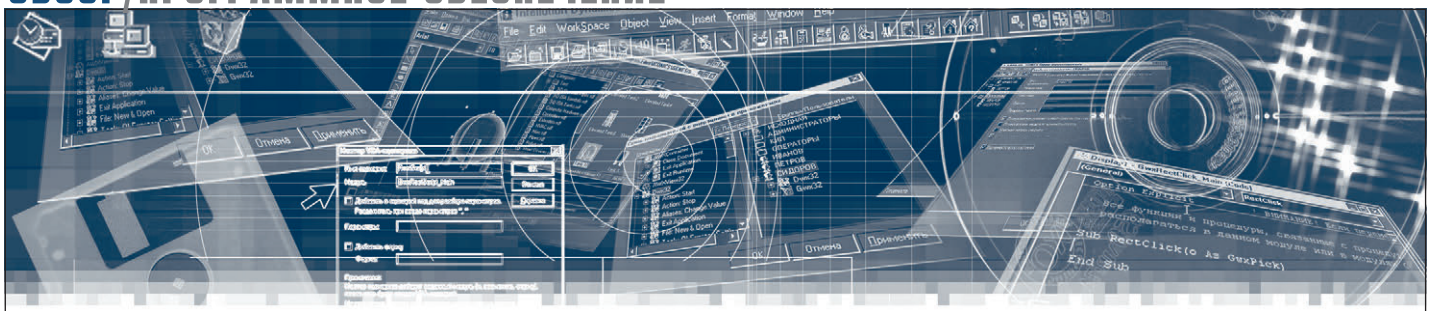


Николай Горбунов

Безопасность и сертификация программного обеспечения

Часть 2. Нормативно-техническая база

В статье приводится обзор современной терминологической и нормативно-технической базы функциональной и информационной безопасности ПО, затрагивается ряд основополагающих вопросов качества ПО и их привязки к нормативной базе. Рассматриваются примеры программных продуктов, соответствующих современным требованиям сертификации, и практические подходы к подтверждению соответствия. Вторая часть описывает текущее состояние нормативно-технической базы.

Разобравшись с терминологией безопасности ПО, логично было бы начать разбираться с тем, как эту самую безопасность ПО обеспечить и продемонстрировать. Процедура демонстрации в общепринятой терминологии называется *подтверждением соответствия* – термин очень удачный, так как сама его формулировка подразумевает наличие *требований*, которым ПО должно соответствовать, и стороннего *оценщика*, который это соответствие должен засвидетельствовать. Здесь, правда, имеет смысл сразу оговориться, что коль скоро обеспечение качества продукции является процессом комплексным, то подтверждение соответствия бывает двух видов: *для продукции* (то есть демонстрация того, что продукция обладает необходимыми свойствами) и *для предприятий* (то есть демонстрация того, что предприятие-производитель удовлетворяет предъявляемым критериям).

В данной статье рассматривается подтверждение соответствия для *продукции*, причём только с точки зрения требований к ней, вне контекста процедуры взаимодействия с оценщиком. Иными словами, настоящая статья призвана ответить на вопрос: «*Каким должно быть ПО, чтобы его можно было сертифицировать как безопасное?*» – вопросы сертификации производства и аттестации объектов, а также сами сертификационные и аттестационные процедуры представляют собой отдельное поле для исследований и выходят за рамки данного материала.

Далее приводится обзор современной нормативно-технической базы функциональной и информационной безопасности ПО с акцентом на общих моментах рассматриваемых стандартов (забегая немного вперёд, можно сказать, что их окажется подозрительно много).

Функциональная безопасность

С точки зрения нормативно-технической базы функциональной безопасности ПО (с терминологической оговоркой, сделанной ранее), отрасли делятся

Таблица 1

Соответствие российской и международной нормативно-технической базы функциональной безопасности ПО

Отрасль		Международный стандарт	Российский аналог	Примечания
Авиация		DO-178B/C	КТ-178B/C, ГОСТ Р 51904	
Любая; общие вопросы		IEC 61508	ГОСТ Р МЭК 61508	Требования к ПО содержатся в части 3
Другие отрасли (не авиация)	**Железнодорожный транспорт**	IEC 62279 (EN 50128)	–	Во многом аналогичен IEC 61508 часть 3; аналог разрабатывается
	Атомная энергетика	IEC 60880	ГОСТ Р МЭК 60880	Во многом аналогичен IEC 61508 часть 3
	Автомобилестроение	IEC 26262	–	Во многом аналогичен IEC 61508, требования к ПО содержатся в части 6; российского аналога нет
	АСУ ТП	IEC 61511	ГОСТ Р МЭК 61511	Ссылается на IEC 61508 часть 3
	Медицинское приборостроение	IEC 62304	ГОСТ Р МЭК 62304	Ссылается на IEC 61508 часть 3
	Машиностроение	IEC 62061	ГОСТ Р МЭК 62061	Ссылается на IEC 61508 часть 3

