Скоординированная оценка

рисков кибербезопасности сетей 5G в ЕС

Отчётный доклад

9 октября 2019 г.

Содержание

1. Введение

1.1. Сети 5G будут играть центральную роль в достижении цифровой трансформации экономики и общества ЕС. Действительно, сети 5G имеют потенциал для включения и поддержки широкого спектра приложений и функций, выходящих далеко за рамки предоставления услуг мобильной связи между конечными пользователями. Учитывая, что мировой доход от 5G в 2025 году оценивается в 225 млрд. евро, технологии и услуги 5G являются ключевым активом для способности Европы конкурировать на мировом рынке.

1.2. Таким образом, кибербезопасность сетей 5G имеет существенно важное значение для защиты наших экономик и обществ и обеспечения полного потенциала тех важных возможностей, которые они предоставят. Она также имеет решающее значение для обеспечения стратегической автономии Евросоюза.

Политический контекст и процесс

1.3. После того как 22 марта с.г. Европейский совет поддержал согласованный подход к обеспечению безопасности сетей 5G, Европейская комиссия приняла Рекомендацию Комиссии по кибербезопасности сетей 5G (далее – Рекомендация). В Рекомендации определен ряд конкретных мер, которые будут способствовать разработке единого подхода к обеспечению кибербезопасности сетей 5G. В частности, каждому государству-члену предлагается провести национальную оценку риска сетевой инфраструктуры сетей 5G.

1.4. В июле 2019 г. государства-члены представили Еврокомиссии и агентству ENISA результаты своих

национальных оценок рисков, в частности, на основе вопросника. Информация, представленная государствами-членами, позволила собрать информацию об основных активах, угрозах и уязвимостях, связанных с 5G-инфраструктурой и сценариями основных рисков, а также описать потенциальные способы, с помощью которых субъекты, создающие угрозу, могли бы использовать определенную уязвимость того или иного актива для воздействия на цели правительства.

1.5. Государствам-членам было предложено ответить на вопросник, составленный на основе результатов их национальных оценок риска кибербезопасности сетей 5G, с точки зрения правительств (т.е. законодательных/регулирующих органов), которые в случае необходимости могли бы опираться на мнения других заинтересованных сторон (включая операторов или поставщиков сетей). В работе по разработке национальных оценок рисков участвовал целый ряд ответственных субъектов в государствах-членах, таких как, в частности, органы кибербезопасности и телекоммуникаций, службы безопасности и разведывательные службы.

1.6. Согласно Рекомендации национальные оценки рисков будут служить основой для скоординированной оценки рисков Евросоюза.

1.7. С этой целью государства – члены ЕС согласовали настоящий доклад высокого уровня, который был подготовлен при поддержке Комиссии и совместно с ENISA.

1.8. В дополнение к этому докладу ENISA завершает разработку специальной карты ландшафта угроз, которая состоит из подробного анализа некоторых технических аспектов, в

частности, определения сетевых активов и угроз, конкретно влияющих на данный ландшафт.

1.9. В настоящем докладе высокого уровня излагаются основные общие выводы, вытекающие из национальных оценок рисков для сетей 5G, подготовленных каждым государством-членом. В нем освещаются моменты, имеющие особое стратегическое значение для ЕС. Доклад не ставит перед собой цели представить исчерпывающий анализ всех аспектов или типов отдельных рисков кибербезопасности, связанных с сетями 5G.

1.10. Доклад является первым шагом в процессе, направленном на обеспечение надежной и долгосрочной безопасности сетей 5G. По мере развития технологии 5G и связанных приложений и с учетом быстро меняющейся среды угроз этот отчет может пересматриваться ежегодно или при необходимости в рамках группы NIS Cooperation Group. Любые будущие обзоры должны учитывать соответствующие изменения на национальном уровне.

1.11. Скоординированная оценка рисков Евросоюза послужит основой для подготовки инструментария возможных мер по снижению рисков. Это соответствует Рекомендации, которая призывает государства-члены согласовать набор инструментов к 31 декабря 2019 г. Данная работа будет осуществляться в рамках группы NIS Cooperation Group.

Область применения: сети 5G и связанные приложения

1.12. Данный доклад берет за основу определение сетей 5G, приведенное в Рекомендации Комиссии ЕС:

«Сети 5G – это набор всех соответствующих элементов сетевой инфраструктуры для мобильных и беспроводных коммуникационных технологий, используемых для подключения и предоставления дополнительных услуг с улучшенными эксплуатационными характеристиками, такими как очень высокая скорость передачи данных и емкость, низкая задержка связи, сверхвысокая надежность или поддержка большого числа подключенных устройств. Они могут включать в себя устаревшие элементы сетей, основанные на предыдущих поколениях мобильных и беспроводных коммуникационных технологий, таких как 4G или 3G. Сети 5G следует понимать как включающие в себя все соответствующие части сети».

1.13. Сети 5G обеспечивают практически повсеместную, сверхвысокую пропускную способность и низкую задержку подключения не только для отдельных пользователей, но и для подключенных объектов. Благодаря этим техническим характеристикам ожидается, что сети 5G будут обслуживать широкий спектр приложений и секторов. Как указано в Рекомендации, они могут включать *«широкий спектр услуг, необходимых для функционирования внутреннего рынка, а также для поддержания и функционирования жизненно важных социальных и экономических функций – таких как энергетика, транспорт, банковское дело и здравоохранение, а также системы промышленного контроля. Организация демократических процессов, таких как выборы, также, как ожидается, будет все больше полагаться на цифровую инфраструктуру и сети 5G».*

1.14. В этом контексте следует отметить, что, хотя основные свойства и функции будущих сетей 5G уже хорошо известны и описаны, в частности, в стандарте, разработанном консорциумом 3GPP, технология и ее точная архитектура все еще развиваются. Кроме того, поскольку сети 5G еще не были полностью развернуты в государствах – членах ЕС, потенциальные новые возможности использования еще не включены. Это создает определенные ограничения, которые были учтены в процессе оценки рисков.

Основные технологические новинки сетей 5G

1.15. С технологической точки зрения, сети 5G будут использовать ряд новых технических возможностей, по сравнению с существующими сетями:

Переход к программному обеспечению и виртуализации с помощью технологий виртуализации программно-определяемых сетей (SDN) и сетевых функций (NFV). Это будет представлять собой значительный сдвиг от традиционной сетевой архитектуры, поскольку функции больше не будут строиться на специализированном аппаратном и программном обеспечении. Вместо этого функциональность и дифференциация будут иметь место в программном обеспечении. С точки зрения безопасности это может принести определенные преимущества, позволяя упростить обновление и исправление уязвимостей. В то же время такая повышенная зависимость от программного обеспечения и частые обновления, которых они требуют, значительно увеличат вероятность воздействия от сторонних поставщиков и важность надежности процедур управления исправлениями.

«Сетевая нарезка» позволит в высокой степени поддерживать разделение различных уровней обслуживания в одной и той же физической сети, тем самым расширяя возможности предоставления дифференцированных услуг по всей сети. «Сетевая нарезка» сети на фрагменты потребует развертывания новой базовой сети, т.е. замены базовой сети 4G на базовую сеть 5G, следуя так называемой «автономной» сетевой архитектуре.

