


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

**АННОТАЦИЯ**  
**РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**  
**«Вредоносные программы в компьютерных сетях»**  
**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 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 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-1 Способен формировать комплекс мер для защиты информации ограниченного	Знать: основные средства и способы обеспечения

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

доступа, управлять процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	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 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.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

## **6. Контроль успеваемости**

Программой дисциплины предусмотрены виды текущего контроля: Лабораторные работы, тестирование.

Промежуточная аттестация проводится в форме: зачета.