АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Вредоносные программы в компьютерных сетях»

по специальности 10.05.01 «Компьютерная безопасность»
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 ВО

Дисциплина относится к числу базовых дисциплин и читается в 5-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения. Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Математический анализ», «Программирование», «Дифференциальные уравнения».

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Моделирование информационных процессов», «Технология разработки программного обеспечения», «Анализ уязвимостей программного обеспечения», «Теоретико-числовые методы построения алгоритмов и систем защиты информации», а также для прохождения практик, защите ВКР и государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

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-1 Способен формировать комплекс	Знать:

мер для защиты информации ограниченного доступа, управлять процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; принципы построения систем защиты информации Уметь: использовать средства защиты, предоставляемые системами управления КС; проводить обоснование и выбор рационального решения по защите КС с учетом заданных требований Владеть: навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем
ПК-2 Способен осуществлять тестирование систем защиты информации компьютерных систем	Знать: требования нормативно - технических документов по проведению сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации. 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; навыками формирования требований по защите информации
ПК-6 Способен разрабатывать математические модели безопасности компьютерных систем	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

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;

- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение экзамена.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы, проверка решения задач

Итоговая аттестация проводится в форме: экзамен.