

Понятие и специфика исследований измерений Интернета

Мадина Касенова

Аннотация
Автор рассматривает специфику ландшафта интернет-измерений через призму многомерности Интернета и его эволюционного развития. С учётом масштабного и разнообразного состава вовлечённых в интернет-измерения субъектов в статье отмечены складывающиеся международные организационные механизмы, а также в общем плане рассмотрен ряд документов, предметно затрагивающих интернет-измерения.

Ключевык слова:
измерения Интернета, RFC 1262, стейкхолдеры, эмерджентность, IETF, Конференция по измерениям в Интернете, Internet-Drafts

Исследования, предметно относящиеся к проблематике измерений Интернета (Internet Measurement), иначе – «измерения в Интернете», «измерение параметров Интернета», «мероприятия по измерению Интернета» и т.д. (далее – «интернет-измерения»), – проводятся несколько десятилетий. Спектр исследований интернет-измерений многообразен и контекстно затрагивает как теоретические, так и практические аспекты, анализируя среди прочего технологические параметры функционирования инфраструктуры Интернета, включая её фундаментальные принципы и свойства; углубляют понимание перспектив дальнейшего развития Интернета как глобальной «сети сетей» [1]; рассматривают вопросы планирования будущего интернет-технологий с учётом масштабов их роста, сложности и роли в современных реалиях цифровой трансформации и т.д. Едва ли можно подвергнуть сомнению, что сам Интернет как таковой, включая эволюционное развитие форматов его использования, по сути, объективно и всецело обусловливают интернет-измерения (их формат, контекст, параметры, средства, методы и проч.).

Здесь целесообразно обратить внимание на 1983 год, т.е. на тот период, с которого исторически принято отсчиты-

вать появление Интернета, функционирующего в качестве открытой и доступной всем технологически-горизонтальной «сети сетей», универсальность которой изначально зиждилась на трансграничном децентрализованном администрировании её использования (Internet Governance) с опорой на «саморегулирование» (Self-Regulation). Между тем, ретроспективный взгляд позволяет обозначить 90-е годы XX века – т.н. эпохи интернет-классицизма – как временной срок начала проведения интернет-измерений, и аргументировать сказанное можно соображениями следующего порядка.

Отметим, что именно к 90-м годам минувшего века Интернет превратился в важный инфраструктурный ресурс, а часть его компонентов и технологических элементов получила применение в экспериментах, обеспечивающих и поддерживающих технологии иных сетевых инфраструктур. В то же время интернет-технологии стали использоваться в деятельности широкого круга осуществляющих интернет-измерения стейкхолдеров, охватывая в т.ч. масштабное число технических специалистов, операторов-компьютерщиков, инженеров, представителей бизнес-кругов, академического и гражданского сообщества и т.д. Помимо этого, в рассматриваемый временной период вниманию широкого интернет-сообщества были адресованы первые документы, касающиеся проведения интернет-измерений, и в их числе: «Этика и Интернет» (Ethics and the Internet, 1987) [2], «Руководство относительно мероприятий по измерению Интернета» (Guidelines for Internet Measurement Activities, 1991) [3]. Критическая значимость упоминаемых документов во многом вытекает из факта их закрепления в статусе документов RFC (Request for Comments) [4]. Так, первый из названных документов был выпущен в формате документа RFC 1087, а второй – RFC 1262. Отрицать решающую регуляторную авторитетность положений, закреплённых документами в статусе RFC для обеспечения функционирования технологической инфраструктуры Интернета, невозможно, поэтому также следует отметить немаловажное обстоятельство «отсутствия сроков действия» названных документов RFC.

Вышеизложенное позволяет утверждать, что к настоящему моменту интернет-измерения преодолели de facto 35-летний рубеж, вместе с тем, за такой относительно длительный срок ландшафт исследований интернет-измерений устойчиво продолжает сохранять свою специфику. Такая специфика, наряду с прочим, неразрывно связана с двумя объективно существующими факторами, которые дополняют друг друга, взаимосвязаны, взаимообусловлены и, по сути, равным образом определяют как содержание, так и параметры проводимых интернет-измерений.

