# «Гарантоспособность» критического ПО

Гарантоспособная компьютерная система (ГКС) – это система, обладающая полным или частичным набором первичных свойств (атрибутов), составляющих гарантоспособность. Иными словами ГКС – отказоустойчивая, высоконадежная, безопасная система с гарантированно достоверными вычислениями. Также, гарантоспособность это способность компьютерных систем предоставлять требуемые услуги, которым можно оправданно управлять.

Ключевым фактором обеспечения характеристик гарантоспособности (надежности, готовности, обслуживаемости) и функциональной безопасности критического ПО являются информационно-управляющие системы (ИУС). Уровень критичности ИУС определяются от тяжести последствий неправильного функционирования. В силу этого возрастает зависимость безопасности от качества критического ПО. Не выявленные на этапах тестирования дефекты ПО являются факторами риска аномального функционирования систем, что может привести к плохим последствиям. Это обуславливает статус критического ПО, как важного элемента нормативного регулирования, определяющего гарантоспособность и функциональную безопасность ИУС в целом. Функциональная безопасность критического ПО трактуется как нахождение системы в условиях проектного риса аномального функционирования в течении установленного срока эксплуатации.

Рентабельность оценки характеристик гарантоспособность и функциональной безопасности критического ПО означает достижение приемлемых прогнозируемых уровней рисков, связанных с остаточными дефектами ПО, при допустимых затратах ресурсов.

Одним из строго рекомендуемых требования является проведение независимой верификации критического ПО, обеспечивающая:

* независимую верификацию на основе усовершенствованной методологии статического анализа исходного ПО, обеспечивающую повышение достоверности оценок характеристик ПО и прогнозирование рисков аномального функционирования из-за остаточных дефектов ПО;
* интегрированную инструментальную поддержку сценария независимой верификации критического ПО на аналитическом, информационном и организационном уровнях;
* рентабельную оценку и прогнозирование рисков, связанных с остаточными дефектами критического ПО.