2) Если ключ шифрования определяется парой (I, X), то уровень D ключа должен быть параметром алгоритма диверсификации ключа. Однако в этом случае не совсем корректно говорить именно о параметре D как об уровне ключа. Скорее, это уже параметр ключевой системы. Кроме того, вопрос о заголовке I как параметре алгоритма снятия защиты ключа остается актуальным.

3) Если ключ шифрования определяется только своим значением X, то для алгоритма защиты ключа заголовок I должен быть параметром алгоритма, а для алгоритма диверсификации такими параметрами должны быть заголовок I и уровень ключа D. Это не выглядит правильным, поскольку параметр I (в меньшей степени D) является атрибутом ключа, а не алгоритма.

Эти соображения влияют на то, какие параметры содержатся в структуре *AlgorithmIdentifier* описания алгоритмов одновременно шифрования и имитозащиты (прямого и обратного преобразования) и диверсификации ключа. В стандарте СТБ 34101.31-2011 сказано, что при указании параметров I и D в структуре *AlgorithmIdentifier*, они должны представляться в виде ASN.1-типа *OCTET STRING*, этого недостаточно (при одновременном использовании непонятен порядок следования).

СТБ 34101.45-2013. “Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых”.

В документе описываются основные крипто алгоритмы: выработка и проверка электронной подписи и алгоритм транспорта ключа. Транспорт ключа имеет прямое преобразование (в СТБ 34101.45-2013 называется алгоритмом создания токена ключа) и обратное (разбор токена ключа). Частью алгоритма транспорта ключа является алгоритм одновременно шифрования и имитозащиты ключа. Поэтому вопросы, связанные с интерпретацией ключа шифрования из предыдущего раздела, актуальны и в контексте транспорта ключа. Поскольку описание транспорта ключа в структуре *AlgorithmIdentifier* для почтовых приложений и протокола SSL/TLS является критичным, в стандарте СТБ 34101.45-2013 во избежание неоднозначности явно указывается, что *“поле parameters должно равняться NULL, а заголовок I транспортируемого ключа полагаться равным 0…0”*.

Поэтому встают следующие вопросы:

1) Если ключ шифрования определяется тройкой (D, I, X) или парой (I, X), то формулировка ограничивает использование алгоритма транспорта для почтовых приложений и протокола SSL/TLS ключами с нулевым заголовком. Как в первом варианте восстановить уровень ключа D после выполнения алгоритма разбора токена ключа, если в нем параметр D вообще не фигурирует?

2) Если ключ шифрования определяется только значением X, то заголовок I ключа должен быть параметром транспорта и формулировка ограничивает использование параметра I алгоритма транспорта в почтовых приложениях и протоколе SSL/TLS только нулевыми значениями.

На наш взгляд, более логично было бы в поле parameters структуры AlgorithmIdentifier помещать не NULL, а структуру AlgorithmIdentifier для одновременно шифрования и имитозащиты ключа (естественно, после ее формального описания, не допускающего неоднозначностей).

В заключение заметим, что исправление указанных недостатков было бы проще произвести, если бы белорусские стандарты описывали только криптографические алгоритмы, а их ASN.1-структуры и использование в рамках криптографических протоколов было бы описано в отдельном документе (стандарте или RFC).

УДК 535.24

СОЗДАНИЕ НАЦИОНАЛЬНОЙ ЭТАЛОННОЙ БАЗЫ БЕЛАРУСИ ДЛЯ СПЕКТРОРАДИОМЕТРИЧЕСКОЙ КАЛИБРОВКИ ОПТИЧЕСКОЙ АППАРАТУРЫ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Длугунович В.А. [1], Никоненко С.В. [1], Беляев Ю.В. [2], Кучинский П.В.[2], Попков А.П.[2], Цикман И.М.[2], Скумс Д.В.[3], Тарасова О.Б.[3]

[1]Институт физики НАН Беларуси

[2]НИИПФП имени А.Н. Севченко БГУ

[3]Белорусский государственный институт метрологии

Минск, Республика Беларусь

Выполнение национальной космической программы и развитие Белорусской космической системы дистанционного зондирования (ДЗ) Земли выдвигают задачи метрологического обеспечения спектрально-энергетических калибровок аэрокосмических систем. Это обусловлено тем, что спектрорадиометрические и радиометрические измерения играют значимую роль среди методов и средств измерений, используемых в ДЗ (геоинформационные системы, производственно-хозяйственная инфраструктура, сельское и лесное хозяйство, экология, мониторинг и контроль

чрезвычайных ситуаций и др.). Качество метрологического обеспечения этих измерений во многом определяет эффективность полученных данных средствами ДЗ, что нашло отражение в документе QA4EO "Стратегия обеспечения качества данных наблюдения Земли" (англ. Quality Assurance Framework for Earth Observation), разработанного в рамках проекта GEOSS по созданию международной глобальной системы наблюдения Земли [1 – 3]. Подходы, изложенные в этом документе, тесно связаны с основами обеспечения единства измерений:

– чёткое определение измеряемых величин, данное с достаточной полнотой и принятое всеми исполнителями измерений;

– выражение результатов измерений в узаконенных единицах;

– прослеживаемость результатов измерений к первичному эталону;

– определение точностных характеристик результатов измерений по единой методике с условием, что они не выходят за установленные пределы с заданной вероятностью.