Расширенные функциональные возможности на краях сети и менее централизованная архитектура, чем в предыдущих поколениях мобильной сети, найдут свое отражение как в расширенных возможностях подключения в сети радиодоступа, так и в поддержке Mobile Edge Computing (мобильных периферийных вычислений) и позволят сети направлять трафик к вычислительным ресурсам и сторонним службам максимально близко к конечному пользователю, обеспечивая тем самым низкое время отклика.

1.16. Эти новые функции принесут многочисленные новые проблемы безопасности. В частности, они придадут дополнительное значение сложности цепочки поставок телекоммуникационных услуг при анализе безопасности, когда различные существующие или новые игроки, такие как интеграторы, поставщики услуг или поставщики программного обеспечения, будут еще более активно участвовать в настройке и управлении ключевыми частями сети. Это, вероятно, еще больше усилит зависимость операторов мобильной связи от этих сторонних поставщиков. Кроме того, распределение обязанностей также станет более сложным, с той конкретной

проблемой, что некоторые новые игроки не знакомы с критически важными аспектами телекоммуникационных сетей. Этот источник риска станет еще более важным с появлением «сетевой нарезки», различных требований безопасности для каждого «среза» и последующим увеличением поверхности атаки.

1.17. Кроме того, некоторые чувствительные функции, выполняемые в настоящее время в физически и логически разделенном ядре, вероятно, будут перемещены ближе к краю сети, что потребует также перемещения соответствующих элементов управления безопасностью, чтобы охватить критические части всей сети, включая часть радиодоступа. При неправильном управлении эти новые функции, как ожидается, увеличат общую поверхность атаки и количество потенциальных точек входа для злоумышленников, а также увеличат вероятность злонамеренного подражания сетевых частей и функций.

1.18. В то же время технологии и стандарты 5G могут улучшить безопасность по сравнению с предыдущими поколениями мобильных сетей благодаря нескольким новым функциям безопасности, таким как более строгие процессы аутентификации в радиоинтерфейсе. Эти новые функции безопасности, однако, не все будут активированы по умолчанию в сетевом оборудовании, и поэтому их реализация будет в значительной степени зависеть от того, как операторы будут развертывать и управлять своими сетями.

1.19. Вопросы безопасности 5G все чаще рассматриваются в работе, проводимой органами по стандартизации, в частности, в рамках рабочей группы SA3 проекта 3GPP.

1.20. Рабочая группа SA3 также рассматривает законные требования к перехвату в системах 5G и намерена подготовить все спецификации, необходимые для удовлетворения этих требований. Действительно, необходим новый комплексный подход и новые методы для поддержания возможности своевременного реагирования на потребности правоохранительных и судебных органов, в частности, посредством осуществления функций законного перехвата. В этой работе также участвуют региональные органы по стандартизации.

Экосистема 5G и её развертывание в ЕС

1.21. «План действий по 5G» Евросоюза направлен на активизацию усилий ЕС по развертыванию инфраструктуры и услуг 5G на Едином цифровом рынке. В «Плане действий» изложена дорожная карта для государственных и частных инвестиций в инфраструктуру 5G на территории ЕС и намечен запуск коммерческих сетей 5G не позднее конца 2020 года. Конкретные сроки развертывания сетей 5G варьируются в зависимости от государств-членов и операторов мобильной связи. Государства-члены находятся на различных этапах своего национального процесса лицензирования соответствующих диапазонов спектра. Ряд операторов ЕС уже запустили коммерческие предложения, но крупномасштабное развертывание 5G на общеевропейской основе начнется только в 2020 году. Это также подразумевает различия в том, что операторы находятся на разных этапах процесса закупки 5G-оборудования и услуг и определения потенциальных новых требований к безопасности.

1.22. Согласно имеющейся информации о планах развертывания операторов мобильной связи некоторые из новых функций, описанных выше, будут внедрены в соответствии с поэтапным подходом. На первом этапе (очень краткосрочном) развертывание 5G будет состоять в основном из «автономных» сетей, где только сеть радиодоступа модернизирована до технологии 5G, а в остальном все зависит от существующих базовых сетей 4G, которые будут обеспечивать расширенные возможности мобильного широкополосного доступа для конечных пользователей. Это первое обновление будет основано, главным образом на уже существующей инфраструктуре, а это означает, что безопасность будущих сетей 5G может в определенной степени определяться текущим сетевым оборудованием и его конфигурацией.

1.23. На последующих этапах (краткосрочном/ среднесрочном и долгосрочном) развертывание «автономных» сетей 5G, включая функции базовой сети 5G, и внедрение ранее описанных новых функций в 1.15, которые будут лежать в основе инновационных и критически важных услуг, потребует и со временем приведет к гораздо более обширным изменениям в архитектуре сети.

1.24. Основными заинтересованными сторонами в инфраструктуре 5G-сетей являются:

Операторы мобильной сети (MNOs): предприятия, предоставляющие услуги мобильной сети пользователям, управляющим собственной сетью с помощью третьих лиц.

Поставщики операторов мобильной связи: организации, предоставляющие услуги или инфраструктуру для мобильных

операторов с целью создания и/или эксплуатации их сетей. Эта категория включает в себя телекоммуникационных производителей оборудования, других сторонних поставщиков, таких как поставщики инфраструктуры облака, системные интеграторы, подрядчики по обеспечению безопасности и техническому обслуживанию, производители оборудования для передачи.

Производители подключенных устройств и связанные с ними поставщики услуг: организации, предоставляющие объекты или услуги, которые будут подключаться к сетям 5G (например, смартфоны, подключенные транспортные средства, электронное здравоохранение) и сопутствующие сервисные компоненты 5G, размещенные в плоскости управления, как определено в Service Based Architecture или Mobile Edge Computing.

Другие заинтересованные стороны, включая поставщиков услуг и контента и конечных пользователей мобильных сетей 5G.

1.25. Все эти заинтересованные стороны имеют важное значение для обеспечения безопасности как с точки зрения содействия кибербезопасности сетей 5G, так и с точки зрения потенциальных точек входа или векторов атак. Поэтому важно оценивать риски, связанные с их положением в экосистеме 5G, чтобы обеспечить их работу надлежащим безопасным образом.

1.26. Две заинтересованные стороны имеют особое значение для кибербезопасности сетей 5G. Это операторы мобильной связи, которые играют главную роль в принятии решений, предоставляя рычаги воздействия на общую безопасную работу своих сетей, и производители телекоммуникационного оборудования, которые отвечают за предоставление

программного и аппаратного обеспечения, необходимого для работы сетей.

1.27. Операторы мобильной связи, предоставляющие услуги в ЕС, подчиняются национальному законодательству Союза и государств-членов. В частности, на них могут распространяться общие разрешения, т. е. законодательная база, обеспечивающие права на предоставление сетей или услуг электронной связи и устанавливающие конкретные секторальные обязательства, которые реализуют ответственные национальные органы власти. Операторы мобильной связи, предоставляющие услуги в ЕС, демонстрируют ряд различий в определенных аспектах, таких как право собственности, рыночные стратегии, позиционирование на рынке, а также стратегии выбора поставщиков оборудования, систем и услуг. Например, некоторые операторы развертывают и эксплуатируют свои сети с использованием нескольких поставщиков оборудования, в то время как другие, как правило, полагаются на одного поставщика для некоторых или для большинства частей своей сети.

