АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Защита программ и данных**»**
по направлению 10.05.03 «Информационная безопасность автоматизированных систем»
(специалитет)
специализация *«*Безопасность открытых информационных систем*»*

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 вариативных дисциплин в рамках образовательной программы и читается в 9-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Языки программирования», «Технологии и методы программирования», «Безопасность операционных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Безопасность систем баз данных».

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Разработка и эксплуатация защищённых автоматизированных систем», «Безопасность открытых информационных систем» а также для прохождения практик и 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-3 - способностью	Знать:

применять языки, системы и инструментальные средства программирования в профессиональной деятельности	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
ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий	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-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать: принципы построения защиты информации АС Уметь: применять принципы построения подсистем защиты информации в АС. Владеть: принципами построения защиты информации в АС.
ПК-26 - способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать: основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; - принципы 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

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.