации и связи: передовой опыт создания культуры кибербезопасности

Промежуточный итоговый документ за 2024 г.

Резюме

В настоящем промежуточном итоговом документе подчеркиваются ключевые аспекты кибербезопасности 5G в условиях усиливающихся глобальных киберугроз, когда инфраструктура электросвязи критически важна. По мере внедрения технологии 5G, совершенствования связанного с ней программного обеспечения, облачной архитектуры и расширения спектра возможностей для установления соединений появляются **новые парадигмы безопасности**. Эта технология имеет значительные преимущества, но в то же время сопряжена с новыми рисками, требующими принятия продуманных мер по обеспечению кибербезопасности для защиты от угроз.

Учитывая сложность сетей 5G, необходимы перспективные стратегии обеспечения безопасности и сотрудничества между различными заинтересованными сторонами. **Организации по разработке стандартов** (ОРС) начали стандартизацию аспектов кибербезопасности сетей 5G, что требует постоянного сотрудничества и обмена информацией во избежание дублирования усилий.

Решающее значение на всех этапах развертывания сетей имеют **упреждающие меры по обеспечению кибербезопасности**, при этом ответственность за управление рисками кибербезопасности возложена на поставщиков оборудования и операторов.

Разрабатываются **различные национальные правила и нормативные акты в области кибербезопасности 5G**. Многие страны уже разработали и внедрили свои подходы к снижению рисков безопасности и в настоящее время уделяют особое внимание их реализации и контролю за соблюдением действующих правил.

Инвестиции в образование и профессиональную подготовку имеют жизненно важное значение для удовлетворения растущего спроса на квалифицированных специалистов в области кибербезопасности.

Говоря о перспективах, отметим, что с самого начала **планирования 6G** особое внимание уделяется повышению кибербезопасности и устойчивости систем. Разработанная МСЭ "Основа IMT-2030" отражает приверженность внедрению продуманных мер по обеспечению безопасности для обеспечения дальнейшего технологического прогресса.

Введение

На последней Всемирной конференции по развитию электросвязи, состоявшейся в Кигали, Руанда, в июне 2022 года, был рассмотрен круг ведения по Вопросу 3/2 "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности" 2-й Исследовательской комиссии МСЭ-D. Одним из конкретных вопросов, определенных для дальнейшего изучения, было "обсуждение проблем и подходов к обеспечению кибербезопасности 5G".

В утвержденном круге ведения по Вопросу 3/2 признано, что угрозы кибербезопасности продолжают вызывать серьезную обеспокоенность правительств, организаций и частных лиц во всем мире. Согласно Отчету Всемирного экономического форума о глобальных рисках за 2024 год[1], во всем мире кибербезопасность занимает четвертое место среди наиболее серьезных краткосрочных рисков. Сети электросвязи, которые во многих юрисдикциях считаются важным компонентом критической национальной инфраструктуры или основных служб, уязвимы для кибератак, которые могут нарушить работу основных служб и угрожать общественной безопасности.

Внедрение технологии 5G представляет собой важное изменение в области электросвязи, поскольку эта технология обеспечивает более высокие скорости и более широкие возможности для установления соединений, что потенциально может способствовать развитию отраслей промышленности, более широкому использованию приложений интернета вещей (IoT) и внедрению новых подходов к цифровой связи. Однако в то же время сложная архитектура, обеспечивающая эти преимущества, чревата сложными проблемами в плане кибербезопасности, которые необходимо полностью понимать и принимать продуманные меры защиты.

С учетом исключительной важности защиты инфраструктуры и услуг 5G 2 мая 2024 года в рамках работы по Вопросу 3/2 2-й Исследовательской комиссией был организован продолжавшийся целый день специальный семинар-практикум, в котором приняли участие представители директивных и регуляторных органов, операторов и другие представители отрасли электросвязи, чтобы обсудить трудности в обеспечении кибербезопасности 5G, поделиться информацией о существующей практике и изучить инновационные подходы к устранению возникающих угроз. По мере развертывания сетей 5G по всему миру, создание безопасной экосистемы становится крайне важным для обеспечения целостности, доступности и конфиденциальности информации, а также для защиты инфраструктуры, которая становится основой цифровой экономики.

В настоящем отчете содержится информация о том, что обсуждалось в ходе семинара-практикума, и представлены вклады, полученные в ходе этого исследовательского цикла. Это не технический отчет о кибербезопасности 5G – его цель, скорее, состоит в том, чтобы поделиться соображениями и информацией о передовой практике, которая была получена в ходе изучения данного исследуемого Вопроса и которую Члены МСЭ могут проанализировать и внедрить в своих условиях. Основное внимание в этом отчете уделяется кибербезопасности электронных сетей 5G общего пользования.

