

VI. Метрологическое обеспечение средств измерений на цифровой основе

УДК 006:621.39

**МЕТРОЛОГИЯ ЦИФРОВЫХ ПОТОКОВ ИНФОРМАЦИИ
В ПАКЕТНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ**

А.В. Апрелев, В.С. Беляев, В.Н. Шорин

ФГУП «ВНИИФТРИ», Менделеево, Московская обл.

aprelev@vniiftri.ru

belyaev@vniiftri.ru

chorin@vniiftri.ru

Рассматриваются вопросы развития системы обеспечения единства измерений для ключевых параметров современных сетей цифровой связи, таких как пропускная способность сетей, объём переданных данных, задержка передачи пакета данных, джиттер задержки пакета переданных данных. Обосновывается необходимость модернизации национального первичного эталона единиц измерения объёмов передаваемой цифровой информации.

Ключевые слова: цифровая информация, единицы измерения объёмов информации, государственный первичный эталон.

**METROLOGY OF DIGITAL FLOWS OF INFORMATION
IN PACKET NETWORKS OF DATA TRANSMISSION**

A.V. Aprelev, V.S. Belyaev, V.N. Shorin

FSUE "VNIIFTRI", Mendeleevo, Moscow region

aprelev@vniiftri.ru

belyaev@vniiftri.ru

chorin@vniiftri.ru

The article deals with the development of a system to ensure the unity of measurements for the key parameters of modern digital communication networks, such as the bandwidth of networks, the amount of data transmitted, the delay of data packet, the jitter delay of the transmitted data packet. The necessity of modernization of the national primary standard of units of measurement of volumes of the transferred digital information is proved.

Key words: digital information, information volume measurement unit, national primary standard.

В последнее время возросло количество публикаций, посвящённых вопросам метрологического обеспечения цифровой электросвязи и цифровой обработки информации [1–4]. Возросший интерес к этой области измерительной техники обусловлен несколькими факторами. С одной стороны — это возросшее влияние информационных технологий на экономическое и политическое развитие общества. Отражением этого является принятие программы цифровизации экономики [5]. С другой стороны, область цифровой

коммуникации становится опорной частью современной экономики, требующей технического регулирования для согласования качества предоставляемых услуг и регламентов, определяющих взаимодействия сторон, участвующих в технической организации цифровой связи. Несмотря на то, что обеспечение качества предоставляемых услуг коммерческими операторами не является предметом государственного регулирования, руководство таких компаний должно быть заинтересовано в доказательности утверждений об уровне качества предоставляемого сервиса.

Опережающее развитие систем цифровой коммуникации обусловило появление ряда проблем взаимодействий операторов связи с потребителями услуг и между собой, где роль арбитра для разрешения конфликтов должны играть измерительные приборы. Другая, не менее важная роль метрологии в системах связи, связана с обеспечением целостности и устойчивости сетей связи общего пользования. Из самого характера этих задач следует, что обеспечение единства измерений в системах информационного обмена должно быть предметом государственного регулирования, что и прописано в пункте 9 раздела 3 статьи 1 главы 1 Федерального Закона от 26 июня 2008 года № 102-ФЗ «Об обеспечении единства измерений».

Технологии обмена информацией в человеческом обществе стали наиболее быстро развивающейся отраслью науки и техники. Причём эволюция порой идёт с такой скоростью, что можно говорить иногда о революционных скачках в способах доставки информационных сообщений. Новые технологии связи существенно влияют на развитие других отраслей деятельности человечества, поэтому справедливо утверждение о новой эпохе информационного общества. Такое ускоренное развитие приводит к тому, что за появлением и становлением новых технических решений не успевает формироваться система устойчивых понятий и терминов. Устаревшие термины и определения просто транслируются на вновь появившиеся системы и подходы. При этом разные группы специалистов и пользователей начинают по-разному трактовать эти термины и понятия, так что их истинный смысл оказывается полностью утраченным, а возможность говорить на общем языке отсутствует.

