

## **COTS - и CrOTS - ПОДХОДЫ К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ КРИТИЧЕСКИХ И КОММЕРЧЕСКИХ ИТ - ПРОЕКТОВ**

д.т.н., проф. В.С. Харченко, К.В. Харченко

*Анализируются тенденции, связанные с использованием коммерческих программных и аппаратных продуктов в критических приложениях на основе COTS-подхода. Формализуется конверсионный CrOTS - подход, который базируется на использовании критических технологий в коммерческих ИТ - проектах. Систематизируются и анализируются варианты COTS - и CrOTS - подходов, включая варианты их совместного использования.*

**Введение.** На рубеже 90-х годов в повседневную жизнь прочно вошло понятие конверсии. Не оценивая ее последствия для науки, экономики и обороны, следует сказать, что в области компьютерных технологий и систем этот процесс был менее болезненным, чем в других сферах, хотя и недостаточно формализованным. В то же время на "гребне" конверсии набрала скорость и мощь встречная и противоположная ей, в некотором смысле, тенденция, которая получила широкое распространение во второй половине 90-х годов. Она непосредственно связана с формализацией **COTS - подхода** (от английского выражения "Commercial Off The Shell", т.е. "коммерческий продукт с полки") [1 - 4]. Он предполагает максимально возможное и строго регламентированное использование коммерческих ИТ - продуктов в критических приложениях (вооружении и военной технике, аэрокосмических комплексах, информационно - управляющих системах АЭС и др.). Сфера действия этого подхода распространяется не только на аппаратные и программные средства, компьютерные технологии в целом, но и на другие типы компонент и систем, которые в данной статье не рассматриваются.

Учитывая многолетние реалии конверсионных (в широком смысле слова) тенденций и отдавая должное полезности (или традициям, существующим, прежде всего, в аналогичной научно - технической литературе, которые переносятся и используются без изменений при переводе) введения аббревиатур, можно говорить, по крайней мере, для компьютерных технологий о целесообразности формализации и анализа **CrOTS - подхода** (Critical Off The Shell), который предполагает наличие "на полке" и последующее использование в коммерческих приложениях продуктов и технологий, созданных и апробированных в критических системах. В известной литературе рассмотренные подходы не анализируются совместно, несмотря на их взаимосвязь и методологическое единство.

В связи с этим в данной статье ставится **задача** систематизации множе-

ства вариантов реализации COTS - и CrOTS - подходов, их предварительного сравнительного анализа, определения возможностей и условий для взаимодополняющего использования.

**Классификация вариантов COTS - и CrOTS - подходов.** В табл. 1, 2 приведены результаты классификации и анализа вариантов реализации COTS -, CrOTS - и смешанного COTS&CrOTS - подходов. При этом выделены группы субподходов, варианты каждого из которых характеризуются типом переносимой компоненты (аппаратных средств HW, программных средств SW, системных решений или технологий Tech), исходной и конечной областями применения (коммерческой CAp или критической CrAp). Кроме того, для всех вариантов определены необходимость регламентации (нормативного регулирования) переноса продуктов из одной области применения в другую с точки зрения обеспечения требуемого в критических приложениях уровня надёжности и безопасности, а также особенности реализации такого переноса.

Анализируемые подходы характеризуются следующими вариантами переноса продуктов (технологий) между коммерческими и критическими приложениями:

$$\text{COTS: } (CAp \rightarrow CrAp) \vee (CAp_i \rightarrow CAp_j); \quad (1)$$

$$\text{CrOTS: } (CrAp \rightarrow CAp) \vee (CrAp_v \rightarrow CrAp_\mu); \quad (2)$$

$$\text{CrOTS\&COTS: } (CrAp_v \rightarrow CAp \rightarrow CrAp_\mu) \vee (CAp_i \rightarrow CrAp \rightarrow CAp_j). \quad (3)$$

В выражениях (1 - 3) индексы указаны только для приложений с изменяемой областью применения ( $i \neq j, v \neq \mu$ ).

Все варианты, связанные с реализацией COTS или CrOTS & COTS - подходов требуют нормативного регулирования (в табл. 1, 2 в графе НР они отмечены знаком «+»).