на два лагеря: авиация и всё остальное. В авиации (в том числе беспилотной – [1], п. 6.1) господствует стандарт RTCA DO-178B, сейчас постепенно заменяемый новой версией DO-178C (квалификационные требования КТ-178В и КТ-178С в российской версии соответственно); в АСУ ТП, атомной энергетике, автомобилестроении, железнодорожном транспорте и прочих критичных отраслях основой являются IEC 61508 и его производные (IEC 60880, 26262, 62279 и т.д.) – большая часть их переведена на русский язык и имеет статус государственных стандартов РФ (табл. 1).

Космонавтика в этой картине держится особняком, и требования функциональной безопасности, предъявляемые к космическим проектам, могут основываться на различных стандартах (а порой и на их комбинации), в зависимости от конкретного случая.

В таблице 1 есть два очевидных белых пятна, и если отсутствие в отечественной нормативно-технической базе аналога IEC 26262 традиционно не вызывает удивления (все, наверное, видели карикатуру, на которой манекен для краштестов упирается из последних сил, стараясь не дать инженеру АвтоВАЗа посадить себя в LADA Priora), то на ситуации с железнодорожной отраслью имеет смысл остановиться чуть подробнее.

В настоящий момент отечественная нормативно-техническая база функциональной безопасности ПО на железнодорожном транспорте имеет вид дырявого лоскутного одеяла. Технические регламенты Таможенного союза [2] «О безопасности железнодорожного подвижного состава» (ТР ТС 001/2011), «О безопасности высокоскоростного железнодорожного транспорта» (ТР ТС 002/2011) и «О безопасности инфраструктуры железнодорожного транспорта» (ТР ТС 003/2011), вступившие в силу в августе 2014 года, картину не проясняют, так как программные средства в них явно указаны в числе составных частей, подлежащих сертификации с предварительной разработкой обоснования безопасности (читай: сертификационного пакета, о котором сказано ранее), но в указанных в [2] перечнях стандартов ссылки на нормативно-техническую базу функциональной безопасности ПО напрочь отсутствуют.

Надежду на скорое изменение ситуации к лучшему, впрочем, вселяет «Транспортная стратегия РФ на период до 2030 года» [3], в числе целей которой заявлены интеграция в мировое транспортное пространство и реализация транзитного потенциала страны и повышение уровня безопасности транспортной системы. Одним из важных шагов к реализации этих целей является начало масштабного внедрения в российской железнодорожной отрасли международного стандарта качества IRIS, явно содержащего требования к безопасности ПО и ссылающегося по этой части на стандарт EN 50128 (он же IEC 62279). В настоящее время ведутся работы по созданию российского аналога EN 50128, причём у отечественной версии есть все шансы оказаться лучше своего зарубежного родителя, так как за годы использования EN 50128/IEC 62279 у зарубежных коллег накопилась ценная обратная связь, и грех этим не воспользоваться.

Информационная безопасность

Сразу оговоримся, что в данном разделе речь идёт только о системе сертификации Федеральной службы по техническому и экспортному контролю (ФСТЭК), под юрисдикцию которой подпадают технические средства защиты информации (СЗИ) некриптографическими методами. Системы сертификации Федеральной службы безопасности России и Министерства обороны РФ в силу ограниченной доступности своих нормативно-методических документов в настоящей статье не затрагиваются.

Основой российской нормативно-технической базы информационной безопасности в системе сертификации ФСТЭК являются руководящие документы (РД) ФСТЭК, те из них, которые были выпущены до 2005 года, также известны как РД Гостехкомиссии (ФСТЭК была создана на её базе в 2005 году). В мировом сообществе, в свою очередь, основным на текущий момент стандартом в области информационной безопасности является IEC 15408 (так называемые «Общие критерии» – фактически метастандарт, задающий систему понятий, в рамках которой можно единообразно описывать требования информационной безопасности) и связанные с ним IEC 18045 и 19791. На этом обзор нормативной базы можно было бы и закончить, если бы не одно «но».