Во-первых, уместно повторить, что сам Интернет per se объективно обусловливает интернет-измерения, а имманентные свойства его горизонтально-сетевой технологической инфраструктуры и эволюционное развитие форматов использования Интернета также существенным образом определяют специфику проведения соответствующих исследований. Примечательно, что в целом ряде специализированных исследований обращалось внимание на решающее свойство горизонтально-сетевой инфраструктуры Интернета, выражающееся в «эмерджентности» (или «эмергентности», от англ. слова – emergent), которое означает наличие у системы качества, не присущего составляющим её компонентам по отдельности, а также несводимость качеств системы к сумме свойств её компонентов [5]. Необходимость учёта качества эмерджентности инфраструктуры Интернета, с одной стороны, выступает основой проведения измерений любого технологического компонента Интернета, однако, с другой стороны, эмерджентность усложняет получение актуальных и достоверных данных о сетевой инфраструктурной функциональности в глобальном масштабе и, среди прочего, затрудняет репрезентативность понимания показателей производительности Интернета в целом, а также оценки его сетевых настроек, конфигураций и так далее [6].

Нельзя обойти вниманием также то, что специфические особенности ландшафта интернет-измерений сопряжены с эволюционными этапами развития использования Интернета. В этом контексте можно, в частности, обратиться к авторитетному исследованию группы специалистов «Общества Интернета» (ISOC), представивших обобщённые модели-этапы хронологически последовательного развития Интернета: так называемая классическая эпоха; время развития периферийной инфраструктуры по региональному принципу («начало освоения кеш-памяти»); максимальное приближение такой инфраструктуры к пользователю («гипермасшабирование»); переход на оказание услуг по модели телекоммуникационных операторов («расслоение Интернета») [7]. Этапы эволюционного развития Интернета соответственно определяют ландшафт интернет-измерений, когда тематика и направленность исследований не только диверсифицируется, но и выражается в усложнении применяемых средств и экспериментальных методов и т.д. Например, по мере того как Интернет превращался в объект критически важной инфраструктуры, насущной необходимостью становилась потребность в изучении актуальных угроз кибербезопасности, оценке степени внедрения соответствующих средств защиты и анализе эффективности мер по снижению рисков. С использованием разнообразных методов измерения параметров Интернета в контексте кибербезопасности — от угроз в конкретных прикладных областях до анализа самих угроз — исследования измерений параметров Интернета, связанных с кибербезопасностью, предложено классифицировать через призму двух измерений: (i) охватывая различные вертикальные уровни (и компоненты) экосистемы Интернета; (ii) противопоставляя нормальное внутреннее функционирование системы и негативное воздействие внешних субъектов как в цифровом, так и в физическом пространстве [8].

Во-вторых, объективно существующим фактором специфики ландшафта интернет-измерений является то, что его контуры неизменно формируются разнообразным и масштабным кругом стейкхолдеров (представители технического и инженерного сообщества, бизнес-сферы, академических кругов, гражданского общества), которые осуществляют свою деятельность на принципах «саморегулирования» и децентрализованного управления использованием Интернета. При такой множественности и разнообразии стейкхолдеров важно не упустить из виду принципиально важный момент, связанный с правовым

статусом вовлечённых субъектов и их принадлежностью к различным правовым системам. Конкретно речь идёт как о субъектах системы национального права, так и о субъектах системы международного права. Сказанное можно подтвердить некоторыми примерами.

Так, многообразные сферы широкого круга исследовательских тем интернет-измерений с охватом теоретических и практических аспектов рассматриваются в рамках Инженерного совета Интернета (Internet Engineering Task Force, IETF), а конкретные исследования осуществляются проектными исследовательскими лабораториями и создаваемыми рабочими группами (Internet Measurement Research Group, IMRG), которые, в т.ч. выступают площадками для: (i) обсуждения вопросов измерения интернет-параметров в контексте содействия координации различных исследовательских проектов; (ii) оценки и разработки новых методов и средств интернет-измерений; (iii) расширения взаимодействия между операторами, разработчиками инструментов и методов измерения и исследователями, анализирующими и моделирующими динамику Интернета; (iv) анализа всех видов измерения сетевых параметров (активные методы, пассивный мониторинг, зондирование конечных точек, внутрисетевые методы, сетевой уровень, транспортный уровень, прикладной уровень и т.д.), а также полученных результатов сетевых измерений [9].

Проблематика интернет-измерений систематически исследуется на международном уровне, охватывая как деятельность международных организаций, так и проведение мероприятий разнообразного международного формата. Интерес в этой связи представляет определение понятия «Измерение Интернета», разработанное Организацией экономического сотрудничества и развития (ОЭСР) и означающее многомерную систему для оценки функционирования Интернета в технологическом, социальном и экономическом плане, в т.ч. с использованием стандартизированных индикаторов, определяющих возможности широкополосного доступа, уровень подключения домохозяйств и предприятий, производительности сетей, а также вклада цифровизации в обобщённо-совокупный рост добавочной стоимости [10].