Часто проблемы отсутствия общего понимания оказываются завуалированными, поскольку каждый участник процесса вкладывает в понятие того или иного термина свой интуитивный смысл, кажущийся ему наиболее правильным, считая при этом, что и все остальные понимают его таким же образом. Именно метрология зачастую помогает вскрывать эти противоречия в пониманиях и заставляет приводить их к общему знаменателю, поскольку при проведении оценки, обеспечивается или нет единство измерений той и иной величины, приходится достаточно строго доказывать, о чем идёт речь.

Самая глубокая проблема связана с самим понятием об информации и её объёме. Распространено мнение, что минимальной единицей информации

является 1 бит, т.е. ответ на вопрос «да» или «нет». Но это не так. Коварство заключается как раз в вопросе: его сначала нужно задать, а это — неизмеримо больший объём сведений. Можно утверждать, что зажжённый костёр или поднятая стрелка семафора — это и есть 1 бит данных. Но для того, чтобы обеспечить однозначность этого бита, сначала нужно договориться о его значении, тем самым ввести априорную дополнительную информацию. Белый или чёрный дым из трубы в Ватикане будет означать, избран Папа Римский или нет. А без этого контекста он ни о чём не говорит, кроме того, что там что-то сжигают. Передаваемые данные только тогда становятся информацией, когда они начинают нести какой-то законченный смысл, выраженный на том или ином языке, минимальной семантической единицей которого является символ.

В силу известной избыточности человеческой речи этот смысл можно передать разным количеством символов. Недаром говорят, что стихи Пушкина обладают большой информационной ёмкостью. Малым количеством слов ему удавалось удивительно точно выразить многое.

Отсюда напрашивается вывод, что минимальная единица информации не может быть меньше символа. А при подходе к цифровым представлениям — это байт.

То же самое утверждает и теория информации, где даётся определение, что собственной информацией $I(x)$ сообщения x , имеющего вероятность $p(x)$, выбираемого из дискретного ансамбля $X = \{x, p(x)\}$, называется величина, вычисляемая по формуле [6]:

$$I(x) = -\log_2 p(x). \quad (1)$$

Такой подход к определению количества информации близок к комбинаторному подходу, описанному в 1965 году А.Н. Колмогоровым [7], когда говорят об информационной энтропии $H(x)$ переменной x , принадлежащей конечному множеству X из N элементов:

$$H(x) = \log_2 N. \quad (2)$$

В соответствии с этими определениями, количество информации, передаваемое 1 байтом (или информационная энтропия), будет равно 8, а общее количество информации, переданное независимой последовательностью байт, будет равно количеству этих байт, умноженному на 8.

Отметим только самые важные революционные технологические переходы всего пути развития коммуникационных технологий. Пропуская достаточно большой период, когда человечество передавало информацию при помощи сигнальных костров, семафоров и телеграфных линий (кстати, первые технологии передачи информации были по своей сути цифровыми), а также аналоговых телефонных каналов, рассмотрим только последний период, связанный со становлением цифровых технологий, когда информационные технологии стали играть едва ли не доминирующую роль в социальном общении. Одной из важных ступеней развития было появление оптоволо-

конных каналов, позволивших передавать петабитные потоки данных на межконтинентальные расстояния. Развитие сетей связи навсегда оставило в прошлом технологии коммутации каналов, перейдя на технологии передачи пакетов. При этом протоколы синхронных сетей остались только для магистральных каналов. А для широко используемых, особенно на последней миле, асинхронных каналов продолжили использовать термины, неоднозначно трактуемые в этих случаях.

Ключевым является термин «объём переданных данных». Казалось бы, в чём проблема. Скажем, 1 Мегабайт данных — величина счётная, и интерпретироваться всеми должен одинаково.

Первая неоднозначность вот в этих приставках — Кило-, Мега-, Гига- и т.д. Известны случаи, когда в Росстандарт были обращения рассерженных потребителей о том, что они приобрели у поставщика накопитель на жёстком диске объёмом в 1 Терабайт, а он оказался объёмом меньше 1000 Мегабайт.