1. Появление новых парадигм безопасности сетей электросвязи в рамках 5G

Обзор кибербезопасности 5G

Технология 5G основывается на передовых программных системах, которые обеспечивают возможность простой конфигурации и массовое подключение абонентов и устройств. Эта технология позволяет передавать и получать данные с низкой задержкой в разных областях применения, таких как дополненная реальность, дистанционная хирургия и интегрированные интернет-услуги, которые зависят от эффективности и надежности сети. Одним из основных сценариев использования 5G является интернет вещей (IoT), который работает благодаря способности 5G устанавливать соединения между множеством конечных точек. Технология 5G готова коренным образом изменить ситуацию в плане установления соединений, и это также сопряжено с новыми и постоянно меняющимися рисками и проблемами в области кибербезопасности.

В отличие от предыдущих поколений беспроводных технологий, 5G представляет собой значительный сдвиг в сторону облачной архитектуры, сетей с программируемыми параметрами (SDN) и виртуализации сетевых функций (NFV). Этот сдвиг делает ситуацию в области кибербезопасности более сложной и динамичной.

Ожидается, что по мере распространения 5G инфраструктура связи также будет становиться все более привлекательной мишенью для злонамеренной кибератаки, что потребует принятия повышенных мер безопасности, которые можно адаптировать к меняющимся угрозам. Обеспечивая кибербезопасность 5G, следует сосредоточить внимание на повышении устойчивости всей экосистемы, включая инфраструктуру и приложения. Это включает в себя защиту подключенных устройств, данных и сетей от киберугроз.

Ввиду того, что разные организации используют разные определения кибербезопасности[2], важно учитывать, что в настоящем отчете термин "кибербезопасность 5G" означает кибербезопасность в контексте технологий 5G с их новыми параметрами, стандартами, технологическими функциями, которыми необходимо надлежащим образом управлять для защиты всей цифровой экосистемы и обеспечения киберустойчивости.

[1] WEF_The_Global_Risks_Report_2024.pdf (weforum.org).

[2] https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

МСЭ определяет кибербезопасность в Рекомендации X.1205 Сектора стандартизации электросвязи (МСЭ-Т) как "*набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее:*

- доступность;
- целостность, которая может включать аутентичность и неотказуемость;
- конфиденциальность"[3].

Развертывание традиционных сетей

На начальном этапе операторы стремятся развертывать сети 5G в виде неавтономных сетей, используя существующую инфраструктуру 4G перед развертыванием автономной сквозной сети 5G[4]. Неавтономные сети 5G наследуют уязвимости 4G или даже 2G/3G, которыми необходимо соответствующим образом управлять. Для некоторых операторов это равносильно "техническому долгу": управление более старыми системами означает необходимость разработать набор стандартизованных методов обеспечения безопасности для измерения состояния безопасности компонентов инфраструктуры на разных этапах "зрелости", т. е. принадлежности к тому или иному поколению[5].

Важно подчеркнуть, что автономная сеть 5G предоставляет возможности для повышения кибербезопасности по сравнению с предыдущими поколениями мобильных технологий: она разработана таким образом, чтобы быть более безопасной, чем 4G. Улучшения были отмечены в таких аспектах, как безопасность и конфиденциальность абонентов, сеть радиодоступа (RAN), безопасность базовой сети и роуминга[6, 7].

2. Работа многочисленных ОРС в области стандартов обеспечения безопасности 5G и необходимость ОРС прилагать согласованные усилия по взаимодействию и избежанию дублирования работы

Активное участие ОРС в обеспечении кибербезопасности 5G

Из-за сложности технологий 5G и связанных с ней проблем не существует какой-то одной организации по разработке стандартов (ОРС), которая обладала бы исключительными полномочиями в области кибербезопасности 5G. Во избежание дублирования были разработаны механизмы обмена информацией между ОРС, а также координации предложений и направлений работы.

Для того чтобы помочь сопоставить виды деятельности этих различных организаций и определить направление деятельности по стандартизации в области безопасности 5G в рамках МСЭ-Т, 17-я Исследовательская комиссия (ИК17) подготовила технический отчет, в котором приведены существующие стандарты, в том числе те, которые находятся в стадии разработки в ОРС, и указано, как они применяются в отношении сетей 5G[8]. В отчете указаны стандарты, разработанные МСЭ-Т, Проектом партнерства третьего поколения (3GPP), Европейским институтом стандартизации электросвязи (ЕТСИ) и Ассоциацией стандартов Института инженеров по электротехнике и радиоэлектронике (IEEE-SA), а также не связанные со стандартами ресурсы, имеющие отношение к кибербезопасности 5G.

Исследовательская комиссия опубликовала 11 Рекомендаций по безопасности 5G на основе вкладов, подготовленных операторами, поставщиками оборудования, производителями смартфонов, поставщиками контента и другими сторонами. Они посвящены безопасности в пяти областях: SDN-NFV, нарезка сети, мобильные устройства, управление сетью 5G и услуги 5G. ИК17 наладила связи с другими ОРС, такими как 3GPP и Целевая группа по инженерным проблемам интернета (IETF), а также с отраслевыми группами, работающими над спецификациями по вопросам стандартизации кибербезопасности 5G.

