Информационные технологии в законодательной метрологии
(IT issues in legal metrology)
Дж.Ф. Магана, директор Международного Бюро Законодательной Метрологии
(J.F. Magana, BIML Director)

OIML
BULLETIN
(Бюллетень Международной Организации Законодательной Метрологии (МОЗМ))
v. XLIX, N 2, 2008 (p.p. 28-29)

Электронные устройства появились в средствах измерений как субъект законодательного метрологического контроля в 1970х годах. В то время эти устройства не программировались и были составлены главным образом из более простых компонент.

Инженеры, ответственные за утверждение типа надежности компонент, были, в основном, озабочены следующими проблемами:
каково поведение аналоговых компонент при изменении окружающей температуры, как ведет себя долговременная стабильность, и в какую сторону она меняется для этих компонент, какова доля отказов числовых компонент и какова доля постепенных и вне-запных отказов и т.п., и как обнаруживать отказы и действовать при наличии неисправных компонент. Результаты измерений детально обрабатывались и представлялись в реальном времени, они не сохранялись в электронной памяти, а сохранение суммированных резуль-татов осуществлялось с помощью электро - механических дисплеев. Проверка электрон-ных схем средства измерений была достаточна для понимания их принципа действия, а проверка электронных плат была достаточной для оценки их соответствия типу.

В то время было принято считать, что все объекты законодательной метрологии должны охватываться тестированием окружения посредством визуальной проверки ком-понент. МОЗМ создала комитет D11, в который были приглашены специалисты по зако-нодательной метрологии, при этом считалось, что новые технологии были охвачены на годы вперед. В Европейской комиссии имелся только один объект для дискуссии, отно-сящийся к электронным средствам измерений: как представить и определить различие между надежностью и продолжительностью действия электронных компонент (тестиро-вание окружения и СВМО - Среднее Время Между Отказами) и обнаруживать поломки и внутренние отказы. Предохранение электронных устройств достигалось физическим опе-чатыванием, а доказательство воздействия могло быть предоставлено проверкой элек-тронных плат.

Однако уже тогда появились определенные сложности, относящиеся к соответст-вию типу: поставщик электронных компонент мог изменить их спецификацию без ин-формирования об этом своих клиентов, так что производитель средства измерений не мог гарантировать с достаточной степенью уверенности соответствие типу на время жизни средства измерений. Поскольку производители средств измерений имели очень мало по-требителей производимых электронных компонент, у них было недостаточно возможно-стей для заключения сделок с ними.

Оценивание типа средств измерений продолжалось в 1970х и в начале 1980х, при-нимая во внимание возрастающую сложность функций электронных схем, которые осу-ществляли все больше и больше автоматизированных функций, но все еще не программи-ровались. Специалисты по утверждению типа повышали свою компетентность в электро-нике, но не могли полностью проверить функции средств измерений. Сохранение данных измерений в переписанной (переносной) памяти привело к большей надежности изделий, а дублирование сохраненных данных могло предоставить приемлемые решения.

Когда микропроцессоры впервые появились в средствах измерений, специалисты по законодательной метрологии считали, что это был нормальный прогресс приложения автоматизированных технологий. Используемое программное обеспечение было относи-тельно простым, могло быть полностью описано и оценено, не содержало интерфейсов пользователя больше, чем это было в предшествующих электронных средствах измере-ний, и записывалось на неуничтожаемых носителях памяти. Сохранение данных обеспе-чивалось дублированием, как памяти, так и линий их передачи. Защита целостности средств измерений могла выполняться механическим опечатыванием, а соответствие типу могло устанавливаться проверкой электронной платы, и, если необходимо, сопоставле-нием ROM (постоянных запоминающих устройств).

Во второй половине 1980х годов становится все более очевидным, что средства из-мерений не могут рассматриваться далее как более или менее простой набор электронного оборудования, и что проблемы стали другой природы. Средства измерений могли теперь воспринимать ряд команд и данных от интерфейсов, могли выбирать разные способы функционирования, в средство измерений могли загружаться ключевые метрологические параметры, а также дополнительное и улучшенное программное обеспечение, а само средство

измерений могло трансформироваться за счет внешних модулей.

Первым следствием этого было то, что уполномоченный за утверждение типа ор-ган мог знать только ту информацию, которая описывалась производителем в документа-ции. Средства измерений все в большей степени основывались на персональных компью-терах, оснащаемых внешней периферией, датчиками и дополнительными интерфейсами. Некоторые части программного обеспечения могли разрабатываться специально для раз-ных стран, чьи потребности и требования отличаются друг от друга; другие части разра-батываются только для утверждения исполнения производителя и т.д. Необходимо было знать, какая часть программного обеспечения должна активизироваться и что не требует его знания, когда оно не имеет отношение к делу. Каким образом предотвратить активи-зацию неавторизованной части и функций программного обеспечения - это трудная про-блема.

Какие возможности существуют для доступа к "защищенным" данным или коман-дам с использованием операционной системы, возможен ли перехват данных от перифе-рийных устройств и датчиков без использования программных средств, возможна ли ин-сталляция другого альтернативного программного обеспечения на том же самом жестком диске (т.е. программного обеспечения, которое может использовать тот же самый интер-фейс пользователя и которое может быть ошибочно принято за исходное утвержденное программное обеспечение) - таковы вопросы, на которые органы, ответственные за ут-верждение типа, не способны дать корректные ответы.

Если программное обеспечение защищено от вирусов и троянов, может ли быть дозагружена "шпионская" программа для передачи конфиденциальных данных, и явля-ются ли программные продукты и базы данных надежно защищенными от атак хакеров - вот новые проблемы, которые не могут быть решены тотчас и для всех систем. Хакеры постоянно предпринимают новые атаки, и механизмы защиты регулярно совершенству-ются. Поскольку имеется риск разрушения защиты, то, что должно делаться, когда она разрушена, вот вопрос, на который на настоящий момент законодательная метрология не способна состоятельно ответить.

Но ясно, что все эти вопросы являются решающими для законодательной метроло-гии, чьей задачей является обеспечение доверия к результатам измерений, полученными средствами измерений, действующими без систематического и постоянного надзора со стороны компетентных третьих лиц.

Если технологии защиты информации не будут использоваться в этих средствах измерений, доверие не может быть обеспечено, и все другие метрологические и техниче-ские решения, поставляемые законодательной метрологией, будут иметь очень ограни-ченный интерес.

Таким образом, работа технического комитета МОЗМ ТС 5/SC 2 Программное обеспечение является решающей для обеспечения доверия и существования законодатель-ной метрологии.