Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 05.07.2024 09:35:26
Уникальный программный ключ:
b47f96eea65a16e179f94d8f7b0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	**Методы верификации и тестирования программных средств**
Содержание	Основные понятия. Верификация и валидация. Характеристики качества программного обеспечения. Место верификации в жизненном цикле программного обеспечения. Задачи верификации в рамках жизненного цикла программного обеспечения. Верификация и другие процессы разработки и сопровождения программного обеспечения. Верификация различных артефактов жизненного цикла программного обеспечения. Международные стандарты, касающиеся верификации программного обеспечения. Методы верификации программного обеспечения. Экспертиза. Оценка программного обеспечения по Фагану. Другие виды общих экспертиз. Специализированные методы экспертиз. Методы анализа архитектуры программного обеспечения. Статический анализ. Формальные методы верификации. Логико- алгебраические модели. Исполнимые модели. Модели промежуточного типа. Классификация формальных методов. Методы и инструменты дедуктивного анализа. Методы и инструменты проверки моделей. Методы и инструменты проверки согласованности. Динамические методы верификации. Мониторинг. Тестирование. Виды тестирования. Критерии полноты тестирования. Техники построения тестов. Инструменты автоматизации тестирования. Синтетические методы. Тестирование на основе моделей. Мониторинг формальных свойств. Статический анализ формальных свойств. Синтетические методы генерации структурных тестов. Роль верификации в жизненном цикле разработки программного обеспечения. Модели жизненного цикла разработки программного обеспечения. Современные технологии разработки программного обеспечения. Сравнение технологий разработки программного обеспечения. Роли в проекте. Документы, разрабатываемые на разных этапах жизненного цикла. Тестирование программного обеспечения. Методы тестирования программного обеспечения. Методологии управления проектами. Современные технологии разработки программного обеспечения. Сравнение технологий разработки программного обеспечения.
Реализуемые компетенции	ПК-4. Способен проводить инструментальный анализ защищенности компьютерной системы и осуществлять поиск уязвимостей программного обеспечения. ПК-6. Способен к формированию и утверждению стратегии тестирования программных средств.
Результаты освоения дисциплины (модуля)	**ПК-4** **Знать:** принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных

	федеральных органов исполнительной власти по защите информации; организационные меры по защите информации. **Уметь**: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. **Владеть**: навыками выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнения анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок. **ПК-6** **Знать:** теорию различных стратегий тестирования; базовые понятия качества программного продукта и качества процесса разработки программного обеспечения; метрики и риски тестирования. **Уметь**: определять наиболее значимые критерии качества программного продукта; выделять оптимальный вариант; принимать решения в критических ситуациях. **Владеть**: навыками определения целей тестирования, уровня тестирования, ролей и обязанностей каждого члена команды; определения требования к тестовым данным; определения инструментальных средств для достижения целей тестирования; определения требований к окружению и программному обеспечению, необходимых для достижения целей тестирования; проведения анализа рисков и выработка плана по снижению рисков; оценки сроков выполнения тестирования; принятие решения об автоматизации тестирования; определения рабочих ресурсов (количества тестировщиков, списка рабочих станций, тестовых сред), для проведения тестирования; определения и документирования механизмов передачи продукта на тестирование.
Трудоемкость, з.е.	4
Формы отчетности	Зачет с оценкой, 7 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учеб. пособие вузов / В. И. Завгородний. – М.: Логос, 2001. – 264 с.: ил. – Гриф: Рек. УМО для студентов вузов. – Библиогр.: с. 259-263. – ISBN 5-94010-088-0. 2. Липаев, В. В. Надежность программных средств. – М.: СИНТЕГ, 1998. – 232 с.: прил. – (Информатизация России на пороге XXI века). – Библиогр.: с. 216-219. – ISBN 5-89638-008-9.
Дополнительная литература	1. Сорокин, А. А. (СевКавГТУ). Разработка и стандартизация программных средств и информационных технологий: учеб. пособие (курс лекций) / Александр Анатольевич Сорокин, Анатолий Александрович Сорокин; ГОУ ВПО Сев.-Кав. гос. техн. ун-т. – Ставрополь: Издательство СевКавГТУ, 2011. – 432 с.: ил. – Библиогр.: с. 418-419. – Прил.: с. 420-432.