**Варианты реализации COTS - подхода.** Необходимо подчеркнуть, что COTS - подход сейчас необыкновенно популярен и востребован вследствие реализации парадигмы «cost-effective technologies» (технологий, эффективных по стоимости) во многих критических приложениях [2]. Подтверждением этому является проведение специальных международных конференций, непосредственно связанных с COTS - решениями в критических системах (примерами могут служить ежегодные конференции, проводимые оборонными ведомствами США, NASA, МАГАТЭ (IAEA) в сотрудничестве со всемирно известными компаниями Motorola, Lockheed, ИТТ, такие как COTScop East2002, STC 2002 и др.), а также анализ публикаций по рассматриваемым проблемам в наиболее рейтинговых научных журналах IEEE Transactions on Computers, on Software Engineering, on Reliability.

Группы COTS - вариантов (табл.1) могут быть разделены на COTS/HW-, COTS/SW - и SelfCOTS - подгруппы. В свою очередь, COTS/HW - подгруппа включает решения, основанные на переносе коммерческих аппаратных средств в критические приложения, сопровождаемые дополнительными





испытаниями и сертификацией (HW\*), доработками (HW\*\*) или использованием различных схем резервирования.

Резервирование электронных компонент класса “Industry” позволяет для бортовых компьютеров аэрокосмических систем получать решения, удовлетворяющие заказчика с точки зрения надежности, радиационной стойкости и являющиеся более экономичными, чем решения на основе компонент класса “Military” или “Space” [4]. Это обусловлено тем, что электронные компоненты “Industry” на порядок и более дешевле, чем компоненты “Military” (“Space”), а их мажоритарное выполнение позволяет обеспечить тот же уровень безопасности, что даёт возможность снизить стоимость бортового компьютера в 1,5 - 2 раза даже с учётом уменьшения ресурса из-за более низкой радиационной стойкости. Критичность по показателю радиационной стойкости может быть уменьшена при сеансовом режиме работы бортовой аппаратуры.

Сейчас практически ни один крупный проект в таких критических приложениях, как информационно - управляющие системы АЭС, не реализуется без использования коммерческих компонент программного обеспечения, при условии их соответствия требованиям нормативных документов [5, 6]. Примерами использования программных COTS - продуктов являются проекты [1, 3].

Возможны различные варианты COTS/SW - решений, аналогичные рассмотренной выше подгруппе COTS/HW. Особенности их реализации является проведение анализа опыта эксплуатации, по результатам которого разрешается использование коммерческих программных продуктов, их независимая верификация, валидация и сертификация (SW\*), а также определение возможности использования таких продуктов для проектирования резервных (диверсных) каналов (SW'). Варианты, относящиеся к SelfCOTS - продукции (также как и для SelfCrOTS - подгруппы), описывают ситуации возможного или неприемлемого переноса продуктов коммерческих (критических) приложений внутри области:  $CAp_i \rightarrow CAp_j$  ( $CrAp_v \rightarrow CrAp_\mu$ ).

**Варианты реализации CrOTS - подхода.** CrOTS - подход может быть реализован путём переноса программных продуктов или электронных компонент, разработанных для критических приложений, в коммерческие проекты (табл. 2). На практике чаще реализуется перенос технологий или системных решений из критических в коммерческие приложения. Основными потребителями результатов этого переноса являются так называемые бизнес - критические системы (банковские информационные системы, системы e - коммерции и др.), в которых реализуются отказоустойчивые архитектуры, например, Tandem, Continuum, FTServer и др., основанные на двух - четырёхкратном резервировании аппаратных и программных средств, использовании развитых средств контроля, диагностирования и реконфигурации [7, 8]. В последнее время резервирование используется и в массовых коммерческих продуктах. Подтверждением этому является внутрикристальное дублирование процессоров Pentium, чипов BIOS, серверов Sequoia и др. Эти факты

позволяют сделать вывод о том, что миграция отказоустойчивых технологий в коммерческие приложения (что является сердцевинной CrOTS - подхода) будет нарастать как в количественном, так и в качественном отношении.

**Варианты реализации CrOTS & COTS - подхода.** Данный подход предполагает возможность последовательного переноса продуктов или технологий из критической области CrAr<sub>v</sub> в коммерческие приложения – область CAp, а затем возврат в иные критические приложения CrAr<sub>и</sub> (табл. 2). Примером такого варианта может служить разработка операционной системы реального времени для бортового комплекса, обеспечивающего акцентированную реализацию функций отказоустойчивости. Далее такая система может быть "продвинута" в соответствующих сегментах рынка крупными коммерческими компаниями, что позволит получить массовый опыт эксплуатации. После этого данный продукт, рассматриваемый уже как COTS - средство, может быть применён в других приложениях как аэрокосмической, так и иных критических областей. Теоретически возможен и другой вариант реализации смешанного CrOTS&COTS - подхода (CAp<sub>i</sub>→CrAr→CAp<sub>j</sub>). При этом коммерческая компонента может стать частью отказоустойчивых решений для критических приложений, которые затем могут быть распространены в бизнес - критических системах.