Необходимость приведения российской нормативной базы информационной безопасности в соответствие международным требованиям, вызванная вступлением России в ВТО, послужила основанием для перевода стандартов IEC 15408, 18045 и 19791 на русский язык и получения ими статуса государственных стандартов РФ (ГОСТ Р ИСО/МЭК 15408, 18045 и 19791 соответственно). Кроме того, принятие «Общих критериев» сулило ещё один плюс: развитие сетевых технологий за последние десятилетия привело к тому, что современные средства вычислительной техники (СВТ) и автоматизированные системы (АС) перестали укладываться в классификацию, приведённую в традиционных РД ФСТЭК, разработанных в 1990-х годах, в связи с чем возникла необходимость в унифицированной основе для разработки новых нормативно-методических документов. «Общие критерии» как раз предоставляли такую основу.

Однако, несмотря на вступление ГОСТ Р ИСО/МЭК 15408 в силу еще в 2004 году, немедленного широкомасштабного перехода на «Общие критерии» в России не произошло, как минимум, потому что сами по себе «Общие критерии» проблему не решают, они лишь предоставляют единый каркас для нормативных документов, содержащих конкретные требования к *объектам оценки* (ОО). Таким образом, переходить нужно не на сам стандарт, а на нормативные документы, созданные на его основе, а их ещё надо разработать.

В рамках «Общих критериев» предусматривается два типа таких документов.

- **Профиль защиты** (ПЗ, англ. Protection Profile) содержит набор требований безопасности к определённому *классу* ОО.
- **Задание по безопасности** (ЗБ, англ. Security Target) описывает требования к *конкретному* ОО; если ОО принадлежит к одному или более утверждённых классов, ЗБ будет ссылаться на соответствующие ПЗ.

В свою очередь, требования безопасности, содержащиеся в этих документах, делятся на две категории.

- **Функциональные требования безопасности** (не путать с требованиями функциональной безопасности!), то есть *что* нужно реализовать в продукте для достижения заданных целей безопасности.
- **Требования доверия**, то есть *как* этот продукт следует разрабатывать, эксплуатировать и оценивать, чтобы быть уверенным, что заданные функциональные требования реализованы корректно. Степень этой уверенности выражается так называемым *оценочным уровнем доверия* (ОУД, англ. Evaluation Assurance Level, EAL): чем выше требуемый ОУД (всего их определено 7),

тем более строгие требования доверия предъявляются к ОО.

Здесь важно отметить, что именно ЗБ (а не сам стандарт, как, скажем, в случае IEC 61508 и его производных) служит отправной точкой для сертификационных испытаний конкретного ОО. Из этого, кстати, напрямую следует, что заявления производителей о сертификации своей продукции по «Общим критериям» на заданный ОУД на самом деле полной картины не дают, так как ОУД по определению не содержит информации о функциональных требованиях безопасности, – необходима ссылка как минимум на применимые ПЗ.

После введения в действие ГОСТ Р ИСО/МЭК 15408 на его базе ФСТЭК была разработана группа РД «Безопасность информационных технологий» (БИТ), регулирующих процессы разработки и принятия ПЗ и ЗБ в рамках «Общих критериев», а затем на их основе выпущен и утверждён ряд ПЗ, в частности, для систем обнаружения вторжений, средств антивирусной защиты и межсетевых экранов [4]. На настоящий момент в качестве базы для сертификационных испытаний оценщиками используются как традиционные нормативно-методические документы ФСТЭК (см. золотое правило «работает – не ремонтируй»), так и инновационные, созданные на базе РД БИТ. Ожидается, что по мере разработки и утверждения новых нормативно-методических документов они будут постепенно вытеснять старые, и роль «Общих критериев» в регулировании процесса сертификационных испытаний будет расти.

Следующим перспективным шагом совершенствования отечественной нормативной базы информационной безопасности может послужить распространение требований безопасности на все этапы жизненного цикла ОО – проект соответствующего РД («Положение по обеспечению безопасности в жизненном цикле изделий информационных технологий») был разработан ФСТЭК ещё в 2004 году и терпеливо ждёт своего часа.

Подробный обзор российских систем сертификации по информационной безопасности, соответствующих нормативных документов и применимых испытательных методик приведён в [5].