Одной из таких отраслевых групп является Ассоциация GSM (GSMA). Хотя GSMA не является органом по стандартизации, она разрабатывает спецификации путем консультаций со своими членами и взаимодействия с ОРС в целях совершенствования этих спецификаций и/или их принятия в качестве стандартов. GSMA опубликовала перечень базовых мер по обеспечению безопасности, возможность принятия которых на добровольной основе операторы подвижной связи могут рассматривать при развертывании сетей 5G[9].

Учитывая многочисленные источники информации, важной для обеспечения безопасности 5G, Европейское

---

[3] https://www.itu.int/rec/T-REC-X.1205-200804-I.

[4] Устройства, работающие в неавтономных сетях 5G, обычно подключаются к частотам 5G для передачи данных, когда требуется бóльшая пропускная способность и меньшая задержка (например, для связи между "умными" автомобилями), или для снижения энергопотребления устройств с поддержкой IoT, но по-прежнему используют сети 4G и даже 2G/3G для голосовых вызовов и SMS-сообщений. Источник: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf.

[5] Материал семинара-практикума – Maxis.

[6] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf.

[7] https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era.

[8] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf.

[9] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/.

агентство по кибербезопасности (ENISA) опубликовало единый репозиторий технических мер безопасности сетей 5G, известный как Матрица мер безопасности 5G[10]. В настоящее время этот репозиторий опубликован в виде электронной таблицы, но агентство также разрабатывает веб-инструмент для повышения удобства использования.

По мере того, как сети электросвязи становятся все более сложными и происходит конвергенция с IP-сетями, тем или иным ОРС все труднее претендовать на то, чтобы отвечать за стандарты в конкретной области. Это повышает риск частичного совпадения и дублирования выполняемых функций, поэтому взаимодействие и обмен информацией между ОРС становятся еще более важными.

Включение стандартов в обязательные нормативные требования

Стандарты помогают обеспечить функциональную совместимость технологий и способствуют тому, чтобы инновации быстрее появлялись на глобальных рынках. Стандарты кибербезопасности могут определять согласованный общий уровень безопасности, отражающий примеры универсального передового опыта. Стандарты являются результатом процессов согласования на основе консенсуса. Устанавливаемые в результате стандарты могут быть обязательными, однако в большинстве случаев они таковыми не являются, что дает поставщикам и операторам бóльшую гибкость при принятии решений о развертывании систем. В некоторых случаях, когда требования того или иного технического стандарта включаются в национальные технические регламенты, стандарты могут приобретать обязательный характер. Национальные стратегии кибербезопасности 5G должны представлять собой баланс между мировой передовой практикой и местными эксплуатационными реалиями. Как правило, национальные нормативные требования должны основываться на согласованных международных стандартах, адаптированных к местным условиям и потребностям, чтобы обеспечить успешное развертывание 5G и кибербезопасность сетей.

3. Необходимость дополнения стандартов и спецификаций упреждающими мерами кибербезопасности на различных этапах развертывания сети

Соображения безопасности на уровне поставщика оборудования

Стандарты и спецификации являются лишь одним из компонентов обеспечения кибербезопасности 5G. Уровень безопасности сетей 5G определяется тем, как поставщики оборудования и операторы применяют эти стандарты и адаптируют их. Компания Ericsson взяла на вооружение комплексный подход к обеспечению безопасности 5G, который предусматривает действия на четырех уровнях: стандарты, разработка продуктов поставщиками, развертывание сетей и эксплуатация сетей[11]. Компания считает, что такой комплексный подход может гарантировать принятие мер по снижению рисков так, чтобы они соответствовали взаимозависимостям между уровнями, а также конкретным потребностям на каждом уровне.

Одним из конкретных примеров мер безопасности 5G является разработанная GSMA и 3GPP Схема обеспечения безопасности сетевого оборудования (NESAS)[12], цель которой – повысить уровень безопасности оборудования для сетей подвижной связи при помощи схемы гарантирования безопасности, которая может применяться во всем мире. Основу этой схемы составляет внутренний аудит, проводимый независимыми экспертами и представляющий собой оценку процессов поставщиков в сочетании с оценкой продукта, что обеспечивает аккредитацию. Эта схема призвана снизить нагрузку на поставщиков сетевого оборудования, связанную с проведением тестирования на предмет безопасности, поскольку эти поставщики, как правило, действуют в глобальном масштабе. Ведущие поставщики уже получили аккредитацию в рамках NESAS. Схема NESAS также является кандидатом на получение сертификата ЕС по кибербезопасности в 5G[13] – сертификата уровня ЕС, подтверждающего соответствие требованиям во всех странах ЕС. Эта сертификация не заменит собой существующую схему NESAS, но будет существовать наряду с ней. Очень важно разрабатывать схемы сертификации и соответствующие инициативы таким образом, чтобы они оставались гибкими и могли быстро обновляться в условиях меняющегося ландшафта угроз.