Согласно пунктам 18 и 19 Приложения № 3 к Положению о единицах величин, допускаемых к применению в Российской Федерации, введённым в действие постановлением Правительства Российской Федерации от 31 октября 2009 г. № 879, в области информационных технологий и связи допускается применение внесистемных единиц величин для количества информации (бит и байт) и для скорости передачи информации (бит в секунду и байт в секунду). При этом Примечанием 6 этого Приложения установлено соотношение между единицами количества информации (1 байт = 8 бит), а также установлено, что единица байт применяется с двоичными приставками «Кило», «Мега», «Гига», которые соответствуют множителям 2^{10} , 2^{20} и 2^{30} (1 Кбайт = 1024 байт, 1 Мбайт = 1024 Кбайт, 1 Гбайт = 1024 Мбайт). В этом случае для кратных единиц не выполняется соотношения между единицами величин бит и байт (1 Килобайт не равен 8 Килобит и т.д.). Международным стандартом ИЕС 60027-2:2005 устанавливается возможность применения префиксов «kilo», «mega», «giga» и т.д. только для кратных единиц степеней числа 10. А для кратных единиц, формирующихся на базе множителей десятичных степеней числа 2, использовать префиксы и обозначения согласно приведённой ниже табл. 1.

Таблица 1

ГОСТ ИЕС 60027-2—2015

3.8.3 Префиксы для кратных двоичных единиц измерения

Множитель	Название префикса	Символ	Полное наименование	Источник происхождения
2^{10}	киби	Ki (Ки)	килобинарный: $(2^{10})^1$	кило: $(10^3)^1$
2^{20}	меби	Mi (Ми)	мегабинарный: $(2^{10})^2$	мега: $(10^3)^2$
2^{30}	гиби	Gi (Ги)	гигибинарный: $(2^{10})^3$	гига: $(10^3)^3$

Продолжение таблицы 1

Множитель	Название префикса	Символ	Полное наименование	Источник происхождения
2^{40}	теби	Ti (Ти)	терабинарный: $(2^{10})^4$	тера: $(10^3)^4$
2^{50}	пеби	Pi (Пи)	петабинарный: $(2^{10})^5$	пета: $(10^3)^5$
2^{60}	эксби	Ei (Эи)	экзабинарный: $(2^{10})^6$	экса: $(10^3)^6$
2^{70}	зеби	Zi (Зи)	зеттабинарный: $(2^{10})^7$	зетта: $(10^3)^7$
2^{80}	йоби	Yi (Йи)	йоттабинарный: $(2^{10})^8$	йотта: $(10^3)^8$
Примеры: один кибит: 1 Кибит = 2^{10} бит = 1 024 бит один килобит: 1 Кбит = 10^3 бит = 1 000 бит один мебибит: 1 МиБ = 2^{20} Б = 1 048 576 Б один мегабайт: 1 МБ = 10^6 Б = 1 000 000 Б				
Примечание. Предлагаемое произношение: первый слог в наименовании префикса произносится так же, как и первый слог соответствующего префикса системы СИ. Второй слог произносится как «би»				

Соответствующие изменения в постановлении о применении префиксов для обозначения объёмов двоичной информации ожидаются в ближайшее время, а психологически нам предстоит привыкать к этому ещё долгое время.

Следующая путаница при измерении объёмов информации обусловлена самой системой передачи или хранения информации. Типичная структура такой системы представлена на рис. 1, изображающем блок-схему системы связи.



Рис. 1. Блок-схема системы связи

Источник информации — это любой объект природы, порождающий сообщения. Кодер источника необходим для представления информации в наиболее компактном виде. Кодер канала обеспечивает защиту информации от помех, а модулятор служит для преобразования сигналов от кодера в сигналы, согласованные с физической природой среды распространения или хранения данных. Чтобы информация достигла потребителя, сигналы и сообщения должны быть преобразованы в обратном порядке.

Проблема задачи измерения объёма информации в том, что каждый этап её обработки должен вносить дополнительные, в данном случае служебные данные, которые получателю информации не нужны, а необходимы только для осуществления процесса передачи через канал связи. Один и тот же объём исходных первичных данных, измеренный на каждом этапе, будет разным.

