

СОБЫТИЯ И МНЕНИЯ

Сергей С. Шумилин
ДОВЕРЕННАЯ ЭКБ: «СКОЛЬКО ВЕШАТЬ В ГРАММАХ?»

«ДОВЕРЕННАЯ ЭКБ: «СКОЛЬКО ВЕШАТЬ В ГРАММАХ?»»

Аннотация: Предложен подход к определению свойства доверенности и уровней доверия к электронной компонентной базе и радиоэлектронным модулям в разрезе требований функциональной, информационной и технологической безопасности.

Ключевые слова: доверенные ЭКБ и РЭА, уровень доверия, функциональная безопасность, информационная безопасность, технологическая безопасность.

Термин «доверенная электронная компонентная база (радиоэлектронная аппаратура)» (доверенная ЭКБ(РЭА)) стал всё чаще определять повестку дня предприятий и руководителей электронной отрасли. Но пока этот термин не имеет нормативного и даже консолидированного определения. И дело, скорее всего, не в сложности задачи, а в том, что корень слова «доверенная» содержит понятие «вера» – признание чего-либо истинным, независимо от фактического или логического обоснования, преимущественно в силу характера отношения к предмету веры, убежденности и уверенности – то есть, свойств настолько далеких от физических сущностей, что любой технократичный подход к познанию предмета изначально обречен на неудачу.

Если провести лингвистический и статистический анализ выступлений и публикаций, связанных с данной темой, то в них самым популярным словом будет «безопасность». То есть, использование «не доверенной ЭКБ (РЭА)» повышает уровень опасности, и, наоборот, безопасность обеспечивается использованием «доверенной ЭКБ (РЭА)».

Термин «безопасность» более привычен для технических отраслей. Созданы методики количественной и качественной оценки уровня безопасности. Таким образом, считаю, что свойство доверенности ЭКБ (РЭА) следует характеризовать и оценивать в рамках повышения или снижения уровня безопасности.

Для технических систем, в том числе ЭКБ (РЭА), предлагается выделить три базовых сферы безопасности, которые имеют принципиально отличную природу, но тесно взаимосвязаны между собой:

- функциональная безопасность;
- информационная безопасность;
- технологическая безопасность.

Термины функциональной и информационной безопасности широко применяются в технической литературе и документации, но даже при этом в стандартах их определения даются по-разному.

Например, ГОСТ Р МЭК 61511-1-2018 дает следующее определение: «Функциональная безопасность: Часть общей безопасности процесса и основной системы управления процессом, которая зависит от правильного функционирования приборной системы безопасности и других слоев защиты».

ГОСТ Р МЭК 61508-4-20122 определяет функциональную безопасность (functional safety), как «часть общей безопасности, обусловленную применением управляемого оборудования (УО) и системы управления (СУ) и зависящая от правильности функционирования состоящих из электрических и/или электронных, и/или программируемых электронных (Э/Э/ПЭ) систем, связанных с безопасностью и других средств по снижению риска».

ГОСТ Р МЭК 62061-20153 использует модифицированное определение МЭК 61508-4-2012 (п. 3.1.12): «Функциональная безопасность (functional safety): Часть безопасности машины и системы управления машины, которая зависит от корректного

СОБЫТИЯ И МНЕНИЯ

Сергей С. Шумилин
ДОВЕРЕННАЯ ЭКБ: «СКОЛЬКО ВЕШАТЬ В ГРАММАХ?»

функционирования электрических систем управления (ЭСУ), связанных с безопасностью, основанных на других технологиях и внешних средствах снижения риска».

ГОСТ Р ИСО 26262-1-20204 дает определение функциональной безопасности, как «отсутствие неоправданного риска вследствие опасностей, вызванных отклонением от предписанного функционирования электрических и/или электронных (Э/Э) систем».

Таким образом, функциональная безопасность объединяет все аспекты безопасности, определяющие работоспособное, качественное и надежное функционирование объекта в режимах работы и условиях его эксплуатации. Доверие к функциональной безопасности ЭКБ (РЭА) это доверие, что техника, где она применяется, не убьет Вас.

В части определений информационной безопасности:

ГОСТ Р ИСО/МЭК 27000-2021 определяет информационную безопасность, как «сохранение конфиденциальности, целостности и доступности информации», что аналогично понятию «безопасность информации».

ГОСТ Р 53113.1-2008 трактует: «Информационная безопасность (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки».

Таким образом, информационная безопасность объединяет все аспекты безопасности, зависящие от информации (раскрытия, утери, искажения, исследования). Доверие к информационной безопасности ЭКБ (РЭА) это доверие, что тайны, доверенные ей, останутся тайной.

С определением технологической безопасности в нормативной базе имеются проблемы. Если определять по аналогии с функциональной и информационной безопасностями, то технологическая безопасность объединяет аспекты безопасности и возможности выполнения всех этапов жизненного цикла изделий – начиная с планирования разработки, возможности и самое главное стабильности серийного производства, модификации изделия, его эксплуатации и заканчивая утилизацией. Доверие к технологической безопасности ЭКБ (РЭА) это доверие, что ее можно будет произвести и купить в нужном количестве, получить необходимую документацию, при необходимости исправить обнаруженные ошибки. Проще говоря новый кардиостимулятор будет в наличии в самый нужный момент.

В свете последних событий, обеспечение именно технологической безопасности выходит на первый план, так как введенные недружественными государствами санкции ограничили доступ российских компаний к иностранным фабрикам и материалам, препятствуя производству наиболее современной и перспективной отечественной ЭКБ (РЭА).