В Соединенном Королевстве Национальный центр кибербезопасности (NCSC) рекомендует использовать систему оценки поставщиков[14], которая помогает операторам оценить киберриски, связанные с использованием оборудования поставщиков.

Соображения безопасности на уровне оператора

NESAS может обеспечить определенную степень уверенности в безопасности сетевого оборудования до его развертывания. По мере развертывания и эксплуатации сетей операторам необходимо учитывать также другие соображения безопасности, например, для обнаружения атак и автоматического реагирования на них. Именно в этой области операторам следует рассмотреть возможность использования ИИ, обмена оперативной информацией об угрозах и результатах их анализа для обеспечения киберзащиты своих сетей. К преимуществам кибербезопасности 5G относятся обеспечение безопасности и возможность руководствоваться такими стратегиями, как нулевое доверие, которые улучшают

[10] https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

[11] https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security.

[12] https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/.

[13] https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.

[14] https://www.ncsc.gov.uk/report/vendor-security-assessment.

видимость состояния системы. Однако у нее есть свои проблемы: поддержание связи между различными сетями с разными уровнями безопасности, работа с устаревшими компонентами и различными типами сетей, а также сложность интегрирования ИИ в систему обеспечения безопасности. Применение строгих мер контроля доступа по принципу "наименьших привилегий" гарантирует, что различные права в отношении сети (например, права доступа к сетевым функциям, права сетевых администраторов, конфигурация виртуализации) будут сведены к минимуму. Операторам доступно множество работ, посвященных конкретным стратегиям кибербезопасности 5G[15].

Важное значение для определения фактического уровня киберриска, угрожающего сетям, имеет также тестирование работающих сетей электросвязи. Операторы могут проводить тестирование своих сетей и систем на предмет безопасности в той или иной форме – либо с использованием собственных ресурсов, либо привлекая независимых внешних подрядчиков. В Соединенном Королевстве действует TBEST – ориентированная на конкретные результаты программа тестирования на проникновение, в рамках которой имитируются методы и тактика, которые могут использовать в достаточной степени обеспеченные ресурсами лица, совершающие кибератаки. В рамках программы оценивается, насколько эффективно поставщик услуг связи способен обнаруживать такую атаку, ограничивать ее воздействие и реагировать на нее. Общая цель заключается в выявлении и устранении уязвимых мест или других слабых мест в функциях, процессах, правилах, системах или сетях поставщика, которые в совокупности могут быть использованы для получения несанкционированного доступа к критически важным системам компании до их обнаружения. Участвуя в программе TBEST на добровольной основе, поставщики услуг связи могут определить конкретные области, в которых ситуация в плане безопасности может быть улучшена, и Ofcom как регуляторный орган помогает своевременно внедрять соответствующие изменения[16].

Первостепенное значение имеет наличие серьезного экономического обоснования кибербезопасности 5G. Учитывая, что операторы хотят видеть доход от вложений в услуги 5G, соблюдение базовых мер безопасности должно быть признано обязательным и надлежащим образом закладываться в бюджет.

Архитектура Open RAN предполагает дезагрегацию сети радиодоступа (RAN) при стандартизации интерфейсов, соединяющих дезагрегированные компоненты, что позволяет строить сети с использованием оборудования от разных поставщиков.

С одной стороны, архитектура Open RAN может еще больше усложнить цепочку поставок для сетей электросвязи. Эта архитектура, позволяющая обеспечить диверсификацию поставщиков RAN, требует бóльших усилий по интеграции по всей цепочке поставок, что способно увеличить число векторов атак. С другой стороны, Open RAN делает цепочки поставок более прозрачными, улучшает обзор для операторов и позволяет им вести мониторинг рисков безопасности и обнаруживать их. Коротко говоря, он улучшает их понимание сетевой архитектуры и оборудования и делает возможным более комплексное сканирование уязвимостей и управление ими. Альянс O-RAN, основной источник спецификаций Open RAN, работает над спецификациями безопасности для архитектуры Open RAN и стремится стандартизировать эти спецификации в ETSI.

Компания NTT Docomo (Япония) является одним из операторов, внедривших архитектуру Open RAN, допускающую гибкость при выборе оборудования. Это решение вызвало вопросы с точки зрения безопасности, поскольку принято считать, что открытость означает больше возможностей для атак. Однако оператор провел сравнение между традиционной RAN и Open RAN и пришел к выводу, что разница между ними в плане безопасности незначительна[17].

4. Сети 5G и кибербезопасность в центре внимания последних инициатив в области политики и регулирования, находящихся на разных стадиях реализации

Примеры национальных правил и нормативных актов, обеспечивающих безопасность сетей 5G

В дополнение к стандартам и практике поставщиков оборудования и операторов, страны могут принять решение разработать политику и правила по обеспечению безопасности сетей 5G. Они могут принимать разные формы – от оценки поставщиков, тестирования и сертификации до выпуска руководящих указаний или требований. Хотя подходы различаются в зависимости от условий в стране, все эти инициативы направлены на снижение рисков, угрожающих безопасности 5G, в том числе в киберпространстве. Порядок реализации и механизмы контроля за соблюдением правил также следует рассматривать как часть общей системы обеспечения безопасности.