Именно такая ситуация наблюдается в современных цифровых сетях связи. В рамках модели взаимодействия открытых систем [8] структуру сетевых протоколов принято раскладывать на семь уровней — от прикладного уровня L7 до физического L1 (см. табл. 1). Объём трафика возрастает от прикладного уровня к физическому. Коммерческий подсчёт трафика принято выполнять на уровнях L2 – L4. В этом случае подсчитанный объём данных будет всегда превышать полученный пользователем за счёт заголовков пакетов, служебного трафика, повторов сообщений в протоколах TCP/IP. Разница в объёмах на практике может достигать 10–15 % и более.

Таблица 2

Базовая модель взаимодействия открытых систем
(OSI — *Open Systems Interconnection* basic reference model)

Уровни модели OSI		Функции	Примеры	Уровни стека TCP/IP	Примеры
L7	Прикладной	Доступ к сетевым службам	HTTP, FTP, POP3, WebSocket	Прикладной	FTP, telnet, SNMP, SMTP, HTTP, TFTP
L6	Представительный	Представление и шифрование данных	ASCII, EBCDIC		
L5	Сеансовый	Управление сеансом связи	RPC, PAP, L2TP		
L4	Транспортный	Прямая связь между конечными пунктами и надёжность	TCP, UDP, SCTP, PORTS	Транспортный	TCP, UDP
L3	Сетевой	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk	Сетевой	IP, RIP, OSPF, ICMP
L2	Канальный	Физическая адресация	PPP, IEEE 802.22, Ethernet, DSL, ARP	Уровень сетевых интерфейсов	100BASE-T, 100BASE-FX
L1	Физический	Работа со средой передачи, сигналами и двоичными данными	EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11		

Последнее десятилетие ФГУП «ВНИИФТРИ» проводит комплекс работ, направленных на обеспечение единства измерений в цифровых сетях информации. В 2012 году утверждён Государственный первичный эталон единиц измерения объёмов передаваемой цифровой информации по каналам Интернет и телефонии ГЭТ 200-2012 [9]. Одновременно с этим разработана и утверждена трёхступенчатая поверочная схема [10], предусматривающая передачу единицы объёма цифровой информации от первичного эталона к рабочим эталонам и рабочим СИ, в том числе и дистанционным образом.

Государственный первичный эталон должен обеспечивать передачу заданных объёмов информации по всем системам связи с использованием определённого набора стандартов связи, ограниченных по критерию наибольшей распространённости, а также иметь возможность без существенной модернизации поддерживать новые стандарты, которые появятся впоследствии.