Серьёзное развитие получает многолетняя серия регулярных международных мероприятий по проблематике интернет-измерений, и в их ряду значительная роль принадлежит широкомасштабной Конференции по измерениям в Интернете (Internet Measurement Conference, IMC). Первая Конференция по измерениям в Интернете (далее – «Конференция ACM IMC») прошла в 2001 году (США, г. Сан-Франциско) [11]. Она была организована по инициативе Специализированной группы по вопросам передачи данных Ассоциации вычислительной техники (Association for Computing Machinery's Special Interest Group on Data Communications, SIGCOMM ACM) [12]. С этого года Конференция ACM IMC стала проводится в ежегодном формате, способствуя международному многостороннему обмену новейшими методологиями, инструментами и результатами исследований интернет-измерений. Если обобщить, то на Конференции ACM IMC рассматриваются вопросы текущего состояния и будущего функционирования «сетевого взаимодействия», основанного на фундаментальных принципах интернет-инфраструктуры; анализируются модели, свойства и характеристики параметров развития интернет-технологий; обсуждаются проекты документов, рабочие материалы и результаты работ, углубляющие понимание методов сбора и анализа обмена данными в современных условиях т.н. гибридного Интернета, «расслоения Интернета» и т.д. В 2025 году Конференция ACM IMC (Висконсин, США) отметила свой двадцатипятилетний, «серебряный» юбилей. Труды 25 конференций опубликованы и охватывают более 160 работ по конкретным исследованиям интернет-измерений [13]. В октябре 2026 года Конференция ACM IMC проводится в двадцать шестой раз – в г. Карлсруэ (Германия) – и предлагает более масштабную программу, чем обычно [14]. Безусловно, итоги Конференции ACM IMC 2026 ещё предстоит проанализировать, но не вызывает сомнений, что она придаст новый импульс и динамику исследованиям интернет-измерений как на национальном, так и на международном уровне.

В свете представленных выше положений логично обратиться к ряду документов, которые не только выступают ориентиром для исследователей и практиков интернет-сообщества при реализации конкретных мероприятий интернет-измерений разной направленности, но также потенциально могут оказать влияние на дальнейшее формирование возможной нормативной основы проведения интернет-измерений. Значение названных документов невозможно игнорировать, хотя все они носят рекомендательный характер и не устанавливают интернет-стандарты. В числе таких документов следует бегло рассмотреть «Руководство относительно мероприятий по измерению Интернета»; «Руководство по безопасному проведению измерений в Интернете»; «Рекомендации (факторы и условия) безопасного проведения измерений в Интернете».

«Руководство относительно мероприятий по измерению Интернета» получило своё закрепление в формате RFC 1262, о чём говорилось в начале настоящей статьи. В 1991 году под редакцией Винта Серфа (Vinton G. Cerf) был опубликован RFC 1262, адресованный исследователям, рассматривающим возможность проведения экспериментов по измерениям в Интернете [15]. В RFC 1262 указывалось, что данный RFC не является интернет-стандартом, но вместе с тем пользователям Интернета настоятельно рекомендовалось следовать положениям RFC 1262 «...из уважения к интернет-сообществу и профессиональных соображений». Заслуживает внимание тот факт, что временной срок действия RFC 1262 не определен.

Согласно RFC 1262, осуществляющие интернет-измерения лица должны обеспечить соблюдение следующих условий:

- собранные данные не должны нарушать конфиденциальность, безопасность или правила допустимого использования;
- если агрегированные данные потенциально могут нарушать конфиденциальность, исследователь должен защитить конфиденциальность;
- если деятельность по сбору данных может быть истол-

кована как нарушение безопасности, исследователям настоятельно рекомендуется заранее уведомить CERT;

- сбор данных не должен создавать чрезмерной нагрузки или иным образом мешать работе сети или подключённых устройств, соответственно, следует в первую очередь проводить неинвазивные измерения (пассивный мониторинг);
- необходимо связаться с поставщиками услуг, когда возникает влияние на работу системы;
- должны быть широко доступны цели исследования, методология и планы;
- необходимо получить предварительное разрешение, когда интернет-измерения создают чрезмерную нагрузку на удалённое устройство или сеть.