Комплексный подход

Упомянутая тенденция к комплексному рассмотрению задач функциональной и информационной безопасности постепенно находит воплощение в нормативно-технической базе, причём как за рубежом, так и в России. Очевидно, что в зарубежной практике точкой слияния будут методики управления рисками, так как это позволит вывести рассмотрение проблемы на системный уровень и ранжировать задачи по приоритетам, естественно разрешая таким образом противоречия между обеспечением функциональной и информационной безопасности. В частности, в 2008 году была выпущена группа стандартов ISO/IEC 2700x, посвящённая управлению рисками информационной безопасности, входящий в эту группу стандарт ISO/IEC 27005 (российский аналог – ГОСТ Р ИСО/МЭК 27005) содержит множество параллелей с подходом к управлению рисками, используемым в МЭК 61508. Хороший обзор на эту тему есть в статье «Конвергенция современных стандартов функциональной и информационной безопасности в области информационных технологий» [6].

Со стороны отечественной нормативно-технической базы зарождающийся комплексный подход к решению задач функциональной и информационной безопасности получил воплощение в виде приказа ФСТЭК России от 14.03.2014 № 31[7], устанавливающего требования

к защите информации в АСУ ТП на критически важных и потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (читай: на объектах с повышенными требованиями к функциональной безопасности). Явных ссылок на нормативную базу управления рисками в документе, правда, не содержится, однако сам термин «анализ риска» там присутствует, да и приводимая классификация АСУ ТП по уровню защищённости строится, исходя из степеней возможного ущерба, то есть все дороги так или иначе ведут в Рим.

Расстановка приоритетов между функциональной и информационной безопасностью в приказе № 31 очевидна и многократно дублируется в тексте документа в различных формулировках: меры по защите информации должны быть направлены на обеспечение *безопасного функционирования* АСУ ТП и не оказывать отрицательного воздействия на штатный режим. Чем больше при этом вероятный ущерб от нарушения штатного режима (принятая классификация уровней ущерба, кстати, напоминает используемую в стандарте DO-178, о котором сказано ранее), тем выше требуемый класс защищённости АСУ ТП и тем более строгие требования информационной безопасности (согласно применимым РД ФСТЭК) должны к ней предъявляться, в том числе к применяемым коммерческим программным компонентам.

Куда (и когда) приведёт отечественную нормативную базу объединение задач функциональной и информационной безопасности, сказать пока трудно, в первую очередь вследствие явного её перекоса в сторону безопасности информационной. Впрочем, активная работа в области стандартов функциональной безопасности, проводимая сейчас в российских критичных отраслях, наводит на мысль, что скоро требования функциональной и информационной безопасности будут рассматриваться на равных, а значит, неизбежно возникнет вопрос их балансировки, возможно, как раз на базе единой методики управления рисками.

Найдите десять отличий

Если теперь спуститься с заоблачных высот управления рисками на грешную землю требований к ПО, то можно обнаружить подозрительное сходство между тем, какие конкретно меры по обеспечению функциональной и информационной безопасности программных продуктов предписываются соответствующими нормативными документами из этих двух, казалось бы, пока ещё параллельных миров.

На уровне общепринятого здравого смысла ПО считается качественным, если оно:

- корректно делает то, что от него ожидается;
- не делает того, чего от него не ожидается;
- легко модифицируется, переносится на другие платформы и обслуживается;
- эффективно в использовании и эффективно использует вычислительные ресурсы.

К безопасности (как функциональной, так и информационной) относятся все четыре перечисленных пункта (а не только первые два, как может показаться), так как по сути нарушение любого из них может стать причиной систематического отказа. По здравому смыслу, однако, программный продукт не сертифицируешь: чтобы оценить качество, нужны конкретные критерии. Различные стандарты подходят к этой задаче по-разному; однако, если продраться через различия в терминологии (существенные, к слову) и присмотреться повнимательнее, то внезапно выясняется, что требования

всех современных стандартов функциональной и информационной безопасности по сути совершенно аналогичны и отличаются только реализацией деталей.

Возьмём для сравнения четыре нормативных документа:

- **DO-178B** (КТ-178В или ГОСТ Р 51904: 2002);
- **IEC 61508-3:2010** (ГОСТ Р МЭК 61508-3:2012);
- **РД ФСТЭК «Защита от несанкционированного доступа к информации. Часть 1.** Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»;
- **IEC 15408-3:2008** (ГОСТ Р ИСО/МЭК 15408-3:2013 «Общие критерии»).