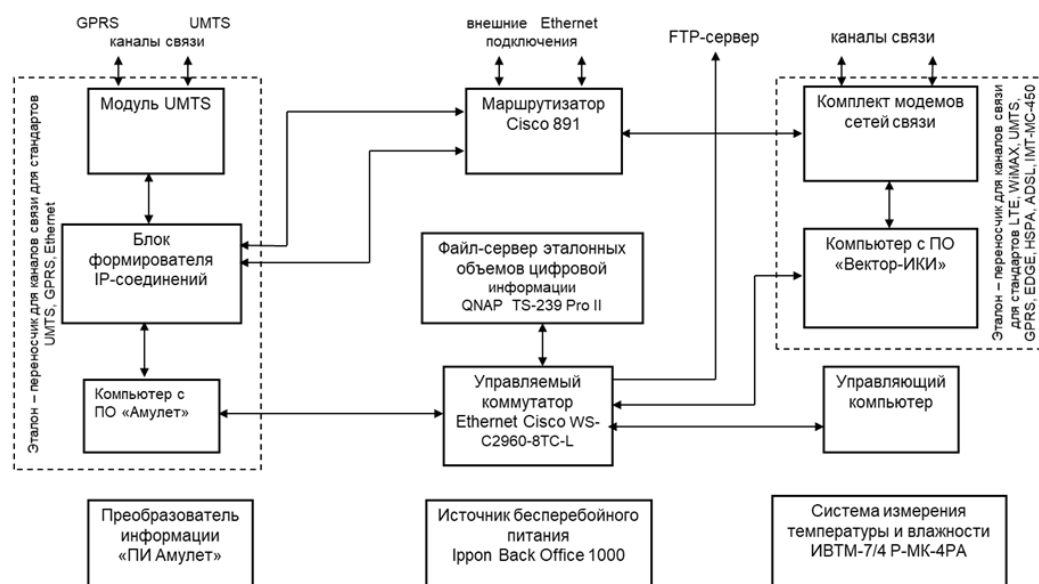


Рис. 2. Структурная схема ГЭТ 200-2012

Основу эталона составляет файл-сервер эталонных объёмов цифровой информации, сохраняемых на нём в виде набора специальным образом созданных файлов. Два эталона-переносчика на базе IP-формирователя «Амулет-М» с модулем UMTS и компьютером с ПО «Амулет» и измерителя количества информации «Вектор-ИКИ» обеспечивают сопряжение с цифровыми сетями наиболее употребительных стандартов. Ethernet коммутатор обеспечивает взаимодействие различных составляющих частей эталона, а маршрутизатор Cisco 891 позволяет осуществлять внешние Ethernet подключения.

Содержимое файлов эталонных объёмов представляет собой псевдослучайную последовательность с равномерным распределением, образованную с помощью специального алгоритма, называемого «Вихрем Мерсенна». «Вихрь Мерсенна» — изобретение японских математиков конца 20 века, являющееся генератором псевдослучайных чисел. Математический алгоритм, лежащий в основе генератора, использует простые числа Мерсена вида $M_n = 2^n - 1$, где n — натуральное число. Названы в честь французского математика Марёна Мерсенна, исследовавшего их свойства в XVII веке. Особенности числовых последовательностей, генерируемых этим алгоритмом, являются их малая предсказуемость, гигантский период повторяемости, отсутствие статистической зависимости и корреляции между последовательными значениями в выходной последовательности. Для генерации последовательностей в файлах ГЭТ 200-2012 использовался вариант алгоритма MT19937, имеющий период повторяемости, равный числу Мерсена $2^{19937} - 1$. Вектор инициализации алгоритма получен с помощью сервиса *ANU Quantum Random Numbers Server* (<http://qrng.anu.edu.au/index.php>), использующего измерение квантовых флуктуаций вакуума в качестве источника истинно случайных чисел.

Предпринятые действия обеспечили не сжимаемость сгенерированных файлов всеми известными алгоритмами. Для проверки целостности файлов при хранении и передаче для каждого из них вычисляется хеш-сумма согласно ГОСТ Р34.11-2012.

Эталонные файлы воспроизводят величину единицы объёма информации на седьмом пользовательском уровне. Реализация метода прямых измерений проводится при участии эталонов-переносчиков, входящих в состав государственного первичного эталона.

Государственная поверочная схема для технических систем и устройств с измерительными функциями, осуществляющих измерения объёмов (количества) цифровой информации (данных), передаваемых по каналам интернет и телефонии, отражена в ГОСТ Р 8.873-2014 и изображена на рис. 3.

До внедрения ГЭТ 200-2012 СИ объёмов переданных данных поверялись с помощью частотомеров, подсчитывающих количество импульсов, соотносённых с каждым байтом переданных данных. Частотомеры, в свою очередь, поверялись как СИ частоты и интервалов времени с прослеживаемостью к эталону времени. Никакого отношения к количественному счёту эта процедура не имела. Эксплуатация эталона ГЭТ 200-2012 позволила приступить к регулированию проблем с обеспечением единства измерений в области цифровой связи. Только за 2018 год количество проведённых поверок СИ объёмов переданных данных с помощью рабочих эталонов, аттестованных на ГЭТ 200, превысило 1500.