1.28. Рынок телекоммуникационного оборудования характеризуется в основном горсткой глобальных компаний, способных поставлять крупным телекоммуникационным операторам необходимые технологии. С точки зрения доли рынка, основными поставщиками являются Huawei, Ericsson и Nokia. Среди других поставщиков – ZTE, Samsung и Cisco. Некоторые из этих поставщиков расположены в ЕС (Ericsson и Nokia), а другие – за пределами ЕС. Их корпоративное управление представляет собой заметные различия, например, с

точки зрения уровня прозрачности и типа структуры корпоративной собственности.

1.29. Кроме того, к другим важным сторонним поставщикам услуг операторов мобильной связи относится целый ряд субподрядчиков, предоставляющих различные услуги (например, управление и обслуживание сети, центры обработки данных и т.д.). Переход к сетям, основанным на программном обеспечении, и их виртуализация еще больше упростит возможность управления ключевыми сетевыми функциями такими субподрядчиками, которые могут находиться в другом государстве-члене, чем оператор мобильной связи, или в третьей стране.

1.30. Также актуален общий контекст сложного и взаимозависимого характера глобальной цепочки поставок и тот факт, что значительная часть поддержки производства многих систем осуществляется за пределами ЕС.

2. Оценка государствами – членами ЕС рисков кибербезопасности 5G

Методология

2.1. Этот документ следует подходу, изложенному в Методологии оценки рисков ISO/IEC: 27005. Он отражает оценку набора параметров:

основные типы угроз для сетей 5G;

основные субъекты угрозы;

основные активы и степень их чувствительности;

основные уязвимости;

основные риски и связанные с ними сценарии.

2.2. Документ исходит из того, что будущие варианты использования еще не полностью известны. Поэтому подход ЕС к оценке рисков кибербезопасности 5G моделируется на основе предположений о вариантах использования и возможных сценариях.

A. Угрозы и субъекты угроз

Угрозы

2.3. Развертывание сетей 5G происходит в сложном глобальном ландшафте кибернетических угроз, особенно характеризующемся увеличением числа атак по цепочке поставок.

2.4. В целом наиболее актуальными считаются угрозы, относящиеся к основным традиционным категориям угроз: это угрозы, связанные с нарушением конфиденциальности, доступности и целостности.

2.5. В частности, было установлено, что ряд сценариев угроз, нацеленных на сети 5G, основывается на:

разрыве локальной или глобальной сети 5G (доступность);

отслеживании трафика/данных в сетевой инфраструктуре 5G (конфиденциальность);

модификации или изменении маршрута трафика/данных в сетевой инфраструктуре 5G (целостность и/или конфиденциальность);

уничтожении или изменении других цифровых инфраструктур или информационных систем через сети 5G (целостность и/или доступность.

2.6. Важное отличие угроз для сетей 5G от угроз для нынешних сетей заключается в характере и интенсивности

потенциальных последствий угроз. В частности, более широкое использование экономических и социальных функций в сетях 5G может существенно ухудшить потенциальные негативные последствия сбоев. Таким образом, целостность и доступность этих сетей станут серьезной проблемой в дополнение к существующим требованиям конфиденциальности и неприкосновенности.

2.7. Таким образом, серьезность конкретных сценариев угроз для сетей 5G может варьироваться в зависимости от ряда факторов, в частности:

количества и типа затронутых пользователей;

продолжительности времени события до обнаружения или исправления;

вида оказываемых услуг (общественная безопасность, аварийные службы, здравоохранение, деятельность правительства, электроснабжение, водоснабжение и т.д.) и размер ущерба или экономических потерь;

типа поврежденной информации.

Субъекты угроз

2.8. В приведенной ниже таблице описаны различные субъекты угроз по оценке государств-членов.

Название	Описание
Не конфликт/случайность	Неконфликтные/случайные угрозы проявляются как события, являющиеся результатом человеческой ошибки, природных явлений и сбоев систем.
Отдельный хакер	Отдельные хакеры представляют собой хакеров-любителей или любителей, движимых финансовой мотивацией или стремлением к дурной славе.
Хактивистская группа	У этого субъекта угрозы есть политическая повестка дня. Его цель – либо создавать публичные атаки, которые помогают ему распространять свою пропаганду, либо наносить ущерб организациям, против которых он выступают. Конечная цель состоит в том, чтобы найти способ принести пользу своему делу или получить понимание своей проблемы.
Организованная преступная	Организованные преступные группы мотивированы

группа (ОПГ)	финансовой выгодой.
Инсайдер	В контексте безопасности сетей 5G инсайдерскую угрозу несёт инсайдер, работающий внутри оператора мобильной связи или субподрядчика. Инсайдер может работать на организованную преступную группу, хактивистскую группу или государственного деятеля, но не исключаются индивидуальные мотивы.
Государственный субъект или субъект, поддерживаемый государством	Мотивы этой категории нападающих, в первую очередь, политические.
Другие возможные субъекты: кибертеррористы и корпоративные организации	Кибертеррористы мотивированы политическими целями и, вероятно, имеют такие же возможности, как и организованная преступная группа. Корпоративные организации могут стремиться получить конкурентное преимущество в технологической области путем хищения интеллектуальной собственности (ИС), кражи конфиденциальных коммерческих данных или путем нанесения репутационного или операционного ущерба своим глобальным конкурентам посредством кибератак.

2.9. Актуальность субъектов угроз в контексте 5G была оценена путем объединения двух параметров: оценки их возможностей (ресурсов) и их намерения атаковать или пытаться атаковать сетевую инфраструктуру 5G (мотивация).

2.10. Угрозы, исходящие от государства, или субъектов, поддерживаемых государством, считаются наиболее актуальными. Такие субъекты угрозы действительно являются как наиболее серьезными, так и наиболее вероятными, поскольку они могут иметь мотивацию, намерение и, что наиболее важно, способность проводить постоянные и сложные атаки на безопасность сетей 5G.

2.11. Сочетание мотивации, намерения и высокого уровня возможностей позволяет государствам совершать нападения, которые могут быть очень сложными и оказывать серьезное воздействие на основные услуги для широкой общественности, ухудшая доверие к мобильным технологиям и операторам. Например, государства или поддерживаемые государством

субъекты могут вызвать крупномасштабное отключение или значительное нарушение телекоммуникационных услуг путем использования недокументированных функций или нападения на взаимозависимые критические инфраструктуры (например, электроснабжение).

2.12. В отношении государства и субъектов, поддерживаемых государством, особая угроза связана с кибернаступательными инициативами стран, не входящих в ЕС. Несколько государств-членов определили, что ряд стран, не входящих в ЕС, представляют собой особый вид киберугрозы для их национальных интересов, основанный на прежнем способе действий атак определенных субъектов или на существовании наступательной киберпрограммы данного третьего государства против них.