Приведенные ниже примеры дают представление о различных мерах в разных странах и текущей ситуации.

- В рамках применяемого в **Бразилии** комплексного подхода к обеспечению кибербезопасности 5G основное внимание уделяется управлению рисками совместно с операторами. В соответствии с условиями

[15] См., например, https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf и https://www.5gamericas.org/security-for-5g/.

[16] https://www.itu.int/md/D22-SG02.RGQ-C-0074/.

[17] Дополнительную информацию о безопасности Open RAN см., например: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf.

аукциона радиочастот для 5G и Регламентом кибербезопасности для сектора электросвязи[18] все операторы сетей 5G обязаны соблюдать нормативные положения, в том числе принципы, руководящие указания, и подлежат предварительному контролю для обеспечения кибербезопасности во всем секторе. Эти меры предварительного контроля включают управление кибербезопасностью, обязательное уведомление об инцидентах, обмен информацией, оценку уязвимости, отчетность о состоянии критической инфраструктуры и другие положения. Кроме того, Национальное агентство электросвязи (Anatel) Бразилии сотрудничает с академическими организациями для проведения специальных исследований в этой области[19].

- В **Соединенном Королевстве** правительство разработало систему обеспечения безопасности для операторов сетей связи общего пользования и поставщиков соответствующих услуг в соответствии с Законом о связи 2003 года с поправками, внесенными Законом о (безопасности) электросвязи 2021 года (TSA). Эта нормативная основа применима к сетям 5G и любым другим сетям: в то время как Соединенное Королевство переходит на 5G и полностью оптоволоконные сети, многие поставщики сетей внедряют в свою инфраструктуру устаревшие технологии. TSA установил новые обязательства по обеспечению безопасности для всех операторов сетей связи общего пользования[20] и наделил руководителя соответствующего министерства новыми полномочиями по разработке нормативных актов и правил, которые с тех пор разрабатываются в процессе открытых консультаций[21]. Закон также содержит положения, наделяющие Ofcom более широкими полномочиями по осуществлению мониторинга и контролю за выполнением провайдерами их новых обязанностей.
- Действующие в **Республике Корея** правила и нормативные акты в области кибербезопасности 5G считаются одними из самых строгих в мире, что отражает лидирующие позиции страны в области внедрения технологии 5G. Национальное правительство, действуя через Министерство науки и ИКТ (MSIT) и Корейское агентство по интернету и безопасности (KISA), внедрило комплексную систему защиты сетей 5G. Эта система включает строгие требования к операторам связи по обеспечению кибербезопасности сетевой инфраструктуры, защите пользовательских данных и снижению рисков кибербезопасности. В правилах и нормативах подчеркивается необходимость обеспечения безопасности цепочек поставок, применения усовершенствованных стандартов шифрования и внедрения принципов конструктивной безопасности на этапе проектирования в сетевую архитектуру.

Кроме того, Республика Корея сотрудничает с международными партнерами и организациями по стандартизации, чтобы обеспечить соответствие принимаемых в стране мер по обеспечению безопасности 5G нормам международной передовой практики.

- В **Индии** нормативно-техническая база для укрепления кибербезопасности 5G включает следующие компоненты:
  - директивы по вопросам национальной безопасности для сектора электросвязи, обеспечивающие устранение проблем и уязвимостей в цепочках поставок и поставщиков услуг в этом секторе;
  - тестирование и сертификация оборудования электросвязи в обязательном порядке, что обеспечивает соответствие каждой из сетевых функций 5G основным требованиям по безопасности;
  - условия лицензирования поставщиков услуг электросвязи, включающие периодическое проведение аудитов инфраструктуры электросвязи государственными органами.

Для обеспечения функционирования описанной выше нормативно-технической базы были созданы различные институциональные механизмы: Национальный центр безопасности связи (NCCS), уполномоченный разрабатывать требования/стандарты безопасности электросвязи (Требования к обеспечению безопасности систем электросвязи Индии (ITSAR)) и руководить работой связанных с этим центром лабораторий, занимающихся тестированием и сертификацией систем безопасности; сформирована Telecom-CSIRT, группа реагирования на инциденты в сфере компьютерной безопасности (CSIRT) в национальном секторе электросвязи; а также установлен ряд ориентированных на граждан механизмов для борьбы с мошенничеством, защиты прав потребителей и т.д. Что касается протоколов и стандартов безопасности, таких как 3GPP, то Индия рассматривает возможность применения спецификаций, рекомендуемых отраслевыми стандартами контроля за соблюдением установленных требований, и установления дополнительных условий лицензирования услуг электросвязи, предусматривающих регулярный аудит безопасности сетей поставщиков услуг.

