АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Методы верификации**»**
по направлению 10.05.01 «Компьютерная безопасность» *(специалитет)*
специализация *«*Математические методы защиты информации*»*

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- ознакомление студента с предметом верификации ПО;
- обзор широкой палитры существующих методов и подходов;
- освещение преимуществ и ограничений, присущих методам верификации.

Задачи освоения дисциплины:

- развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций;
- формирование базовых знаний в области обеспечения качества программного обеспечения, как неотъемлемой части теории и практики разработки ПО, адресуемого к проблемам построения корректных и надежных программ, и имеющего важное методологическое значение как для подготовки специалистов в области современных информационных технологий, так и для поддержки разнообразных инновационных сфер деятельности;
- обучение студентов методам функционального тестирования, применяемым в различных сценариях разработки ПО, включая модульное тестирование, случайное тестирование, тестирование с использованием моделей, а также методам оценки полноты тестирования;
- обучение студентов базовым методам анализа корректности программ;
- обучение студентов основам жизненного цикла программного обеспечения и задачам верификации, возникающим в ходе разработки, внедрения и эксплуатации ПО.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к числу прикладных дисциплин в силу отбора изучаемого материала и занимает важное место в вариативной части дисциплин по выбору Б1.В.ДВ образовательной программы и читается в 10-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов дискретной математики, математической логики и теории алгоритмов, информатики, методов программирования, теории информации и системного анализа.

Основные положения дисциплины используются в дальнейшем при изучении дисциплин при прохождении практики и в последующей профессиональной деятельности.

3. Перечень планируемых результатов освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы,	Знать: основные средства и методы анализа программных реализаций на предмет уязвимостей Уметь: разрабатывать программы с защитой от уязвимостей

системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Владеть: навыками выявления и устранения уязвимостей
ПК-10 способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: способы, методы и критерии оценки эффективности реализации систем защиты информации Уметь: пользоваться способами, методами и критериями оценки эффективности реализации систем защиты информации Владеть: способами, методами и критериями оценки эффективности реализации систем защиты информации
ПК-11 способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знать: основные приёмы и методы создания программных закладок Уметь: противодействовать программным закладкам Владеть: навыками выявления уязвимостей в программных реализациях
ПК-15 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знать: способы, методы и критерии оценки эффективности реализации систем защиты информации Уметь: пользоваться способами, методами и критериями оценки эффективности реализации систем защиты информации Владеть: способами, методами и критериями оценки эффективности реализации систем защиты информации
ПК-19 способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать: основные виды и наиболее известные примеры программных уязвимостей Уметь: выявлять и устранять уязвимости программных реализаций и локализовать их последствия Владеть: навыками владения с современными отладчиками
ПСК-2.1 способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знать: группы типичных уязвимостей ПО Уметь: использовать СО модель компьютерной системы для создания эффективных алгоритмов безопасности Владеть: навыками работы с современными дизассемблерами и отдатчиками
ПСК-2.2 способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знать: математические методы оценки безопасности программных реализаций Уметь: оценивать опасность обнаруженных уязвимостей программных реализаций Владеть: приёмами анализа программных реализаций на предмет наличия уязвимостей
ПСК-2.3 способностью строить математические модели для оценки	Знать: математический аппарат построения адекватных систем оценки безопасности ПО

безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Уметь: проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности Владеть: основными методами математического аппарата по анализу несанкционированного доступа к ПК
ПСК-2.4 способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знать: специальные средства защиты в современных средах программирования Уметь: строить соответствующие математические модели Владеть: способами оценки и прогнозирования работы моделей безопасности
ПСК-2.5 способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации	Знать: статические и динамические методы анализы программных реализаций Уметь: выбирать адекватный инструмент для оценки эффективности безопасности ПО Владеть: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы (**108** часа).

5. Образовательные технологии

В ходе изучения дисциплины используются традиционные методы и формы обучения, а также технологии дистанционного обучения в ЭИОС.

При организации самостоятельной работы используются следующие образовательные технологии: самостоятельная работа, сопряженная с основными аудиторными занятиями (проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины); самостоятельная работа под контролем преподавателя в форме плановых консультаций, при подготовке к сдаче зачета; внеаудиторная самостоятельная работа при выполнении студентом лабораторных работ.

6. Контроль успеваемости

Программой дисциплины предусмотрены виды текущего контроля: Лабораторные работы.

Промежуточная аттестация проводится в форме: зачета.