2.13. Отмечается также, что инсайдеры или субподрядчики в определенных обстоятельствах могут также считаться потенциальными субъектами, создающими угрозу, особенно если они привлекаются государствами, поскольку они могут использоваться в качестве канала для получения государством доступа к критически важным целевым активам.

2.14. Другие категории участников также могут рассматриваться как имеющие важную мотивацию для нападения на сети 5G в целях удовлетворения своих интересов, т. е. организованные преступные группы, корпоративные организации, стремящиеся получить конкурентные преимущества в технологической области посредством хищения интеллектуальной собственности (ИС) или кибертерроризма.

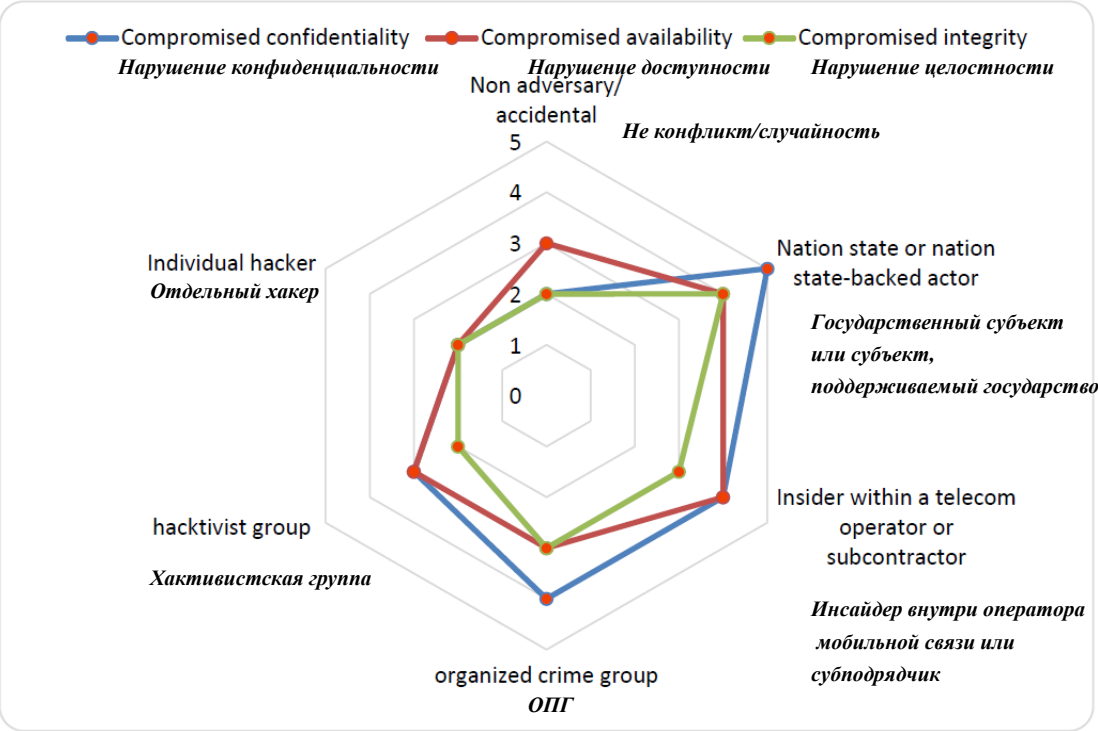

Рисунок 1. Сводный обзор категорий угроз в зависимости от субъекта угроз

2.15. Как показано на рис.1, наиболее серьезными угрозами являются нарушение конфиденциальности, доступности и целостности, поддерживаемые государством, или субъектом, поддерживаемым государством.

2.16. Другими серьезными угрозами являются:

нарушение конфиденциальности и доступности инсайдером, сотрудником оператора мобильной связи или субподрядчика;

нарушение конфиденциальности со стороны ОПГ.

B. Активы

2.17. Внедрение сетей 5G представляет для операторов гораздо большие изменения в сетевых операциях, чем любой другой из предыдущих переходов. Новые функции и процессы потребуют тщательной реорганизации существующих сетей, хотя на первых этапах они будут по-прежнему основываться на

существующих 3G- и 4G-сетях. Кроме того, технология 5G все еще находится в стадии разработки, а архитектура сетей 5G еще не установлена окончательно.

2.18. Оценка чувствительности основных сетевых активов, представленная ниже, основана на ответах государств-членов. Присвоенные рейтинги отражают мнения, выраженные подавляющим большинством государств-членов.

2.19. Сетевые активы оценивались по типам логической и функциональной частей:

Функции, которые определены в стандарте 3GPP:

основные функции, предоставляющие ряд услуг абонентам;

доступ к функциям, связывающим абонентов с их сетевым провайдером.

Функции, которые не определены в стандарте 3GPP:

транспортные и передаточные функции, обеспечивающие связь сети доступа с ядром;

межсетевые обмены, соединяющие разные сети друг с другом;

системы управления и вспомогательные службы, в частности управление сквозным шифрованием сети, а также другие менее важные службы, такие как выставление счетов или производительность сети.

Критерии оценки

2.20. Для оценки чувствительности различных активов были рассмотрены следующие основные критерии:

тип воздействия, т. е. приводит ли материализация угрозы к нарушению конфиденциальности, и/или доступности, и/или целостности сети;

масштаб воздействия, например, с точки зрения пользователей, продолжительности, количества затронутых базовых станций или ячеек, чувствительности измененной или доступной информации.

2.21. В следующей таблице представлены основные категории элементов и функций и их общий уровень чувствительности; а также перечислены ключевые элементы, определенные государствами-членами для каждой категории:

Категории элементов и функций		**Примеры ключевых элементов**
Функции ядра сети сотовой связи	Критичный	Функции аутентификации пользовательского оборудования, роуминга и управления сеансом Функции переноса данных пользовательского оборудования Управление политикой доступа Регистрация и авторизация сетевых услуг Хранение данных конечного пользователя и сетевых данных Связь со сторонними сетями мобильной связи Воздействие функций базовой сети на внешние приложения Отнесение устройств конечных пользователей к сетевым срезам (сегментам)
Управление и контроль сети NFV (MANO)	Критичный	
Системы управления и вспомогательные услуги (кроме MANO)	Умеренный/высокий	Системы управления безопасностью Биллинг и другие системы поддержки, такие как производительность сети
Сеть радиодоступа	Высокий	Базовые станции
Транспортные и трансмиссионные функции	Умеренный/высокий	Сетевое оборудование низкого уровня (маршрутизаторы, коммутаторы и т. д.) Фильтрующее оборудование (межсетевые экраны, IPS ...)
Межсетевые обмены	Умеренный/высо	IP-сети вне операторов мобильной сети

	кий	(MNO) Сетевые услуги, предоставляемые третьими сторонами

2.22. Функции ядра сети сотовой связи 5G обычно считаются критическими. Действительно, воздействие на базовую сеть может потенциально поставить под угрозу конфиденциальность, доступность и целостность всех сетевых сервисов (тогда как компрометация других компонентов может оказывать более ограниченное влияние, например, затрагивать только конкретную функцию или область). Кроме того, наиболее важные данные передаются через компоненты базовой сети.