- В **Объединенных Арабских Эмиратах (ОАЭ)** применяется комплексный подход к обеспечению безопасности сетей 5G, в соответствии с которым проводятся интенсивные тренировочные занятия по кибербезопасности, создан Оперативный центр национальной безопасности (SOC) для выявления угроз в режиме реального времени и реагирования на них и реализуется инициатива Cyber Pulse, в рамках которой ведется работа по повышению осведомленности и обучению персонала важнейшим методам защиты от угроз. Придается важное значение сотрудничеству и обмену информацией с международными партнерами, поставщиками, академическими организациями и другими заинтересованными сторонами в целях усиления мер кибербезопасности. Кроме того, для обеспечения соответствия требованиям во всем

[18] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740 и https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (в том числе на португальском языке).

[19] Некоторые из результатов представлены на следующей странице: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (на португальском языке).

[20] За исключением микропредприятий.

[21] https://www.legislation.gov.uk/uksi/2022/933/contents/made и https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf.

секторе электросвязи создана устойчивая система кибербезопасности, соответствующая международным стандартам, таким как стандарты ИСО и NIST. Для того чтобы укрепить уверенность потребителей и бизнеса в безопасности 5G, в стране действуют правила, процедуры и законы в области управления, обеспечивающие применение принципа безопасности по умолчанию и обязывающие поставщиков применять ответственную практику обеспечения безопасности. Наконец, страна придерживается подхода к кибербезопасности, ориентированного на интересы людей, уделяя особое внимание обучению, информированию и поддержке, способствуя расширению возможностей физических лиц и организаций для борьбы с киберугрозами и тем самым усиливая надежную защиту от потенциальных угроз в сети 5G.

- В **Зимбабве** в сфере обеспечения кибербезопасности 5G особое внимание уделяется возрастающему значению периферийных вычислений и изучению возможности внедрения технологии Open RAN, позволяющей поставщикам действовать более гибко. Хотя в Зимбабве нет специального закона о безопасности 5G, в основе применяемого в стране подхода лежит действующее законодательство о защите данных и разрабатываемый документ по управлению ИИ. В Зимбабве намерены привести свои методы обеспечения безопасности в соответствие с международными стандартами, такими как стандарты ISO/IEC 27001 и NIST, с тем чтобы новые радиоинтерфейсы 5G соответствовали установленным протоколам безопасности. Регуляторный орган почты и электросвязи Зимбабве обеспечивает соблюдение руководящих принципов безопасности и повышает осведомленность отрасли о необходимости поддержания целостности национальной инфраструктуры электросвязи.
- В апреле 2022 года в **Кении** были утверждены новая дорожная карта и стратегия развития мобильной связи 5G. В этой стратегии признается, что безопасность является важным аспектом сетевой архитектуры 5G. Непрерывное развитие подключаемых услуг и ожидаемое значительное увеличение количества и видов подключаемых устройств делают еще более важным обеспечение конфиденциальности данных, их защиту и кибербезопасность в Кении, включая способность обнаруживать угрозы, аутентифицировать пользователей и обеспечивать надлежащую работу. Технология 5G изначально обеспечивает более высокий уровень безопасности, внедряя расширенные требования безопасности на основе эволюции сетей и адаптируя опыт, накопленный в ходе развития более ранних технологий. Управление связи Кении приняло и утвердило международный стандарт, разработанный МСЭ и 3GPP, для обеспечения функциональной совместимости и безопасности мобильных систем. Управление планирует использовать опыт различных заинтересованных сторон и передовой международный опыт в области кибербезопасности для разработки технических кодексов и внедрения стандартизированного минимального контрольного списка для оценки защищенности систем, чтобы гарантировать соответствие сетей 5G современным техническим стандартам и глобальным нормам в отношении безопасности 5G.
- Всесторонне проанализировав риски кибербезопасности сетей 5G, **Европейский союз (ЕС)** разработал набор инструментов ЕС для снижения рисков[22] с целью определения общего набора мер для снижения основных рисков кибербезопасности 5G и содействия приоритизации мер в планах действий по смягчению этих рисков на общеевропейском уровне и в странах-членах. Стратегия кибербезопасности на цифровое десятилетие подчеркивает важность защиты широкополосных сетей подвижной связи следующего поколения и включает специальное приложение о дальнейших шагах по обеспечению кибербезопасности сетей 5G[23]. В рамках Системы сертификации ЕС продолжается разработка схемы сертификации кибербезопасности для 5G[24].

Задачи реализации и контроля за соблюдением

Разработка политики имеет важное значение, как и уделение внимания эффективной реализации. Для обеспечения надежной работы кибербезопасности сетей 5G необходимы механизмы отчетности, соответствие определенным стандартам и практические меры по обеспечению соблюдения политики и нормативных актов. В рамках новой системы вносятся изменения в интересах безопасности сетей электросвязи, что потребует от поставщиков услуг электросвязи постоянно осуществлять контроль за соблюдением правил и требований и, следовательно, тесно взаимодействовать с отраслью. В **Соединенном Королевстве** Ofcom использует модель контроля в рамках своего режима обеспечения безопасности сетей электросвязи и взаимодействует с регуляторными и техническими подразделениями поставщиков услуг электросвязи. Регуляторный орган считает, что реализация политики не должна ограничиваться мерами технического характера: необходимо изменить культуру и отношение поставщиков услуг электросвязи к обеспечению кибербезопасности – они должны идентифицировать те компоненты своих сетей и услуг, которые они передают на аутсорсинг, и отвечать за них. Взаимодействие на уровне руководства, а также поддержка со стороны правительства, регуляторных органов и отрасли являются необходимыми условиями достижения успеха.