Помимо основных рекомендаций для исследователей интернет-измерений, в RFC 1262 затронут общий контекст безопасности проведения измерений, в частности, проблемы, связанные с потенциально возможной путаницей между плановыми измерениями (активными/пассивным) и vice versa враждебными атаками на безопасность.

В отношении трёх далее рассматриваемых документов, принятых в последние два года (2025-2026), принципиально важно оговорить следующие моменты. Первый момент касается формального статуса этих документов, поскольку все они являются «предварительными документами» (Internet-Drafts) [16], которые действуют не более шести месяцев и в любой момент могут быть обновлены, заменены или признаны устаревшими в связи с появлением иных подобных документов. Второй момент относится к тому, что в настоящей статье документы формата Internet-Drafts использованы в качестве справочных материалов и исключительно с рекомендованной ссылкой – «рабочие материалы»/«незавершённая разработка». Третий момент связан с тем, что нижеуказанные документы предметно сфокусированы на проблематике безопасности интернет-измерений, конфиденциальности и безопасности пользователей. Четвёртый момент определяется тем, что объём рассматриваемых ниже документов позволяет затронуть лишь некоторые их положения.

«Руководство по безопасному проведению измерений в Интернете» (Guidelines for Performing Safe Measurement on the Internet) [17] принято в марте 2025 года со сроком действия до 19.09.2025 года. Данный документ (далее – «Guidelines 2025») соответствует положениям IETF Trust [18] и BCP 78 [19]. В Guidelines 2025 отмечается важность интернет-измерений для широкого круга пользователей, но поскольку их проведение нередко создаёт риски для конфиденциальности и безопасности пользователей, документ содержит рекомендации, которые актуальны для проектов, связанных с генерацией, сбором и/или анализом трафика, создаваемого людьми.

Несмотря на тот факт, что Guidelines 2025 утратил своё действие, представляется интересным обратить внимание на закрепление ряда ключевых понятий, с учётом существующих рисков для конфиденциальности и безопасности пользователей, а именно:

- модель угроз (Threat model): угроза — это потенциальная возможность нарушения безопасности, возникающая при наличии обстоятельств, возможностей, действий или событий, способных привести к нарушению безопасности и причинению ущерба (RFC 4949) [20];
- пользователь (User): в контексте Guidelines 2025 интернет-пользователем считается физическое лицо или организация, чьи данные используются при обмене информацией через Интернет, или, в более широком смысле, любой субъект, использующий Интернет для коммуникации;
- активные измерения (Active Measurement): активные измерения предполагают генерацию или модификацию трафика;
- пассивные измерения (Passive Measurement): пассивные измерения заключаются в наблюдении за существующим трафиком без активного вмешательства;
- измерения на пути следования трафика (On-path): измерения, которые выполняются непосредственно в сети;
- измерения вне пути следования трафика (Off-path): измерения, указывающие на активность, осуществляемую через побочный канал, в оконечной точке или в иных местах, где возможен доступ к пользователю, его соединению или данным;
- односторонние измерения (One-ended): измерения, подобные зондированию или трассировке;
- двусторонние измерения/измерения с двусторонним управлением (Two-ended): измерения, требующие взаимодействия обеих оконечных точек; при этом сеть также может выступать в качестве одной из таких точек, если она является объектом измерения.

«Рекомендации (факторы и условия) безопасного проведения измерений в Интернете» (Considerations for Performing Safe Measurement on the Internet draft-irtf-pearg-safe-internet-measurement-13) [21]. Данный документ (далее – «Considerations 13») принят в июле 2025 года со сроком действия 26.01.2026, соответствует положениям BCP 78 и BCP 79, т.е. Considerations 13 исчерпал срок своего действия [22].

По сути, Considerations 13 являлся обновлённой версией предыдущего документа – Guidelines 2025, соответственно, положения Considerations 13 de facto также направлены на определение рисков для конечных пользователей и инфраструктуры третьих сторон в ходе активных или пассивных интернет-измерений, включая как научные исследования, так и прикладные. Вместе с тем, в Considerations 13 особое внимание уделено рискам, сопряжённым с обеспечением безопасности пользователей при проведении интернет-измерений, и необходимости получения согласия пользователей и сбора данных. Отмечается важность учёта того, что даже если риск нарушения конфиденци-

альности не очевиден или не может быть реализован в текущий момент, рост вычислительных мощностей в будущем может сделать это возможным. В Considerations 13 отмечается, что любое проведение интернет-измерений может повлиять на безопасность пользователей, в частности, измерение генерируемого трафика может косвенно дать также представление о трафике других пользователей.