2.23. Системы управления и вспомогательные услуги (MHO и другие системы управления и вспомогательные услуги) считаются важными, несмотря на то, что эти системы не несут трафик, поскольку они контролируют важные сетевые элементы и поэтому могут использоваться для совершения злонамеренных действий, таких как саботаж и шпионаж с серьезными последствиями. Кроме того, потеря доступности или целостности этих систем и услуг может существенно нарушить функционирование 5G-сетей.

2.24. Среди основных функций и систем управления/ вспомогательных услуг ряд элементов и функций считаются особенно важными, в частности, управление и контроль сети NFV (MANO), функции доступа и контроля ядра, функции безопасности, законный перехват функции, криптографические инфраструктуры, необходимые для настройки и эксплуатации сетей 5G, и специальные функции управления.

2.25. Функции сети доступа также оцениваются как имеющие относительно высокую чувствительность. Однако оценка степени чувствительности конкретных элементов в рамках функций доступа варьируется в зависимости от ряда факторов. Кроме того, на последующих этапах разработки 5G традиционно менее чувствительные части сети приобретают все большее значение и становятся более чувствительными, например, некоторые элементы в части радиодоступа сети, в зависимости от степени, в которой они обрабатывают пользовательские данные или выполняют интеллектуальные или чувствительные функции. Кроме того, при внедрении пограничных вычислений ожидается, что некоторые основные сетевые функции будут физически перемещены дальше в сети, ближе к узлам доступа.

2.26. Транспортные и трансмиссионные функции были оценены как умеренно высокочувствительные. Однако подобно функциям доступа оценка степени чувствительности конкретных элементов в функциях транспорта и передачи варьируется в зависимости от ряда факторов.

2.27. Функции межсетевого обмена были оценены как умеренно высокочувствительные в зависимости от их роли во взаимосвязи между операторами мобильных сетей.

Активы, кроме технических (группы пользователей, географические районы, критические инфраструктуры)

2.28. При рассмотрении ключевых активов ряд субъектов и категорий пользователей могут рассматриваться как требующие особого внимания, а именно:

Операторы основных услуг в соответствии с Директивой NIS и операторы критической инфраструктуры.

Государственные органы, правоохранительные органы, системы обеспечения общественной безопасности и оказания помощи при бедствиях (PPDR), вооруженные силы.

Ключевые сектора/предприятия, не охваченные инструкциями кибербезопасности.

Стратегические частные компании.

Районы или организации, для которых не существует резервного решения в случае сбоя сети 5G.

2.29. Кроме того, ряд государств-членов определили географические районы, которые являются особенно чувствительными, на основе анализа демографических, экономических, социальных факторов и факторов национальной безопасности. Действительно, в некоторых районах могут происходить более серьезные нарушения из-за концентрации экономической и социальной зависимости от сетевых и информационных систем (например, как в случае с умными городами) или из-за того, что в них находятся чувствительные объекты или категории пользователей.

C. Уязвимости

Уязвимости, связанные с оборудованием, программным обеспечением, процессами и политиками

2.30. Как и любая цифровая инфраструктура, сети 5G могут быть связаны с целым рядом общих технических уязвимостей, которые могут повлиять на программное или аппаратное обеспечение или возникать в результате потенциальных

недостатков в процессах безопасности любой из заинтересованных сторон. Кроме того, на ранней стадии развертывания также следует должным образом учитывать уязвимости в существующей инфраструктуре 3G и 4G.

2.31. Хотя многие из этих уязвимостей не являются специфическими для сетей 5G, их число и значимость, вероятно, будут увеличиваться с ростом 5G из-за возросшего уровня сложности технологии и будущей большей зависимости экономик и обществ от этой инфраструктуры.

2.32. В частности, поскольку 5G-сети будут в значительной степени основываться на программном обеспечении, серьезные недостатки в области безопасности, как те, что связаны со слабыми разработками программного обеспечения у поставщиков оборудования, могли бы облегчить участникам злонамеренное включение преднамеренных опорных элементов (бэкдоров) в продукты и затруднить их обнаружение. Это может увеличить вероятность их эксплуатации, что приведет к особенно серьезным и широко распространенным негативным последствиям.

2.33. Кроме того, вероятно появление новых типов технических уязвимостей, связанных с конкретными технологиями 5G, влияющих, например, на технологии, используемые в SDN и NVF, включая облачные системы, и их конфигурацию. Законные функции перехвата, позволяющие уполномоченным государственным органам получить доступ к сетям, также станут программными. Такие процессы, если они не управляются должным образом, могут быть использованы для вредоносных действий.

2.34. Другой тип уязвимости в контексте массового использования 5G по вертикали может быть связан с утечками данных между несколькими виртуальными средами или срезами (например, чтобы шпионить за предложениями/данными конкурента). Изоляция срезов является ключевой проблемой, определенной отраслью и предметом интенсивной работы сегодня.

2.35. Определенные уязвимости, связанные с процессами или настройками, считаются особенно важными в будущей среде 5G.

Для всех заинтересованных сторон, в частности, операторов мобильной связи и их поставщиков:

Нехватка специализированного и обученного персонала для обеспечения безопасности, мониторинга и обслуживания сетей 5G – быстро развивающийся ландшафт угроз и технологии, а также сложность сетей 5G приведут к увеличению потребности в специалистах по ИТ-безопасности, обладающих специальными знаниями (например, компетенцией в сфере облачной архитектуры).

Отсутствие адекватного внутреннего контроля безопасности, методов мониторинга, систем управления безопасностью и недостатки в методах управления рисками – это влияет на способность предотвращать и снижать риски безопасности для физических и ИТ-активов, которые могут быть вызваны ошибкой, аварией, стихийными бедствиями или злонамеренными действиями. Как правило, эффективное снижение рисков должно основываться на надежных и регулярных оценках рисков. Кроме того, для быстрого и точного

реагирования на возможные ситуации с ошибками или раскрытия уязвимостей необходима обновленная инвентаризация сетевых активов.

Отсутствие или неадекватность процедуры обеспечения безопасности или оперативного обслуживания, например, обновление программного обеспечения / управление исправлениями. Эта уязвимость станет гораздо более острой в 5G-сетях, учитывая гораздо более высокую частоту технического обслуживания и системных исправлений, необходимых для обеспечения безопасности и функциональности и сведения к минимуму риска для сети. Поскольку сети 5G будут охватывать более широкий круг заинтересованных сторон, включая новых (например, поставщиков платформ виртуализации и различных других сторонних поставщиков услуг), общая ответственность за обеспечение безопасности будет иметь важное значение.

Несоблюдение стандартов 3GPP или неправильное внедрение стандартов – это приведет к отсутствию адекватных базовых мер безопасности. Стандарты, касающиеся 5G, продолжают изучаться и разрабатываться. Эти стандарты будут направлены на обеспечение большей безопасности, чем предыдущие итерации мобильной беспроводной связи.

