

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

**АННОТАЦИЯ**  
**РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**  
**«Модели безопасности компьютерных систем»**  
**по направлению 10.05.01 «Компьютерная безопасность» (специалитет)**  
**специализация «Математические методы защиты информации»**

### 1. Цели и задачи освоения дисциплины

#### Цели освоения дисциплины:

*Целью* дисциплины «Модели безопасности компьютерных систем» является обучение студентов принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками.

#### Задачи освоения дисциплины:

*Задачами* дисциплины являются:

- развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций;
- изучение основных формальных моделей политик безопасности, моделей дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;
- приобретение практических навыков разработки математических моделей безопасности для защищаемых компьютерных систем;
- формирование у будущего специалиста в области компьютерной безопасности таких качеств, как строгость в суждениях, творческое мышление, организованность и работоспособность, дисциплинированность, самостоятельность и ответственность.

### 2. Место дисциплины в структуре ОПОП

Дисциплина «Модели безопасности компьютерных систем» Б1.О.1.1.38 относится к числу базовых дисциплин программы подготовки специалистов по направлению 10.05.01 – «Компьютерная безопасность».

Дисциплина читается в 8-ом и 9-ом семестрах 4-ого и 5-ого курсов соответственно студентам очной формы обучения.


Для ее успешного изучения необходимы знания и умения, приобретенные в следующих предшествующих учебных дисциплинах: Организационное и правовое обеспечение информационной безопасности Теоретико-числовые методы в криптографии.

Результаты освоения дисциплины «Модели безопасности компьютерных систем» будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: Криптографические протоколы, Научно-исследовательская работа, при подготовке к сдаче государственного экзамена.

### 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 – 8 Способен применять методы	<b>Знать:</b> методы научных исследований при проведении разработок в области обеспечения безопасности

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

научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	<p>компьютерных систем и сетей</p> <p><b>Уметь:</b> применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p> <p><b>Владеть:</b> Способами применения методов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p>
ОПК - 11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	<p><b>Знать:</b> политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p> <p><b>Уметь:</b> разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p> <p><b>Владеть:</b> способностью разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p>

#### 4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 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 лабораторным работам, самостоятельная работа под контролем преподавателя в форме плановых консультаций, при подготовке к сдаче зачета и экзамена; внеаудиторная самостоятельная работа.

#### 6. Контроль успеваемости

Программой дисциплины предусмотрены виды текущего контроля: лабораторная работа.

Промежуточная аттестация проводится в форме: зачета и экзамена.