В ходе интернет-измерений потенциально возможными вариантами воздействия на пользователей могут быть:

- нарушение конфиденциальности (Breach of Privacy). На этапе сбора данных первого уровня (например, имя) возможно идентифицировать конкретного человека; данные второго уровня (например, IP-адрес) могут использоваться для отслеживания поведения. Риск нарушения конфиденциальности также связан с передачей данных пользователя третьим лицам в объёме, превышающем тот, на который пользователь дал согласие; это может произойти в результате случайного или преднамеренного разглашения либо принудительного раскрытия информации. Нарушение конфиденциальности также может касаться риска повторной идентификации или деанонимизации зашифрованных или замаскированных данных пользователей;

- недостаточная защита данных (Inadequate Data Protection). Передаваемые и хранящиеся данные недостаточно защищены от разглашения, и возникает возможность риска несанкционированного доступа к данным, либо отсутствия надлежащего контроля доступа (т.е. когда доступ к пользовательским данным имеют лица, которым он не требуется);

- генерация трафика (Traffic Generation). Генерируемый интернет- трафик – избыточен;

- подмена лица, иначе – имперсонация (Impersonation). В ходе интернет-измерений осуществляется имитация действий пользователя или выдача себя за него;

- правовые аспекты (Legal). Пользователи и поставщики услуг обязаны соблюдать широкий спектр политик и нормативных правил (условия и порядок предоставления услуг, законодательные акты и проч.), применяющихся в зависимости от контекста и юрисдикции. Интернет-измерения способны нарушать такие правила и нормы, а последствия нарушений могут быть серьёзными, и по запросу государственных органов или судов может потребоваться раскрытие конфиденциальных данных;

- недоступность (Unavailability). Пользователи или иные субъекты могут зависеть от информации или систем, задействованных в интернет-измерениях, а неожиданная или запланированная недоступность такой информации или систем может нанести ущерб пользователю;

- нарушение целостности системы или данных (System or Data Corruption). Сгенерированный или модифицированный трафик может привести к нарушению работы системы, что охватывает случаи потери или повреждения данных пользователя, а также ситуации, когда в результате этого нарушается доступ пользователя к системе;

- эмоциональная травма (Emotional Trauma). Проведение интернет-измерений определённых показателей, либо воздействие контента, либо моделей поведения – наносит пользователю эмоциональный или психологический вред.

«Рекомендации (факторы и условия) безопасного проведения измерений в Интернете» (Considerations for Performing Safe Measurement on the Internet draft-irtf-pearg-safe-internet-measurement-14) [23]. Этот документ (далее – «Considerations 14») принят в январе 2026 года со сроком действия 29.07.2026, и соответствует положениям BCP 78 и IETF Trust [24]. В отношении Considerations 14 также следует сказать об исчерпании сроков действия этого документа, равно как и то, что он выступает в качестве обновлённой версии предыдущего документа – Considerations 13. В связи с активным развитием интернет-измерений, проведение исследований в реальной среде Интернета, в отличие от использования изолированных экспериментальных стендов или платформ для моделирования, означает, что эксперименты сосуществуют в одном пространстве с другими сервисами и конечными пользователями. С учётом множественности вовлечённых в интернет-измерения исследователей, Considerations 14 предлагает для них рекомендации, призванные помочь им снизить риски для безопасности конечных пользователей и других сервисов. Нельзя не заметить, что структурно и содержательно Considerations 14 коррелирует ключевым положениям Considerations 13, включая применяемый понятийно-терминологический аппарат, а также потенциально параметры воздействия на пользователей в ходе проведения интернет-измерений [25].

Вполне закономерно и логично было бы в статье не упоминать отдельно каждый из вышерассмотренных документов, принимая во внимание, что и Guidelines 2025, и Considerations 13, и Considerations 14 предметно относятся к безопасности интернет-измерений, являясь «последующими обновлёнными» связанными версиями. Однако рассмотрение исключительно последней версии – Considerations 14, – как представляется, ограничило бы восприятие самого факта самостоятельного значения безопасности проведения интернет-измерений, а также не способствовало бы пониманию важности документального закрепления содержательных границ соответствующих конструируемых понятий, включая определение объёма таких понятий.

***

Принимая во внимание масштаб, разнообразие и стремительно расширяющееся развитие исследований в области интернет-измерений, едва ли можно избежать фрагмен-

тарности и беглости изложения в рамках одной статьи. Однако любое обращение к проблематике интернет-измерений представляется важным в силу того, что такого рода исследования затрагивают не только компоненты Интернета, но и представляют интерес для каждого из нас как пользователей Интернета.