Для операторов мобильной связи:

Плохой дизайн и архитектура сети (в том числе отсутствие эффективных аварийных и непрерывных механизмов, некорректная конфигурация, например, в виртуализации или администрировании или правах доступа и т. д.) – это может значительно увеличить подверженность негативным последствиям (например, отсутствию изоляции от систем с

низким уровнем доверия, потенциально более широким масштабам нарушений безопасности).

Низкая физическая безопасность сети и ИТ-инфраструктуры: недостатки физической безопасности могут привести к недостаточной защите персонала, оборудования, программного обеспечения, сетей и данных от любых вредоносных действий и событий.

Слабые политики для локального и удаленного доступа к сетевым компонентам: сети 5G будут состоять из большого количества виртуальных устройств, к которым можно получить удаленный доступ по всей сети. Эта уязвимость становится значительно более острой в тех случаях, когда обслуживание сетей будет осуществляться сторонними поставщиками.

Отсутствие или недостаточные требования к безопасности в процессе закупок – эта уязвимость может принимать форму неадекватных стратегий выбора поставщиков или отсутствия приоритетов безопасности над другими аспектами в процессе закупок.

Неудовлетворительный процесс управления изменениями – эта уязвимость может ограничить возможность предотвращения человеческих ошибок и несанкционированных изменений конфигурации.

Специфические уязвимости для поставщиков:

2.36. Повышение роли программного обеспечения и услуг, предоставляемых сторонними поставщиками в сетях 5G, приводит к большей подверженности ряду уязвимостей, которые могут проистекать из профиля риска отдельных поставщиков.

2.37. Профили риска отдельных поставщиков могут быть оценены на основе нескольких факторов.

Вероятности вмешательства поставщика из страны, не входящей в ЕС. Это один из ключевых аспектов в оценке нетехнических уязвимостей, связанных с сетями 5G. Такие вмешательства могут быть уменьшены, но не ограничены, наличием следующих факторов:

прочная связь между поставщиком и правительством данной третьей страны;

законодательство третьей страны, особенно там, где нет законодательных или демократических сдержек и противовесов или в отсутствие соглашений о безопасности или защите данных между ЕС и данной третьей страной;

характеристики корпоративной собственности поставщика;

способность третьей страны оказывать любую форму давления, в том числе по отношению к месту изготовления оборудования.

Способность поставщика обеспечить поставку.

Общее качество продукции и методы обеспечения кибербезопасности поставщика, включая степень контроля над его собственной цепочкой поставок и вопрос о том, уделяется ли надлежащее приоритетное внимание методам обеспечения безопасности.

2.38. При оценке профиля рисков поставщика могут также учитываться уведомления, выданные органами ЕС и/или национальными органами государств-членов.

Уязвимости, обусловленные зависимостью от отдельных поставщиков

2.39. Существенные уязвимости обусловлены отсутствием разнообразия используемых оборудования и решений, как в рамках отдельных сетей, так и на национальном уровне

2.40. В пределах отдельных сетей большая степень зависимости от одного поставщика (монокультура) создает зависимость от конкретных решений и затрудняет приобретение решений у других поставщиков, особенно там, где решения не полностью совместимы.

2.41. В результате операторы из стран ЕС, которые становятся чрезмерно зависимыми от одного поставщика оборудования, подвергаются ряду рисков, вызванных тем, что этот поставщик находится под постоянным коммерческим давлением, будь то из-за коммерческого сбоя, в результате слияния или приобретения, или помещен под санкции.

2.42. На национальном уровне и уровне ЕС отсутствие разнообразия поставщиков увеличивает общую уязвимость инфраструктуры 5G, в частности, если большое количество операторов получают свои чувствительные активы от поставщика, представляющего высокую степень риска, как описано выше. Зависимость одной или нескольких сетей также существенно влияет на устойчивость в национальном и общеевропейском масштабе и создает единые точки отказа.

2.43. Кроме того, присутствие ограниченного числа поставщиков на рынке может снизить их стимулы для разработки более безопасных продуктов. Это также может оказать негативное влияние на рычаги, доступные национальным органам власти и операторам, чтобы требовать более высоких

гарантий безопасности, особенно для небольших государств-членов или операторов.

2,44. Такая подчинённость также может иметь различные последствия в зависимости от того, какие типы сетевых элементов подвержены влиянию, а также от взаимодействия различных компонентов.

D. Сценарии рисков

2.45. На основании выводов, касающихся различных параметров, изложенных в предыдущих разделах доклада, был определен ряд категорий рисков, имеющих стратегическое значение с точки зрения ЕС.

2.46. Эти риски описаны в нижеследующих пунктах и иллюстрируются конкретными сценариями, которые отражают возможные соответствующие комбинации различных параметров, описанных в предыдущих разделах настоящего доклада (угрозы, субъекты угроз, активы и уязвимости).

2.47. Эти выявленные категории рисков обладают рядом характеристик, придающих им особое стратегическое значение:

Они основаны на сценариях ключевых угроз, актуальных для всего ЕС.

Они приведут к высоким, очень высоким или потенциально системным последствиям.

Их вероятность увеличивается с развитием сетей 5G или они специфичны для сетей 5G.

2.48. Следует отметить, что указанные ниже риски и связанные с ними сценарии рисков охватывают не все существующие риски или все соответствующие комбинации параметров, а направлены на описание возможных путей атаки,

которые могут быть использованы субъектом угрозы для достижения своей цели.

I. Сценарии рисков, связанных с недостаточными мерами безопасности

2.49. Как и в случае сетей 3G и 4G, большое количество рисков возникает из-за систем, которые плохо спроектированы или плохо настроены и/или сконфигурированы, а также из-за слабых мест в мерах безопасности и процессах, применяемых операторами мобильной связи. С переходом к сетям 5G эти риски, вероятно, станут значительно более острыми из-за новых технологических характеристик этих сетей и их гораздо более высокой степени сложности. Это может еще больше усугубиться нехваткой специалистов, что также приведет к увеличению числа человеческих ошибок. Кроме того, децентрализация сетевой инфраструктуры 5G делает надежный и отказоустойчивый сервис более сложным для реализации.

В частности, риск несанкционированного доступа к важным системам уже является проблемой для управления. С внедрением сетей 5G сложные технические решения потребуют дополнительной поддержки со стороны различных типов поставщиков, которая будет предоставляться как на месте, так и через удаленный доступ. Если поставщики имеют доступ к сети, они могут манипулировать определенными функциональными возможностями, например законной функцией перехвата, или перехватывать и/или перенаправлять трафик данных, а также обходить механизмы аудита таким образом, что это нелегко обнаружить оператору.

Связанные сценарии риска:

Неверная конфигурация сетей – используя плохо настроенные системы и архитектуру, субъект состояния проникает в сеть 5G через внешние интерфейсы, что приводит к компрометации основных функций сети или к использованию узлов периферийных вычислений для нарушения конфиденциальности информации и нарушения работы распределенных служб.

Отсутствие контроля доступа – субподрядчик с правами администратора в сети выполняет неблагоприятные действия, что приводит к нарушению конфиденциальности/целостности и/или доступности. Действия субподрядчика могут быть вызваны юридическим требованием третьей страны или мошенническим поведением персонала подрядчика.