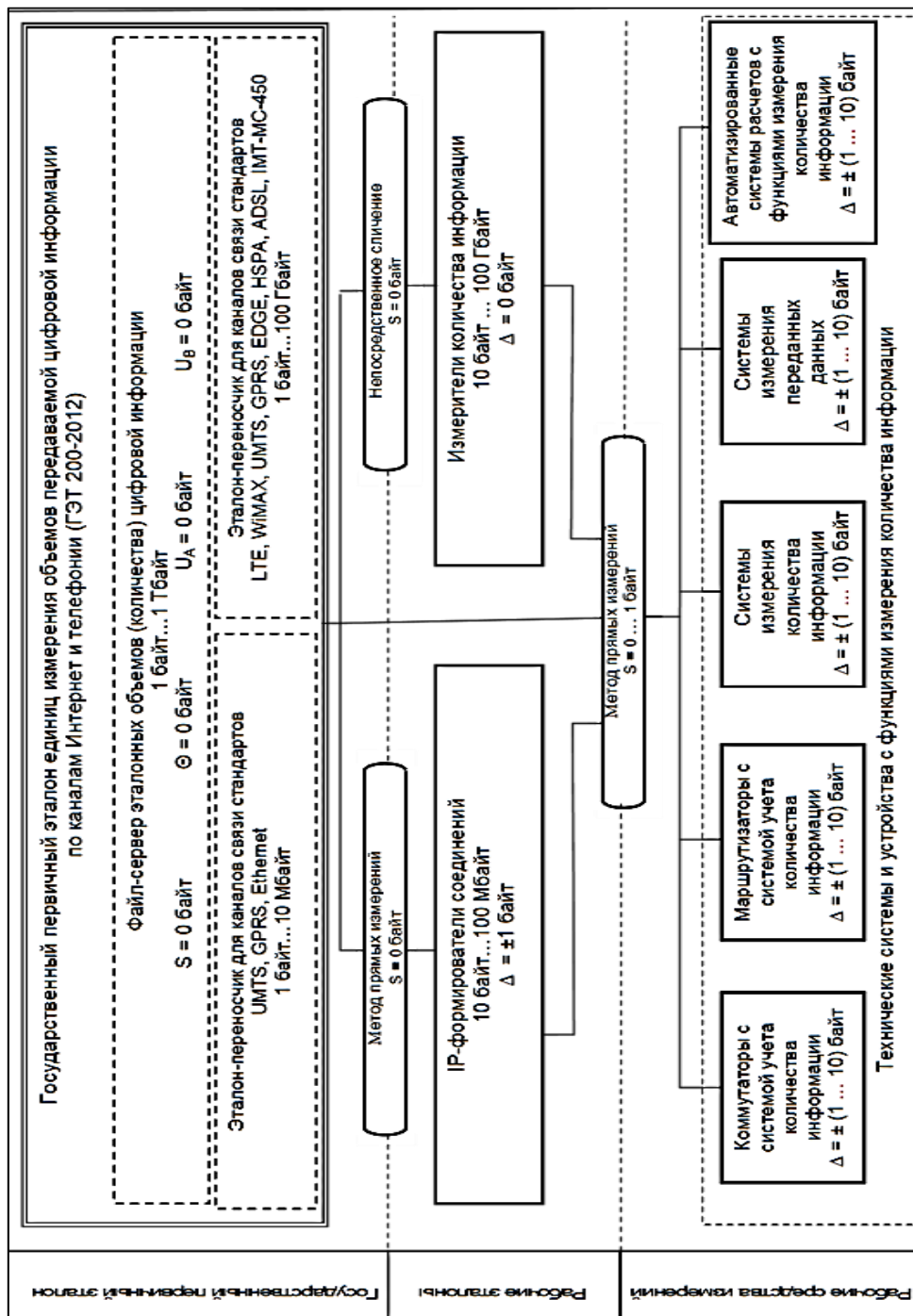


Рис. 3. Государственная поверочная схема для технических систем и устройств с измерительными функциями, осуществляющих измерения объёмов (количества) цифровой информации (данных), передаваемых по каналам интернет и телефони

Накопленный опыт позволяет перейти к следующему этапу работ, предполагая совершенствование поверочной схемы и эталонных средств.

Практика проведения измерений с помощью эталонных средств указывает на необходимость воспроизведения единицы объёмов переданных данных не только на уровне L7 OSI, но и на уровнях L2–L4 непосредственно. В этом случае в состав ГЭТ должны входить не эталоны-переносчики, а эталоны-сравнения, воспроизводящие единицу объёма на более низких уровнях и обеспечивающие процедуру прямых сличений.

Предлагается эталонировать единицы величин, связанных с временными параметрами сетей передачи данных. Важнейшими из них являются: скорость передачи данных, пропускная способность канала, время задержки передачи пакета данных, вариация времени задержки — джиттер. Воспроизведение величин единиц, связанных с измерением временных параметров, требует включения в модернизируемый эталон стандартов частоты, в качестве которого предполагается использовать рубидиевый стандарт частоты и времени Ч1-92. Тем самым будет обеспечиваться прослеживаемость к эталону времени и частоты при воспроизведении величин соответствующих единиц.