В настоящее время в Республике Беларусь метрологическое обеспечение спектрорадиометрических и радиометрических измерений, из-за отсутствия Национального эталона единиц спектральной плотности энергетической яркости (СПЭЯ) и освещенности (СПЭО) имеет фрагментарный характер. Имеющиеся в Беларуси установки и комплексы, прошедшие метрологическую аттестацию (БелГИМ, Институт физики НАН Беларуси, ИПФП имени А. Н. Севченко БГУ), в большинстве случаев позволяют обеспечить поверку (калибровку) средств измерений (СИ) спектрорадиометрических и радиометрических характеристик с неопределенностью не лучше 7 %. Аккредитованные калибровочные и испытательные лаборатории в области оптической радиометрии (Института физики НАН Беларуси, ИПФП имени А. Н. Севченко БГУ, ООО «ТМ» и др.), а также большинство производителей спектральной и оптической техники (Белорусское оптико-механическое объединение (БелОМО), ОАО Пеленг, ПО «Горизонт», Рогачевский завод «Диапроектор», ЗАО «Солар ЛС» и др.) вынуждены обращаться за пределы страны, в частности во ВНИИОФИ (Россия) или PTB (Германия), для метрологического обеспечения создаваемых и используемых СИ.

Учитывая необходимость разработки национальной эталонной базы Беларуси для спектрорадиометрической калибровки оптической аппаратуры в 2016 г. в рамках подпрограммы «Эталоны Беларуси» ГНТП «Эталоны и научные приборы» на 2016 – 2020 годы начаты работы по созданию Национального эталона единиц СПЭЯ, СПЭО и силы излучения в диапазоне длин волн от 0,2 до 3,0 мкм. Его основные метрологические характеристики следующие:

- диапазон воспроизведения СПЭЯ от $1 \cdot 10^7$ до $1 \cdot 10^{12}$ Вт·ср$^{-1}$·м$^{-3}$ при стандартной неопределенности воспроизведения СПЭЯ не более 0,7 %;

- диапазон воспроизведения СПЭО от $1 \cdot 10^2$ до $1 \cdot 10^{10}$ Вт·м$^{-3}$ при стандартной неопределенности воспроизведения СПЭО не более 0,72 %;

- диапазон измерений СПЭО от $1 \cdot 10^2$ до $1 \cdot 10^{10}$ Вт·м$^{-3}$;

- диапазон воспроизведения силы излучения от 3,5 до $1 \cdot 10^2$ Вт·ср$^{-1}$.

Состав эталона единиц СПЭЯ, СПЭО: комплекс СИ для воспроизведения единиц СПЭЯ излучения и создаваемой им СПЭО на базе модели эталонного высокотемпературного черного тела (МВЧТ); система для измерений СПЭЯ и СПЭО в УФ области спектра (УФ-система); система для калибровки широкоапертурных СИ.

Система для калибровки широкоапретурных СИ (широкоапертурного эталона) предназначена, в первую очередь, для калибровки приборов ДЗ. Схема широкоапертурного эталона приведена на рис. 1.

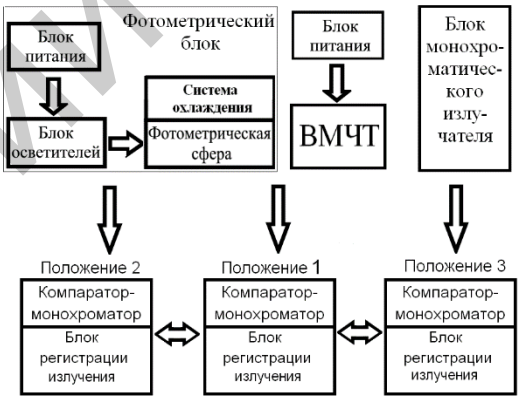

Рис. 1. Схема широкоапертурного эталона

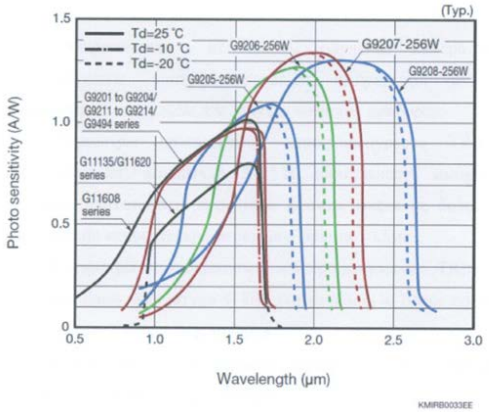

Рис. 2. Относительная спектральная чувствительность InGaAs-линеек Hamamansu

Блок регистрации излучения системы для калибровки широкоапретурных СИ включает два регистратора. Регистратор оптического