II. Сценарии риска, связанные с цепочкой поставок 5G

2.50. Существует ряд конкретных рисков безопасности, связанных с цепочкой поставок 5G. Они включают, в частности:

Неисправности или уязвимости в оборудовании, вызванные устаревшим оборудованием, неудовлетворительными процессами разработки программного обеспечения или плохим управлением уязвимостями.

Зависимость от какого-либо одного поставщика, либо на уровне отдельной сети, либо в масштабе страны или ЕС.

2.51. Низкое качество оборудования. Более высокая степень сложности сетей 5G и их более высокая зависимость от программного обеспечения и услуг сторонних поставщиков увеличивает риски, связанные с наличием значительных дефектов в поставляемом оборудовании и последующим процессом исправления. Неопознанные уязвимости являются

основной причиной потенциально необнаруженных, длительных вторжений в сети и как таковые ставят под угрозу конфиденциальность, целостность и доступность сетей 5G. В этом контексте значительные уязвимости могут быть вызваны плохо написанным кодом и плохим процессом разработки программного обеспечения. Низкое качество продукции может также возникать из-за несоответствия стандартам 5G или из-за отсутствия реализации определенных стандартизированных функций безопасности.

2.52. Зависимость. Зависимость оператора мобильной связи от одного стороннего поставщика или доминирующее положение поставщика в сети создает ряд серьезных уязвимостей. В частности, это повышает риск воздействия любых системных сбоев или враждебной эксплуатации. Этот риск также варьируется в зависимости от профиля(ей) риска поставщика(ов) и может быть косвенным в том смысле, что несколько различных операторов могут полагаться на одного и того же поставщика в отношении важнейшей части своих услуг. Кроме того, риск зависимости усугубляется потенциальными трудностями обеспечения обратной совместимости между новым оборудованием 5G и существующим оборудованием при использовании различных поставщиков. Риск национальной зависимости от одного поставщика особенно остро ощущается в части доступа к сети, где меньше участников рынка.

Связанные сценарии риска:

Низкое качество продукции – шпионаж со стороны государства или поддерживаемых государством субъектов, использующих вредоносные программы для злоупотребления

некачественными сетевыми компонентами или непреднамеренными уязвимостями, влияющими на чувствительные элементы в основной сети, такие как функции виртуализации сети.

Зависимость – оператор мобильной связи получает большое количество своих чувствительных сетевых компонентов или услуг от одного поставщика. Наличие оборудования и/или обновлений у этого поставщика впоследствии резко сокращается из-за неспособности поставщика осуществить поставку (например, из-за торговых санкций со стороны третьего государства или других коммерческих обстоятельств). Вследствие этого качество оборудования поставщика снижается из-за того, что приоритет отдается обеспечению поставок, а не повышению безопасности продукта.

III. Сценарии риска, связанные с методами работы основных субъектов угроз

2.53. Некоторые сценарии риска напрямую связаны с типичными возможностями и намерениями основных субъектов угроз, например, их потенциальными намерениями выполнять определенные типы атак и их способностью использовать определенные векторы атаки.

В частности, враждебные третьи страны могут оказывать давление на поставщиков 5G с целью содействия кибератакам, служащим их национальным интересам. Степень подверженности этому риску в значительной степени зависит от того, в какой степени поставщик имеет доступ к сети, в частности к своим наиболее чувствительным активам, и от профиля риска отдельного поставщика. Она также значительно возрастает в тех

случаях, когда отсутствуют достаточные меры безопасности и контроля доступа. Помехи могут возникать различными способами, например, путем использования встроенных непреднамеренных уязвимостей или путем преднамеренного внедрения уязвимостей.

Кроме того, сети 5G также могут быть объектом сложных вредоносных действий организованной преступности для получения прибыли. Менее влиятельные субъекты, такие как организованные преступные группы, могут также торговать опытом проникновения в сети для получения финансовой выгоды

Связанные сценарии риска:

Государственное вмешательство через цепочку поставок 5G – враждебный государственный субъект оказывает давление на поставщика под его юрисдикцией, чтобы обеспечить доступ к чувствительным сетевым активам через (целенаправленно или непреднамеренно) встроенные уязвимости.

Эксплуатация сетей 5G организованной преступностью – взяв под свой контроль критическую часть сетевой архитектуры 5G, организованная преступная группа нарушает различные услуги для выкупа предприятий, полагающихся на эти услуги, или самого оператора мобильной связи.

В качестве альтернативы, используя аналогичный путь атаки, организованная преступная группа может также нацелиться на конечных пользователей, например, вводя ложные сообщения пользователям сети в рамках крупномасштабной «фишинговой» атаки или онлайн-мошенничества, или используя скомпрометированную сеть для получения доступа к

конфиденциальным данным о пользователях (например, коды двухфакторной аутентификации) для дальнейшей прибыли.

IV. Сценарии риска, связанные с взаимозависимостями между сетями 5G и другими критическими системами

2.54. Учитывая предполагаемую взаимозависимость между сетями 5G и многими другими системами в критических областях (например, здравоохранение, автономные транспортные средства, электроэнергия, газо- и водоснабжение, оборона), ухудшение или отказ служб 5G может привести к значительным сбоям в работе этих систем.

И наоборот, другие критически важные инфраструктуры, от которых зависят сети 5G, такие как электросети и системы ICS, имеют известные уязвимости, которые могут быть объектами кибератак. Потенциальные сбои в предоставлении основных услуг для операторов сети 5G возможны либо из-за отказов в обслуживании со стороны поставщика услуг (например, источника питания), либо из-за кибератак на объект, зависимый от критической информационной инфраструктуры. Контроль над выделенным фрагментом со стороны актора, который является внешним по отношению к сети, также может повысить подверженность киберугрозам. За последние годы многие субъекты, создающие угрозы, развивали эти возможности, включая действующих лиц, пользующихся государственной поддержкой.

Последствия этих двух категорий сценариев риска существенно усугубляются в случае отсутствия эффективных механизмов реагирования на чрезвычайные ситуации и обеспечения непрерывности деятельности.

Связанные сценарии риска:

Значительное разрушение критических инфраструктур или служб – злоумышленники могут скомпрометировать аварийные службы, получив контроль над выделенным участком сети, тем самым ставя под угрозу доступность службы и целостность информации/данных, используемых для/внутри этой службы.

Массовый отказ сетей из-за прерывания электроснабжения или других вспомогательных систем – массовое отключение электроснабжения из-за стихийных бедствий или атак на энергосистему со стороны государства, поддерживаемого государством субъекта или организованной преступной группы.

V. Сценарии риска, связанные с устройствами конечного пользователя

2.55. Этот сценарий риска является следствием огромного увеличения количества и разнообразия устройств (особенно устройств интернета вещей), которые будут подключаться к сетям 5G.

Эти устройства будут охватывать чрезвычайно широкий спектр требований и условий безопасности, таких как устройства управления промышленной автоматизацией, транспортные контейнеры, датчики климата и планшеты и смартфоны следующего поколения.