Всеми этими документами (хотя и под разными названиями и в разном составе) так или иначе предписываются *одни и те же* методы контроля качества:

- **функциональное тестировани**е, то есть проверка соответствия реальной и заявленной функциональности;
- **структурное тестирование**, то есть построение перечня маршрутов выполнения и анализ покрытия этих маршрутов тестовыми сценариями;
- м**одульное тестирование**, то есть тестирование каждого программного модуля по отдельности и в совокупности на различных наборах данных, включая некорректные и граничные значения;
- **проверка соответствия стандартам кодирования**, то есть соответствие требованиям выбранных методик написания и оформления кода (MISRA, CWE, венгерская нотация и т.п.);
- **подсчёт количественных метрик**, то есть численных оценок объёма, сложности, тестируемости и сопровождаемости кода, степени покрытия требований и т.п.;
- **контроль сцепления** (связанности) по управлению и данным, то есть соблюдение принятых ограничений на связи и способы взаимодействия между модулями;
- **отчётность об использовании переменных.**

Конкретный набор применяемых методов контроля зависит от уровня безопасности: для низких уровней всё обычно ограничивается функциональным тестированием, для самых высоких может требоваться всё сразу. И это только если ограничиться требованиями к *самому ПО*, а если рассмотреть ещё и требования к *процессу разработки* (жизненный цикл, трассировка требований, управление конфигурацией и т.п.), то параллелей будет ещё больше.

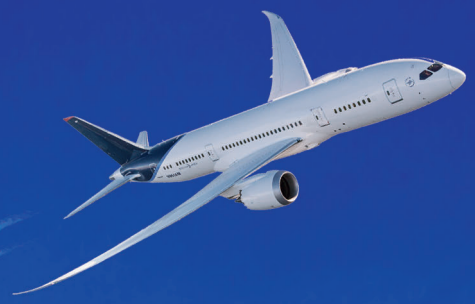
И тут возникает резонный вопрос: коль скоро в основе обеспечения различных видов безопасности лежат одни и те же методы, и это подтверждено нормативной базой, то, может быть, возможен и единый практический подход, подкреплённый единым набором инструментальных средств.

В третьей части статьи речь пойдёт о способах и возможных практических подходах к сокращению стоимости сертификации.

Литература

1. Беспилотные авиационные системы (БАС) : циркуляр ICAO № 328-AN/190 [Электронный ресурс] // Режим доступа : http://www.aerohelp.ru/data/432/Cir328.pdf.
2. Технические регламенты Таможенного союза [Электронный ресурс] // Режим доступа : http://www.tsouz.ru/db/techreglam/pages/tecnicalreglament.aspx.
3. Транспортная стратегия Российской Федерации на период до 2030 года [Электронный ресурс] // Режим доступа : http://www.mintrans.ru/documents/detail.php?ELEMENT_ID=13008.
4. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации [Электронный ресурс] // Режим доступа : http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii.
5. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. – М. : Радио и связь, 2012.
6. Adrien Derock, Patrick Hebrard, Frédérique Vallee. Convergence of the Latest Standards Addressing Safety and Security for Information Technology [Электронный ресурс] // Режим доступа : http://web1.see.asso.fr/erts2010/Site/0ANDGY78/Fichier/PAPIERS%20ERTS%202010/ERTS2010_0067_final.pdf.
7. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ ФСТЭК России от 14.03.2014 № 31 [Электронный ресурс] // Режим доступа : http://fstec.ru/rss-lenta/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. ●

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru



WIND RIVER

- Операционная система реального времени VxWorks 653 для интегрированной модульной авионики, сертифицируемая по DOC-178B/C
- Средства разработки и конфигурирования, соответствующие DOC-178B/C и поддерживающие процессы DOC-279
- Готовые пакеты сертификационной и квалификационной документации

БЕЗОПАСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ — ОСНОВА МОДУЛЬНОЙ АВИОНИКИ

LDRA
Software Technology

- Инструментарий трассировки требований, анализа и автоматизированного тестирования ПО авионики, сертифицированный по DOC-178B/C
- Полуавтоматическая генерация сертификационных документов
- Система поддержки сертификационного процесса DOC-178B/C и взаимодействия с аудитором

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР КОМПАНИЙ WIND RIVER И LDRA

PROSOFT®

МОСКВА Тел.: (495) 234-0636 • Факс: (495) 234-0640 • info@prosoft.ru • www.prosoft.ru
С.-ПЕТЕРБУРГ Тел.: (812) 448-0444 • Факс: (812) 448-0339 • info@spb.prosoft.ru • www.prosoft.ru