**Выводы.** 1. COTS - подход быстро развивается, распространяясь в системе координат "номенклатура коммерческих продуктов – номенклатура критических приложений", что отражает тенденцию перехода в критических приложениях от оптимизации по критерию "функциональность - надёжность (безопасность)" к оптимизации по критерию "функциональность - надёжность (безопасность) - стоимость". Любой перенос коммерческих продуктов должен сопровождаться нормированием и оценкой безопасности получаемых решений. В международных нормативных документах, в частности, касающихся информационно-управляющих систем АЭС этот аспект находит своё отражение [5, 6].

2. При реализации COTS- подхода в критические приложения преимущественно переносятся продукты (аппаратные и программные компоненты). При реализации CrOTS - подхода в коммерческие области мигрируют, прежде всего, технологии и системные решения.

3. COTS - и CrOTS - подходы дополняют друг друга, создавая своеобразную постоянно расширяющуюся базу для стандартизации и унификации проектных решений в компьютерных системах. Это взаимодополнение связано с тем, что, с одной стороны, использование критических технологий в коммерческих приложениях позволяет получить массовый опыт эксплуатации уникальных решений и усовершенствовать их, повысив надёжность и безопасность ответственных проектов, с другой, – тщательный отбор коммерческих продуктов для применения в критических системах даёт возможность (без ущерба для надёжности и безопасности) снизить стоимость и повысить таким образом их эффективность.

4. При разработке новых компьютерных компонент и технологий необходимо анализировать техническую возможность и экономическую целесообразность реализации COTS - и CrOTS - подходов. На последнюю конференцию Software Technologies Conference, проводимую оборонными ведомствами США, вынесён доклад представителя SEI (Software Engineering Institute) – признанного законодателя мод в области программной инженерии, с гамлетовской формулировкой "To COTS or Not To COTS? - That Is The Question!". Очевидно, что такой же вопрос может быть адресован CrOTS - и CrOTS&COTS - подходам. Факты говорят о том, что практика разработки, внедрения и распространения многих коммерческих и критических систем даёт на него положительный ответ. Задача состоит в нахождении и реализации оптимальных решений для вариантов, представленных в данной статье.

#### ЛИТЕРАТУРА

1. Scott J.A., Preckshot G.G., Gallagher J.M. *Using Commercial-Off-The-Shelf(COTS) Software in High-Consequence Safety Systems*// Lawrence Livermore National Laboratory, UCRL –122246. – 1995.
2. IAEA Working Materials. *Scientific Basis and Engineering Solutions for Cost-Effective Assessments of Software-Based I&C Systems*// *Proceeding of Coordinated Research Meeting, Vienna, Austria, 8-12 November, 1999.*
3. Radice R. *Software Inspections: Past, Present, and Future* // *Proceedings of Software Technology Conference, Solt Lake City, Utah, USA, 29 April – 4 May, 2001.*
4. Харченко В.С., Юрченко Ю.Б., Байда Н.К. *Реализация проектов отказоустойчивых бортовых компьютеров космических аппаратов с использованием электронных компонент Industry* // *Технология приборостроения.* – 2002. – №1. – С. 29 - 36.
5. IAEA Safety Standards Series, No. NS-G-1.1. *Software for Computer-based Systems Important to Safety in Nuclear Power Plants.* – 2000.
6. Харченко В.С., Ястребенецкий М.А., Васильченко В.Н. *Нормирование и оценка безопасности информационных и управляющих систем АЭС: регулирующие требования к программному обеспечению* // *Ядерная безопасность.* – 2002. – №2. – С. 14 - 27.
7. Кузнецов С. *Живучие системы* // *Открытые системы.* - 2000. – № 9.
8. <http://www.cpm.ru/product/stratus>.

Поступила 18.03.2002

**ХАРЧЕНКО Вячеслав Сергеевич**, докт. техн. наук, профессор, зав. кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского "ХАИ", эксперт Государственного научно-технического центра ядерной и радиационной безопасности. В 1974 году окончил Харьковское ВВКИУ. Область научных интересов – критические компьютерные технологии и системы, методы и средства обеспечения надежности, живучести и безопасности.

**ХАРЧЕНКО Кирилл Вячеславович**, студент 4-го курса Харьковского национального университета им. В.Н. Каразина, специальность - экономическая кибернетика. Область научных интересов – системный анализ и моделирование рынка компьютерных технологий.