Очень большое количество устройств, одновременно пытающихся получить доступ к сети, действительно может вызвать перегрузку сети. Принимая во внимание ожидаемую растущую зависимость общества от сетей 5G, последствия для безопасности, связанные с использованием большого количества плохо защищенных устройств в сети, могут быть значительными.

Связанный сценарий риска:

Использование интернета вещей: хактивистская группа или актор, поддерживаемый государством, берет под контроль устройства с низким уровнем безопасности, такие как IoT (датчики, бытовая техника и т.д.), чтобы атаковать сеть, подавляя ее сигнальную плоскость.

E. Существующие смягчающие меры/базовый уровень безопасности

2.56. На уровне ЕС требования безопасности, относящиеся к экосистеме сетей 5G и соответствующим критическим системам, изложены, в частности, в законодательстве ЕС о телекоммуникациях и в Директиве NIS. В рамках телекоммуникационной системы ЕС обязательства могут быть возложены на операторов электросвязи соответствующим государством-членом(ами), в котором предоставляются услуги. Директива NIS требует от операторов основных услуг в других областях (энергетика, финансы, здравоохранение, транспорт, водоснабжение и т.д.) принимать надлежащие меры безопасности и уведомлять о серьезных инцидентах соответствующие службы.

2.57. К другим мерам на уровне ЕС и на национальном уровне относятся правила защиты данных и конфиденциальности (в частности, Общий регламент о защите персональных данных (GDPR) и Директива об обработке персональных данных и охране частной жизни в сфере электронных коммуникаций(e-Privacy Directive), а также требования, применимые к критически важным инфраструктурам.

2.58. На национальном уровне государства-члены приняли различные подходы к осуществлению вышеупомянутых

положений о безопасности и к их применению. Там, где обязательные правила применяются к операторам мобильной связи, они могут охватывать различные типы технических и организационных мер.

2.59. Кроме того, операторы мобильной связи могут применять различные меры безопасности, например, технические меры (шифрование, аутентификацию, автоматизацию, обнаружение аномалий) или меры, связанные с процессом (управление уязвимостью, планирование инцидентов и ответов, управление привилегиями пользователей), планирование аварийного восстановления).

2.60. С точки зрения стандартизации, рабочая группа SA3 3GPP решает несколько проблем безопасности 5G, поддерживая, в частности, сквозное шифрование. Однако работа, проводимая в этих органах, не связана с проблемами безопасности, связанными с развертыванием и настройкой технологии.

3. Выводы и дальнейшие действия

3.1. В данном документе указывается на ряд важных проблем безопасности, которые, вероятно, будут возникать или усиливаться с появлением сетей 5G, принимая во внимание эволюцию технологий и среды 5G.

3.2. Хотя технология и стандарты сетей 5G также принесут определенные улучшения безопасности по сравнению с предыдущими поколениями сетей, ряд важных проблем связан с новыми функциями сетевой архитектуры и широким спектром услуг и приложений, которые в будущем могут в значительной степени зависеть от сетей 5G.

3.3. Эти проблемы безопасности также связаны с расширением доступа сторонних поставщиков к сетям и взаимосвязями между сетями 5G и сторонними системами, а также со степенью зависимости от отдельных поставщиков.

3.4. В частности:

a) технологические изменения, внесенные 5G, увеличат общую поверхность атаки и количество потенциальных точек входа для атакующих:

расширенные функциональные возможности на границе сети и менее централизованная архитектура, чем в мобильных поколениях предыдущих поколений, означают, что некоторые функции базовых сетей могут быть интегрированы в другие части сетей, что делает соответствующее оборудование более чувствительным (например, базовые станции или функции MANO);

увеличение доли программного обеспечения в оборудовании 5G приводит к увеличению рисков, связанных с процессами разработки и обновления программного обеспечения, создает новые риски ошибок конфигурации и отводит более важную роль в анализе безопасности при выборе, сделанном каждым оператором мобильной сети на этапе развертывания сети;

b) новые технологические особенности приведут к большей зависимости операторов мобильной связи от сторонних поставщиков и их роли в цепочке поставок 5G.

Это, в свою очередь, увеличит количество путей атак, которые могут быть использованы субъектами угроз, в частности государствами, не входящими в ЕС, или субъектами,

поддерживаемыми государством, в силу их возможностей (намерений и ресурсов) для совершения атак на телекоммуникационные сети государств – членов ЕС, а также потенциальной серьезности последствий таких атак.

В таком контексте увеличения подверженности атакам, осуществляемым сторонними поставщиками, индивидуальный профиль риска поставщиков станет особенно важным, в частности, когда поставщик имеет значительное присутствие в сетях или областях;

c) большая зависимость от одного поставщика увеличивает риск и последствия потенциального отказа этого поставщика. Это также усугубляет потенциальные последствия слабостей или уязвимостей и их возможного использования субъектами угроз, в частности, в тех случаях, когда зависимость касается поставщика, представляющего высокую степень риска;

d) если некоторые из новых вариантов использования, предусмотренных для 5G, будут реализованы, сети 5G станут важной частью цепочки поставок многих критически важных ИТ-приложений. В результате будут затронуты не только требования конфиденциальности и неприкосновенность частной жизни, но и целостности и доступности этих сетей, что станет основной проблемой национальной безопасности и серьезной проблемой безопасности с точки зрения ЕС.

3.5. В совокупности эти проблемы создают новую парадигму безопасности, что делает необходимым переоценку нынешней политики и методов обеспечения безопасности, применимых к данному сектору и его экосистеме и необходимых

для принятия государствами-членами необходимых смягчающих мер.

3.6. Это требует выявления потенциальных пробелов в существующих методах и механизмах обеспечения соблюдения безопасности, начиная от реализации законодательства в области кибербезопасности, надзорной роли государственных органов и соответствующих обязательств и ответственности операторов и поставщиков.

3.7. Для устранения вышеописанных рисков и полного использования потенциальных возможностей безопасности, связанных с технологией 5G, могут быть рассмотрены различные типы мер. Среди этих мер некоторые из них уже приняты, по крайней мере, частично. Это касается, в частности, требований безопасности, применимых к мобильным сетям предыдущих поколений, которые остаются в силе для будущего развертывания сетей 5G. Кроме того, для многих из выявленных рисков, особенно тех, которые оказывают влияние на уровень ядра или уровень доступа, подходы на случай непредвиденных обстоятельств были определены посредством стандартизации 3GPP.

3.8. Тем не менее фундаментальные различия в работе сетей 5G также означают, что существующие меры безопасности, применяемые в сетях 4G, могут быть не совсем эффективными или недостаточно полными для снижения выявленных рисков безопасности. Кроме того, сущность и характеристики некоторых из этих рисков требуют определения того, могут ли они быть устранены только с помощью технических мер.

3.9. Оценка этих мер будет проведена на следующем этапе выполнения Рекомендации Комиссии. Это приведет к определению набора инструментов для соответствующих, эффективных и соразмерных возможных мер по управлению рисками для снижения рисков кибербезопасности, выявленных государствами-членами в рамках этого процесса.

3.10. Следует также учитывать развитие европейского промышленного потенциала с точки зрения разработки программного обеспечения, производства оборудования, лабораторных испытаний, оценки соответствия и т. д.