Использование иностранных IP-блоков и САПР при разработке проектов отечественных изделий ЭКБ значительно затруднили переработку и перезапуск проектов на доступных производствах, что привело к дефициту комплектующих и микросхем, и серьезно отразилось на безопасности страны.

Таким образом, доверенность ЭКБ (РЭА) определяется технологической безопасностью, в не меньшей степени чем функциональной и информационной безопасностью.

Отсюда предлагаю следующее определение: **«Доверенная ЭКБ (РЭА) – это ЭКБ (РЭА) с подтвержденными уровнями требований по функциональной, информационной и технологической безопасности».**

СОБЫТИЯ И МНЕНИЯ

Сергей С. Шумилин
ДОВЕРЕННАЯ ЭКБ: «СКОЛЬКО ВЕШАТЬ В ГРАММАХ?»

Согласен с тем, что выше представленные определения функциональной, информационной и технологической безопасности требуют уточнения, адаптации, взаимной увязки и нормативного закрепления для предметной области ЭКБ (РЭА), в том числе с учетом действующих отраслевых нормативных документов, регламентирующих собственно изделия ЭКБ (РЭА), а также процессы их разработки, производства и эксплуатации. Очевидно, что это не задача одного дня и требуется длительная и планомерная работа большого коллектива единомышленников в среде отраслевых специалистов и потребителей электронной продукции. Успешность такой работы во многом будет зависеть от возможности выработки единых принципов и исходных требований.

Из предложенного определения вытекает необходимость введения градации ЭКБ (РЭА) по уровням доверия. Например, средства криптографической защиты классифицируются по уровням защищенности (равно безопасности) и требований к классам КС1, КС2, КС3, КВ1, КВ2, КА1 для них.

Еще пример. Для автомобильной электроники требования функциональной безопасности являются наиболее приоритетными, а комплектующие компоненты могут иметь различный уровень полноты безопасности (УПБА) – А, В, С, D (или более привычное английское ASIL – А, В, С, D).

Аналогичным способом должны быть заданы и уровни технологической безопасности (хотя, конкретный пример классификации пока привести сложно). Учитывая многоуровневость характеристик безопасности, очевидно, что и свойство доверенности ЭКБ (РЭА) должно иметь многоуровневую систему оценки.

Из вышеизложенного следует определение: **«Уровень доверия ЭКБ (РЭА) – это результат оценки достигнутых уровней требований по функциональной, информационной и технологической безопасности»**. В этом случае нельзя утверждать, что одна микросхема является доверенной, а другая нет. Можно говорить только, что у них разный уровень доверия. Более того, требования из разных сфер безопасности часто взаимно противоположны. Например, микросхемы для автомобильной электроники или аэрокосмического применения должны быть с максимальным уровнем функциональной безопасности и должны обладать расширенными режимами тестирования, отладки, диагностики и самодиагностики. В то время как в микросхемах с высокими уровнями информационной безопасности, наоборот, эти режимы являются потенциальными каналами утечки информации и должны быть исключены.

Аналогично, предъявляя высокие требования по технологичной безопасности с учетом доступных в стране собственных технологических возможностей нельзя будет достигнуть привычных и нужных для современного мира функциональных возможностей (наглядный пример – современные микропроцессоры для персональных компьютеров и серверов).

Таким образом, количественная характеристика уровней доверенности должна быть многогранной (многовекторной). Увеличение одного уровня скорее всего приведет к снижению других.

Механизм определения доверенности и уровня доверия может применяться не только к ЭКБ (РЭА). Его можно распространить как «вниз» – на базовые материалы, на основе которых производятся микросхемы, так и «вверх» – на электронные модули (ЭМ) и программно-аппаратные комплексы (ПАК) на основе узлов и блоков РЭА.

Для определения уровня доверия более высокой ступени должны использоваться уровень доверия входящих в нее компонент предыдущей ступени. Так, например, при оценке уровня доверия микросхемы, произведенной на отечественном производстве, в

СОБЫТИЯ И МНЕНИЯ

Сергей С. Шумилин
ДОВЕРЕННАЯ ЭКБ: «СКОЛЬКО ВЕШАТЬ В ГРАММАХ?»

полной мере должны учитываться уровни доверия (определяемые качеством, стабильностью, наличием и доступностью) газов, фоторезистов, фотошаблонов, а также используемого технологического и контрольно-измерительного оборудования.

Скептик скажет, что в таком случае даже микросхемы первого уровня (изготовленные на отечественной полупроводниковой фабрике) не могут считаться доверенными. С одной стороны – да, и тогда предложенный подход позволит более разумно, количественно и комплексно оценить реальный обеспечиваемый уровень безопасности. Но, с другой стороны – нет, поскольку на каждом более высоком уровне переработки уровень доверия может быть повышен с помощью дополнительных мер (например, страховых запасов, вариантов замены, копирования и резервирования, параллельного импорта и т.п.).

И чем больше уровней переработки – тем больше возможность повысить уровень безопасности, чем более обеспечивается полнота наших знаний, понимания и возможностей управления всем спектром рисков для разработчиков, изготовителей и потребителей, проявляющимися на всех этапах жизненного цикла каждого из изделий, тем больше реальных инженерных и логистических возможностей для обеспечения заданного уровня доверия продукции, причем не на основе «веры», а по конкретным техническим критериям для каждой категории потребителей.

Автор благодарит д.т.н., проф. Тельца В.А. и д.т.н., проф. Никифорова А.Ю. за полезное обсуждение и оппонирование данного материала.

*Сергей С. Шумилин,
Заместитель генерального директора по науке
АО «ПКК Миландр»,
Георгиевский пр-кт, 5, Москва, 124498, Зеленоград, Россия
e-mail: shumilin.sergei@milandr.ru, <https://orcid.org/0000-0002-3953-7054>*