АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Защита программ и данных**»**
по направлению 10.05.01 «Компьютерная безопасность» *(специалитет)*
специализация *«*Математические методы защиты информации*»*

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- освоение студентом основных методов и средств анализа программных реализаций;
- организация защиты ПО от воздействий вредоносного характера;

Задачи освоения дисциплины:

- формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия недокументированных возможностей;
- формирование навыков выявления вредоносного программного обеспечения и программных закладок;
- формирование навыков оценки опасности у обнаруженных вредоносных программ;
- развитие навыков планирования работ по локализации последствий и пресечению обнаруженной атаки;
- развитие навыков организации антивирусной защиты;
- формирование навыков защиты программных реализации от изучения и модификации.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к числу базовых дисциплин специализации Б1.Б в рамках профессионального цикла Б1 образовательной программы и читается в 8-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Информатика», «Аппаратные средства вычислительной техники», «Защита в операционных системах», «Системы и сети передачи информации», «Теория псевдослучайных генераторов», «Математические модели ИС», «Техническая защита информации», «Системный анализ», Теория игр и исследование операций», «Теория вычислительной сложности», «Неклассические логики».

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Модели безопасности компьютерных систем», «Основы построения защищенных компьютерных сетей», «Основы построения защищенных баз данных», «Криптографические методы защиты информации», «Криптографические протоколы», «Методы алгебраической геометрии в криптографии», «Анализ уязвимостей программного обеспечения», «Методы верификации», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

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
ОПК-2 способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать: известные математические модели безопасности компьютерных систем Уметь: анализировать и оценивать угрозы информационной безопасности объекта с помощью инструментов статистики, численных методов, теории алгоритмов Владеть: способами, методами и критериями оценки эффективности реализации систем защиты информации
ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знать: сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Уметь: анализировать и оценивать угрозы информационной безопасности объекта Владеть: методами анализа безопасности информационных систем на базе промышленных СУБД; - навыками формирования требований по защите информации
ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать: Способы анализа и оценки угрозы информационной безопасности объекта Уметь: применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы Владеть: методами анализа безопасности информационных систем на базе промышленных СУБД; - навыками формирования требований по защите информации
ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать: известные математические модели безопасности компьютерных систем Уметь: проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем Владеть: методами разработки математических моделей безопасности компьютерных систем
ПК-6 способностью участвовать в разработке проектной и технической документации	Знать: основные нормы работы с научно-технической, нормативной и организационно-распорядительной документацией

	Уметь: применять нормативно -техническую документацию в разработке проектной и технической документации Владеть: навыками разработки проектной и технической документации
ПК-7 способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Знать: методы, способы анализ проектных решений по обеспечению защищенности компьютерных систем Уметь: применять методы, способы анализ проектных решений по обеспечению защищенности компьютерных систем. Владеть: методами, способами анализ проектных решений по обеспечению защищенности компьютерных систем.
ПК-8 способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знать: принципы построения подсистем защиты информации Уметь: применять принципы построения подсистем защиты информации. Владеть: принципами построения подсистем защиты информации.
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: требования нормативно - технических документов по проведению сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации. Уметь: пользоваться нормативно - технических документов по проведению сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации. Владеть: приёмами, правилами проведению сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации.
ПК-18 способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения	Знать: основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; - принципы

информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	построения систем защиты информации Уметь: использовать средства защиты, предоставляемые системами управления базами данных; - проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований Владеть: навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем
ПК-20 способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знать: приёмы и правила восстановления работоспособности средств защиты информации при возникновении нештатных ситуаций Уметь: восстанавливать работоспособность средств защиты информации при возникновении нештатных ситуаций Владеть: приёмами и правилами восстановления работоспособности средств защиты информации при возникновении нештатных ситуаций

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); подготовка к тестированию; 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, тестирование.

Промежуточная аттестация проводится в форме: зачета.