Список литературы:

[1] См, например, D. Karrenberg. Measuring Root Server Performance Internet Way of Networking, https://circleid.com/posts/20120217_measuring_root_server_performance; W.Lehr. Measuring the Internet: The Data Challenge. https://ideas.repec.org/p/oec/stiaab/194-en.html; Агафонов А.С. Цифровая суверенность государства: анализ зарубежных подходов // Российский юридический журнал. 2025. N 3. С. 7 – 15, http://www.consultant.ru/

[2] Ethics and the Internet (RFC 1087, January 1989), https://datatracker.ietf.org/doc/html/rfc1087

[3] Guidelines for Internet Measurement Activities. Vinton G. Cerf (RFC 1262, October 1991), https://datatracker.ietf.org/doc/html/rfc1262

[4] Request for Comments, https://www.ietf.org/process/rfcs/. Подробнее об RFC см. также А. Робачевский. Интернет изнутри: Архитектура экосистемы Интернета. 3-е изд. перераб. и дополн. – М.:Серпантин Эджензи, 2024. С. 15.

[5] О сути концепции эмерджентости см., например, А. Себрант, От Аристотеля до Альтмана: почему «эмерджентность» – ключевой термин для понимания ИИ. https://www.forbes.ru/mneniya/522204-ot-aristotela-do-al-tmana-pocemu-emerdzentnost-klucevoj-termin-dla-ponimania-ii

[6] A. Dayekh. The Illusion of Digital Sovereignty (Part II) – Emergence, Sovereign AI Ecosystem, the RIR System, Number Resources, https://circleid.com/posts/the-illusion-of-digital-sovereignty-part-ii

[7] О. Колкман, А. Робачевский, К. Габерг, Х. Бодран. Влияние развития периферийных сетевых вычислений Интернета // Интернет изнутри (апрель). 2025. – N 22. С.2-8.

[8] M. Safaei Pour, C. Nader, K. Friday, E.Bou-Harb. A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security, https://www.sciencedirect.com/science/article/pii/S0167404823000330

[9] Internet Measurement Research Group (IMRG), https://www.icir.org/imrg/

[10] См., например, Measuring the Internet, https://www.oecd.org/en/publications/measuring-the-internet_5k9bhk5fzvzx-en.html

[11] Internet Measurement Conference, https://dl.acm.org/doi/proceedings/10.1145/3730567; и https://www.sigcomm.org/events/imc-conference

[12] Группа ACM SIGCOMM, https://www.sigcomm.org/about

[13] IMC'25 Proceedings of the 2025 ACM Internet Measurement Conference, https://dl.acm.org/action/showFmPdf?doi=10.1145%2F3730567

[14] ACM Internet Measurement Conference 2026, https://conferences.sigcomm.org/imc/2026/

[15] https://www.iab.org/about/

[16] https://en.wikipedia.org/wiki/Internet_Draft

[17] Guidelines for Performing Safe Measurement on the Internet, https://www.ietf.org/archive/id/draft-irtf-pearg-safe-internet-measurement-12.html

[18] Legal Provisions Relating to IETF Documents, TLD, https://trustee.ietf.org/documents/trust-legal-provisions/

[19] BCP 78 – это документ «Наилучшей текущей практики» в рамках IETF, который определяет практику предоставления прав авторами в отношении их вкладов (Contributions) в IETF, https://www.rfc-editor.org/info/bcp78/ https://www.rfc-ditor.org/info/bcp78/

[20] RFC 4949 (Internet Security Glossary, Version 2), https://datatracker.ietf.org/doc/html/rfc4949

[21] Considerations for Performing Safe Measurement on the Internet, https://datatracker.ietf.org/doc/draft-irtf-pearg-safe-internet-measurement/13/

[22] BCP 78, BCP 79, https://www.rfc-editor.org/info/bcp78/ и https://www.rfc-ditor.org/info/bcp79/

[23] Considerations for Performing Safe Measurement on the Internet, https://www.ietf.org/archive/id/draft-irtf-pearg-safe-internet-measurement-14.html

[24] См ссылки 16 и 18.

[25] M. Fayed. The tricky science of Internet measurement, https://blog.cloudflare.com/tricky-internet-measurement/

Об авторе:

Касенова Мадина Балташевна, д.ю.н, юридическая фирма «Лиджист» (научно-консультативный совет).