В **Малайзии** правительство одобрило новый законопроект о кибербезопасности, предусматривающий создание единого ведомства, которое будет управлять всеми критическими инфраструктурами, включая электросвязь. Регуляторный орган разрабатывает набор требований к операторам, которые обязаны отчитываться о соблюдении требований безопасности. Один из действующих в стране операторов подчеркнул, что реализация новой политики может быть сложной задачей, поскольку это предполагает информирование о рисках и формулирование минимальных требований в отношении безопасности, выполнение которых требует времени,

[22] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[23] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
[24] https://certification.enisa.europa.eu/index_en.

затрат и работы, что часто противоречит интересам акционеров. Что касается операторов, у которых есть акционеры, то их структуры, правила и нормативные акты в области обеспечения безопасности могут быть разными, что чревато проблемами для служб, отвечающих за безопасность. В связи с этим при планировании новых систем безопасности необходимо вовлекать все подразделения, включая руководителей высшего звена.

5. Уделение первоочередного внимания инвестициям в образование и подготовке специалистов, способных решать сложные задачи обеспечения кибербезопасности 5G

По данным Allied Market Research[25], к 2031 году объем мирового рынка средств безопасности 5G, согласно прогнозам, достигнет 37,8 млрд. долларов США и резко вырастет спрос на специалистов в области кибербезопасности, особенно на тех, которые обладают специальными навыками и квалификацией в области защиты сетей 5G. Странам, организациям и учреждениям следует уделять первоочередное внимание подбору и обучению кадров для обеспечения кибербезопасности 5G. В настоящее время нелегко найти специалистов, обладающих необходимыми специализированными навыками; кроме того, трудно обеспечить гендерный баланс при приеме на работу. Без достаточного кадрового обеспечения переход на 5G замедлится и будет становиться все более трудным. В то время как странам следует уделять первоочередное внимание обучению в рамках национальных программ, частный сектор также может рассмотреть возможности для обучения и повышения квалификации в рамках соответствующих программ, поскольку для удовлетворения растущих потребностей необходимо будет более широкое участие всей отрасли.

Одним из примеров стран, которые решают эти кадровые проблемы, является **Турция**, где увеличен объем инвестиций в образование и профессиональную подготовку работников, способных решать сложные задачи обеспечения безопасности 5G. В этой связи ключевыми учреждениями, включая Управление информационно-коммуникационных технологий, Ближневосточный технический университет, Университет Билкент Ихсан Дограмаджи, Университет Хаджеттепе, а также операторы электросвязи Türk Telekomünikasyon A.Ş., Turkcell Iletişim Hizmetleri A.Ş. и Vodafone Telekomünikasyon A.Ş., была создана открытая тестовая площадка 5G Valley. Эта площадка важна для исследований, разработки и тестирования технологий 5G и последующих поколений и дает возможность для сотрудничества между научно-образовательными учреждениями и компаниями отрасли. Исполнительный совет 5G Valley, в состав которого входят представители вышеупомянутых учреждений, обеспечивает эффективную реализацию этой инициативы. Являясь платформой, на которой ученые, исследователи, аспиранты и стартапы могут участвовать в работе, связанной с технологиями 5G и последующих поколений, открытая тестовая площадка не только способствует инновациям, но также помогает готовить высококвалифицированных специалистов. Эта инициатива является важной частью реализуемой в Турции стратегии приоритезации и повышения безопасности сетей 5G за счет постоянного инвестирования в образование, профессиональную подготовку и исследования[26].

6. За пределами 5G: определение направлений развития кибербезопасности 6G

Хотя во многих странах и регионах сети 5G все еще находятся на стадии планирования и внедрения, внимание в рамках исследований и разработок, а также процессов стандартизации уже выходит за пределы этих сетей. В связи с этим в конце 2023 года Сектор радиосвязи МСЭ (МСЭ-R) утвердил Рекомендацию "Основа и общие задачи будущего развития IMT на период до 2030 года и далее"[27], в которой определена основа технологий, известных как 6G.