Разработка рабочих эталонов будет производиться с учётом возможности их дистанционного применения и управления, что позволит значительно снизить затраты на проведение метрологических проверок и аттестаций. Предполагается при этом поставить вопрос о взаимодействии с порталом ФГИС «АРШИН» — единого электронного реестра свидетельств о поверке и сертификатов калибровок рабочих эталонов и СИ.

Достижимые после модернизации эталона показатели представлены в табл. 3.

Таблица 3

Воспроизведение величины/ Поверяемые устройства	В настоящее время	Достигается после модернизации
Объём передаваемой информации на уровне L7	1 Байт – 1Тбайт, с суммарной неопределённостью 0 Байт	1 Байт – 1 Тбайт, с суммарной неопределённостью 0 Байт
Объём передаваемой информации на уровнях L2–L4	Через рабочие эталоны 100 Байт – 100 Гибибайт с суммарной неопределённостью 10 Байт	Непосредственно с первичного эталона 13 Байт – 1Тебибайт с суммарной неопределённостью 1 Байт
Скорость передачи информации на уровнях L2–L4	нет	1 Кибибайт/с – 1 Гибибайт/с суммарной неопределённостью 1 Байт/с

Продолжение таблицы 3

Воспроизведение величины/ Поверяемые устройства	В настоящее время	Достигается после модернизации
Пропускная способность канала на уровнях L2–L4	нет	Через рабочие эталоны 10 Кибибит/с – 10 Гибибит/с
Количество средств измерений прослеживаемых к первичному эталону	1 300	50 000
Типы средств измерений, прослеживаемых к первичному эталону	Коммутаторы и маршрутизаторы с системой учёта объёмов переданных данных	То же + Анализаторы сетей + Измерительные зонды магистральных сетей на уровнях L2–L4

Проведение работ по техническому совершенствованию эталонной метрологической базы должно сопровождаться развитием соответствующей нормативно-правовой системы. Необходимы дополнения в соответствующие приказы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, о регламентах работы с электронными свидетельствами о поверке, методиках проведения удалённых поверок.

Литература

1. Бакланов И.Г. Принцип релятивизма в метрологии систем связи. М.: ИРИАС, 2016. 304 с.
2. Бакланов И.Г. Оправдание OSS / под редакцией Баклановой Е. [б.м.]: Издательские решения, 2016. 134 с.
3. Кузнецов А.В., Сторожук Н.Л. Контроль качества оказания услуг в пакетных сетях // Техника связи. 2011. № 1. С. 16–20.
4. Битнер В.И., Попов Г.Н. Нормирование качества телекоммуникационных услуг: учеб. пособие для вузов / под ред. профессора В.П. Шувалова. 2-е изд., стереотип. М.: Горячая линия – Телеком, 2009. 312 с.
5. Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р.
6. Кудряшов Б.Д. Теория информации. СПб.: СПбГУ ИТМО, 2010. 188 с.
7. Колмогоров А.Н. Три подхода к определению понятия количество информации // Проблемы передачи информации. 1965. Том 1. Вып. 1. С. 3–11.
8. ГОСТ Р ИСО/МЭК 7498-1-99. «ВОС. Базовая эталонная модель. Часть 1. Базовая модель».

9. Приказ Федерального агентства по техническому регулированию и метрологии от 28 декабря 2012 г. № 1215 «Об утверждении Государственного первичного эталона единиц измерения объёмов передаваемой цифровой информации по каналам Интернет и телефонии».
10. ГОСТ Р 8.873-2014. Государственная система обеспечения единства измерений. Государственная поверочная схема для технических систем и устройств с измерительными функциями, осуществляющих измерения объёмов (количества) цифровой информации (данных), передаваемых по каналам Интернет и телефонии.
11. Matsumoto M., Kurita Y. Twisted GF2R generators // ACM Trans. on Modeling and Computer Simulations. 1992. 2 (3). 179–194.