Уровень доверия программного обеспечения как показатель качества ПО. Концепция.

Докладчик: **Сабанов А.Г.**

д.т.н., профессор МГТУ им. Н.Э. Баумана
главный эксперт НТК ТИО АО «НИИАС»
Р-эксперт ИСО, член ТК 362, ТК 26, ТК 122
Академик Международной академии связи

НИИАС

Качество систем и программных средств

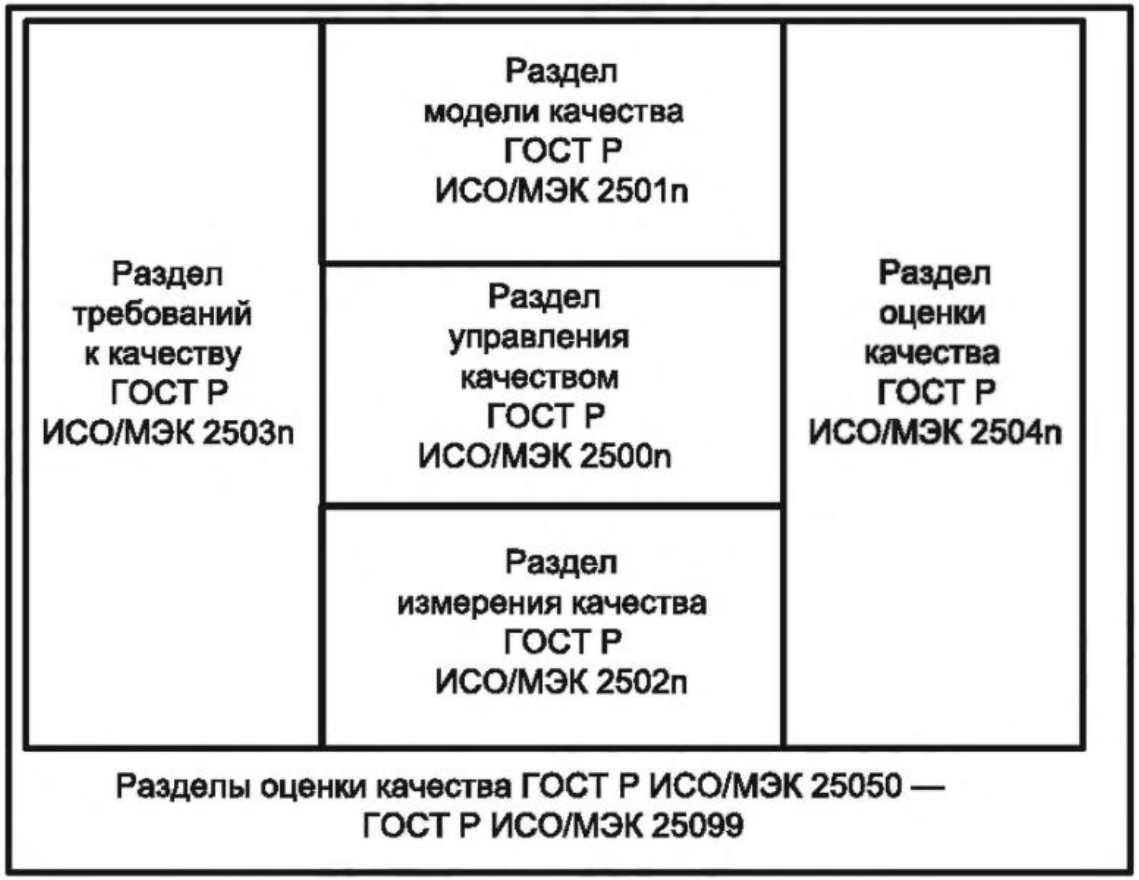
НИИАС

Основные стандарты по качеству ПО в системе ГОСТ Р:

- ГОСТ Р 56921 /ISO/IEC/IEEE 29119-2:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 2. Процессы тестирования.
  - ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств
  - **ГОСТ Р ИСО/МЭК 25000 Системная и программная инженерия. Требования и оценка качества систем и программных средств (SQuaRE). Руководство.**
  - ГОСТ Р ИСО/МЭК 25010 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов
- ГОСТ Р ИСО/МЭК 25022 Системы и разработка программного обеспечения. Требования и оценка качества систем и программного обеспечения (SQuaRE). Измерение качества при использовании
  - ГОСТ Р ИСО/МЭК 25023 Системная и программная инженерия. Требования и оценка качества систем и программной продукции (SQuaRE). Измерения качества системы и программной продукции
- ГОСТ Р ИСО/МЭК 25040 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Процесс оценки.

Требования к качеству могут быть разделены на характеристики/ подхарактеристики с использованием моделей качества, определенных в семействе стандартов ГОСТ Р ИСО/МЭК 2501. Показатели этих характеристик/подхарактеристик, которые определены в семействе стандартов ГОСТ Р ИСО/МЭК 2502n, могут использоваться для определения требования к качеству и оценки качества целевой системы, в том числе ПО как неотъемлемой части ИС.