излучения U2C-16H7136 (регистратор 1), который работает в спектральном диапазоне от 350 до 1050 нм и включает в себя светочувствительную камеру, сетевой блок питания, соединительные кабели и программное обеспечение, позволяющее управлять режимами работы датчика, синхронизацией внешних приборов и установок, производить визуализацию полученных экспериментальных результатов, а также экспортировать полученные файлы данных для их последующей обработки программными пакетами «Origin», «Matlab» и др. Обмен данными осуществляется по интерфейсу USB-2.0 порта. В качестве датчика используется охлаждаемая ПЗС-матрица S7031-1006S фирмы Hamamatsu. Камера работает в режиме аппаратного суммирования столбцов line binning, таким образом, регистрируются спектры, расположенные в виде одной горизонтальной полосы. Регистратор оптического излучения U2C-16G92087 (регистратор-2) работает в спектральном диапазоне от 1000 до 2500 нм. Фотодетектор регистратора 2 представляет собой InGaAs-линейку G9208-256W фирмы Hamamatsu. Как видно из рис. 2, на котором представлена относительная спектральная чувствительность InGaAs-линеек фирмы Hamamatsu, фотодиодная линейка G9208-256W в спектральном диапазоне длин волн от 1,0 до 2,5 мкм имеет достаточно высокую относительную спектральную чувствительность. На участке спектра вблизи 1,0 мкм значение относительной спектральной чувствительности более 0,2 A/W, максимум чувствительности (со значением 1,2 ÷ 1,3 A/W) приходится на диапазон длин волн от 1,8 до 2,5 мкм.

Создаваемый Национальный эталон единиц СПЭЯ, СПЭО и силы излучения будет являться основой национальной эталонной базы Беларуси для спектрорадиометрической калибровки оптической аппаратуры, в том числе и аппаратуры ДЗ, позволит объединить эталонные средства и соответствующие поверочные схемы в единый радиометрический эталон с оптимизацией количества звеньев. Кроме того, для аккредитованных калибровочных и испытательных лабораторий в области оптической радиометрии, а также для большинства производителей оптоэлектронной и, особенно, спектральной техники отпадет необходимость получения метрологического обеспечения за пределами Беларуси, в частности во ВНИИОФИ (г. Москва, Россия).

1. Global Earth Observation System of Systems: GEOSS 10-Year Implementation Plan Reference Document. Group on Earth Observations. GEO 1000. – 2005.
2. Метрологическое обеспечение радиометри-ческих измерений оптической аппаратурой наблюдения земли / Панфилов А.С. [и др.] // Мир измерений. – 2011. – № 12. – С. 14–20.

УДК 004.588

КОМПЬЮТЕРНАЯ ПОДДЕРЖКА МЕТРОЛОГИЧЕСКОЙ ЭКСПЕРТИЗЫ

Матюш И.И., Спесивцева Ю.Б.
Белорусский национальный технический университет
Минск, Республика Беларусь

Производство различной технической продукции зачастую ориентировано на экспорт, поэтому при проведении метрологической экспертизы и нормоконтроля необходимо руководствоваться теми нормами, требованиями и правилами, которые актуальны для страны-импортёра данной продукции. Экспертная работа будет наиболее успешной если процессы ее подготовки и проведения будут максимально формализованы, поэтому надо стремиться к унификации элементов экспертизы и использовать возможности автоматизации (компьютерная поддержка, базы данных, специализированные программные продукты и т.д.). Формализация метрологической экспертизы и нормоконтроля, автоматизация их информационного обеспечения с учетом специфики объектов является актуальной задачей и реализует комплексный и системный подходы к этим видам работ.

При проведении всесторонней эффективной экспертизы, когда необходима высокая квалификация эксперта как в области стандартизации и метрологии, так и области экспертируемого объекта возникает потребность в соответствующей базе знаний. Под знаниями понимается совокупность данных и информации, которая дополняется экспертным мнением, профессиональными навыками и опытом, в результате чего появляется ценный актив, который возможно применять для оказания помощи в принятии решений [1]. Менеджмент знаний должен включать в себя сохранение, классификацию, трансформацию, обеспечение доступности знаний, распространение и обмен знаний, в том числе в рамках организации [2].

Носителями знаний являются сотрудники организации, которые в силу различных обстоятельств, могут покинуть свое место работы, поэтому и с этой позиции целесообразно организовать документирование и систематизацию приобретённой полезной информации, а также обеспечить эффективное управление полученной системой. Таким образом