> В концепции подчеркивается, что IMT-2030, должна стать важным средством обеспечения повышенной безопасности и устойчивости. Ожидается, что она будет безопасна по умолчанию и сможет продолжать работать во время разрушительных событий природного или техногенного характера и быстро восстанавливаться после них. В документе также подтверждено, что безопасность и устойчивость систем IMT-2030 имеют решающее значение для достижения более масштабных социально-экономических целей.
>
> В контексте IMT-2030 безопасность определяется как "*обеспечение конфиденциальности, целостности и доступности информации, такой как пользовательские данные и данные плоскости сигнализации, а также защита сетей, устройств и систем от кибератак, таких как взлом, распределенный отказ в обслуживании, атака типа "человек посередине" и т. п.". Определение устойчивости сформулировано следующим образом: "способность сетей и систем корректно осуществлять свои функции после естественного или искусственного прерывания, например в результате отключения электропитания и т. п.*".

Очевидно, что концепция сетей 6G уже формируется и уже планируется начало процесса их стандартизации, причем особое внимание будет уделяться обеспечению безопасности и устойчивости в отличие от ранних стадий проектирования технологии 5G, в том числе с точки зрения стандартизации. Сравнение с видением IMT-2020 (известной как 5G), утвержденным в 2015 году[28], убедительно иллюстрирует перемену во взглядах и признание необходимости уделения надлежащего внимания вопросам кибербезопасности и киберустойчивости как одним из важнейших факторов цифровой трансформации и развития цифровой экономики.

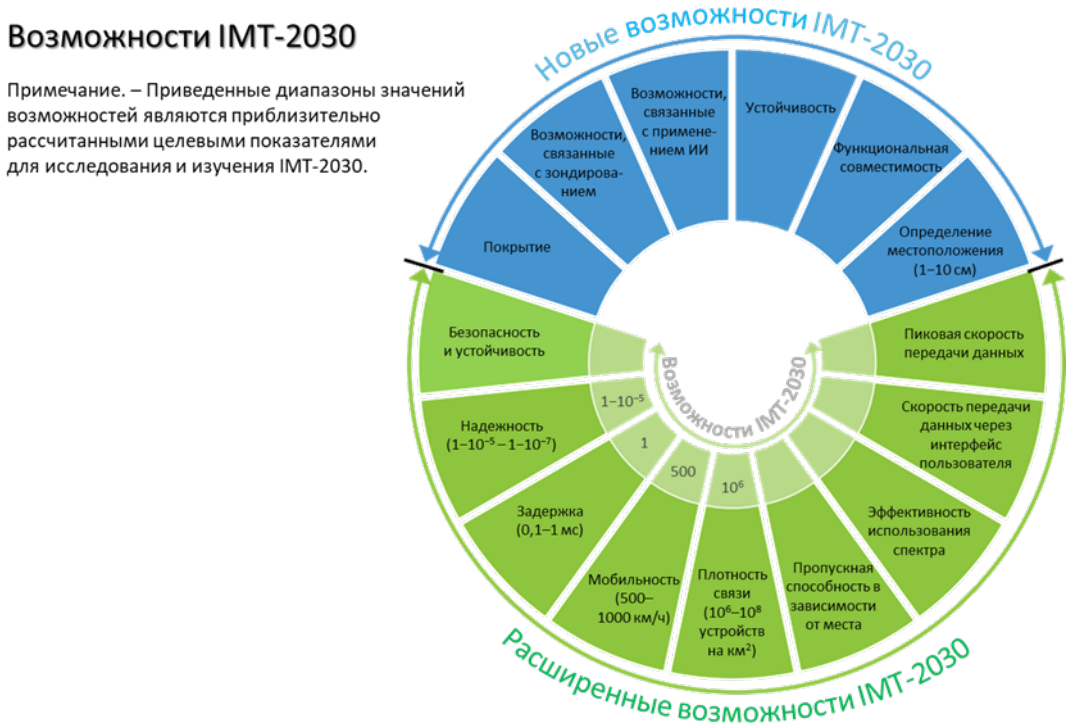
[25] https://www.alliedmarketresearch.com/5g-security-market-A12820.

[26] https://5gtrforum.org.tr/en.

[27] Рекомендация МСЭ-R M.2160 доступна по ссылке: https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en.

[28] Рекомендация МСЭ-R M. 2083 доступна по ссылке: https://www.itu.int/rec/R-REC-M.2083-0-201509-I.

Рисунок 1: Возможности IMT-2030



Источник: Рекомендация МСЭ-R M.2160

Следите за работой **2-й Исследовательской комиссии МСЭ-D по Вопросу 3/2 в исследовательском периоде 2022–2025 годов** "Защищенность сетей информации и связи: передовой опыт создания культуры кибербезопасности"

Веб-сайт, посвященный Вопросу 3/2: http://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx

Списки почтовой рассылки: d22sg3q2@lists.itu.int, подписывайтесь здесь

Веб-сайт исследовательских комиссий МСЭ-D: www.itu.int/itu-d/sites/studygroups/

Присылайте свои сообщения в порядке обратной связи на электронный адрес: devSG@itu.int,
тел: +41 22 730 5999

ITUПубликации

Опубликовано в Швейцарии, Женева, 2024 г.

Правовая оговорка: https://www.itu.int/en/publications/Pages/Disclaimer.aspx

Международный союз электросвязи
Place des Nations, CH-1211 Geneva Switzerland