ТРЕБОВАНИЯ И ОЦЕНКА КАЧЕСТВА СИСТЕМ И ПРОГРАММНЫХ СРЕДСТВ (SQuaRE)



Источник: ГОСТ Р 70921-2023

Пример взаимосвязи показателей качества программного обеспечения

НИИАС

	Функциональная пригодность	Надежность	Эффективность работы	Удобство использования	Безопасность	Совместимость	Ремонтопригодность	Переносимость
Функциональная пригодность		–	–	–	–	–	–	–
Надежность					+		+	
Эффективность работы				+			–	
Удобство использования			–		–			
Безопасность	–	–	–	–		–	–	–
Совместимость	+		–		–			
Ремонтопригодность			–		–			
Переносимость			–		–	+		

Примечание — Знак «+» — положительные эффекты (характеристика качества в строке может положительно повлиять на характеристику в графе); знак «–» — отрицательные эффекты (характеристика качества в строке может отрицательно повлиять на характеристику качества в графе, что означает, что могут возникнуть конфликты).

Источник: ГОСТ Р 70921-2023

Доверие к ПО как подхарактеристика безопасности, одного из основных показателей качества программного обеспечения

НИИАС

- Пункт 50 приказа ФСБ России от 11.04.2025 №117: «Мероприятия по разработке безопасного ПО должны быть направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом оператором программном обеспечении. В случае самостоятельной разработки оператором ПО, предназначенного для использования в ИС, **должны быть** реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939.
- Особенно актуальна задача введения уровней доверия ПО для **систем ЗО КИИ**.
- В настоящее время вопросы безопасности ПО выходят на первый план, требуется пересмотр некоторых положений. Цитата из ГОСТ Р 70921-**2023** (ISO/IEC 25030): «Характеристики безопасности ПО: **конфиденциальность, целостность, неподдельность, подлинность**.

Вывод: проблема разработки критериев безопасности и доверия ПО не решена. Критерии качества ПО в части безопасности информации «размыты» и не отвечают требованиям сегодняшнего дня.

Определение. Под **доверием** ПО будем понимать **обусловленную принятыми мерами уверенность в надежном выполнении программным обеспечением заданных функций при условии обеспечения безопасности принимаемой, хранимой и обрабатываемой** рассматриваемым ПО информации. Безопасность информации при этом обеспечивается **совокупностью** выполнения требований **безопасности процессов разработки** на всем жизненном цикле ПО согласно ГОСТ Р 56939 и корректностью реализации **встроенных в ПО** функций обеспечения **безопасности информации**. Надежность ПО характеризуется выполнением функций безопасности, безотказностью, устойчивостью, безошибочностью, контролируемостью, готовностью и доверенным восстановлением после сбоев.

Понятие и оценка доверия ПО

НИИАС

Примем, что доверие *Tr* может изменяться в диапазоне от нуля до 1: *Tr* є [0;1], при этом доверие может быть сколь угодно близким к единице, но не может быть абсолютным, поскольку в системе всегда есть остаточные риски:

$$Tr(t) = 1 - R_{ост.}(t) \quad (1)$$

где $R_{ост.}(t)$ – величина приведенных остаточных (неустраненных) рисков того, что ПО не сможет обеспечить на 100% функциональную надежность работы, достоверность получаемых результатов и безопасность обрабатываемой программным обеспечением информации, $R_{ост.}(t)$ є [0;1];

t - время.

Формула (1) получена обобщением подхода к оценке доверия интегрированных систем работы [Грызунов В.В., Крюков А.С., Шестаков А.В., Зикратов И.А. Обеспечение информационной безопасности интегрируемых информационных систем на базе доверия // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 110–125.].

Понятие «Доверие ПО» шире, чем понятие «Безопасность ПО» (отсутствие уязвимостей, НДВ, нежелательных конструкций, нарушений целостности и НСД) для принимаемой, хранимой и обрабатываемой рассматриваемым ПО информации.

В упрощенном виде понятие «Доверие ПО» включает в себя одновременное выполнение требований безопасности, надежности, корректности функционирования, сопровождаемости и переносимости.

Уровни доверия ПО (УДПО)

НИИАС

Диапазон УДПО: от первого, низкого уровня доверия, до третьего, самого высокого.

- УДПО - 1 характеризуется некоторой уверенностью в том, что ПО не содержит критических уязвимостей и других недостатков ПО, которые рекурсивно могут нанести ущерб информационной системе после внедрения программного обеспечения.
- УДПО -2 является уровнем обоснованной уверенности в выполнении базовых требований безопасности информации при разработке и применении ПО, подтвержденном документально.
- УДПО -3 характеризуется высоким уровнем уверенности в выполнении всех требований РБПО, что гарантируется разработчиком (выполнение требований РБПО) и подтверждается документально на протяжении всего ЖЦ ПО с помощью регулярного внутреннего и внешнего аудита. К требованиям второго уровня добавляются дополнительные требования по отношению к второму уровню УДПО. Однако даже на этом уровне доверие к безопасности информации не может быть абсолютным, оно может быть близко к единице за вычетом остаточных (неустраненных) рисков.

Уровни доверия ПО в процессах разработки и эксплуатации ПО

НИИАС

В процессах опытной и постоянной эксплуатации остаточные (неустраненные) риски определяются по ГОСТ Р ИСО/МЭК 27005 для **среды эксплуатации** как часть рисков системы, для которой данное ПО разрабатывалось. Используется модель угроз для **системы**, построенная по методике ФСТЭК России от 05.02.2021.

Если остаточные риски оценены с достаточной степенью достоверности, то границы предложенных уровней доверия определяются с помощью формулы (1), исходя из критерия соотношения остаточного и допустимого риска, который равен отношению суммы остаточных рисков к допустимому уровню риска для каждого уровня. В случае невозможности получения достоверных оценок остаточных рисков можно воспользоваться применением нескольких вероятностных методов оценки рисков, рекомендуемых ГОСТ Р МЭК 31010-2021 для последующего анализа полученных результатов и выработки правил установления уровней доверия к конкретному ПО.

В процессах **разработки** ПО риски определяются для **среды разработки** на основе ГОСТ Р ИСО/МЭК 27005, а требования к УДПО – на основе ГОСТ Р 56939, ГОСТ Р 15408-3 и ГОСТ Р 12207.

Пример требований к безопасности ПО в процессе разработки

НИИАС

Требования к безопасности ПО при разработке	УДПО 1	УДПО 2	УДПО 3
Реализация встроенных средств защиты информации	-	+	+
Документированная архитектура ПО	-	-	+
Управление недостатками и запросами на изменение ПО	-	+	+
Моделирование угроз и описание поверхности атаки	-	+	+
Наличие регламента оформления кода	-	+	+
Композиционный анализ (SCA)	-	+	+
Статический анализ кода (SAST)	-	+	+
Динамический анализ API (DAST, FAST, API Sec,…)	-	-	+
Модульные тесты и фаззинг кода	-	-	+
Обеспечение целостности кода	-	+	+
Внутренняя приемка кода	-	+	+
Обеспечение безопасности ПО в процессе эксплуатации	-	+	+
Обучение сотрудников (план и его реализация)	-	+	+
Утвержденное Руководство по РБПО	+	+	+
Утвержденный план внедрения требований РБПО	+	+	+

Выводы

НИИАС

1. Проведен краткий анализ стандартов, определяющих качество программного обеспечения, применительно к характеристике «безопасность». Показано, что в текущей обстановке подхарактеристики показателя безопасности ПО как одной из основных характеристик качества ПО нуждаются в совершенствовании с привлечением специалистов по информационной безопасности. Предложена концепция введения новой подхарактеристики безопасности ПО (уровни доверия ПО) как показателя качества ПО.
2. Показана актуальность введения уровней доверия ПО как меры безопасности информации при ее обработке программным обеспечением. Предложена концептуальная трехуровневая система формирования уровней доверия ПО. Приведен пример требований к уровням безопасности ПО в процессе разработки применительно к среде разработки.
3. Предложенная концепция уровней доверия ПО нуждается в дальнейшей проработке с точки зрения развития теории защиты информации, уточнения требований и характеристик уровней доверия разных видов ПО для систем различного назначения. В частности, установлены, но подлежат дальнейшему дополнению и уточнению следующие общие показатели доверия ПО:
   – обязательность проверки на наличие уязвимостей и их устранение;
   – отсутствие в ПО недекларированных возможностей и нежелательных конструкций;
   – обеспечение целостности ПО;
   – необходимость наличия в ПО функций разграничения доступа;
   – наличие в ПО встроенных функций идентификации и аутентификации, различающихся по уровням доверия (ГОСТ Р 70262.1, 2);
   – применение в ПО криптографических функций при необходимости, в том числе для защиты каналов, данных, использования сервисов безопасности на базе PKI;
   – обеспечение функциональной надежности ПО, наличие функций резервирования (архивирования) и восстановления информации.
4. В зависимости от требований к системе, для которой рассматриваемое ПО разрабатывается, могут изменяться и требования к программному обеспечению.
5. Уровни доверия ПО - более широкое понятие, чем уровни безопасности ПО, поскольку к обеспечению конфиденциальности, целостности и доступности информации для определенных классов систем могут быть добавлены требования функциональной надежности и функциональной безопасности.

НИИАС

Нижегородская ул., д. 27, стр.1, г. Москва
www.niias.ru
info@vniias.ru

Больше о нас в официальном телеграмм-канале АО «НИИАС»