# *Аннотация*
# *к рабочей программе дисциплины*
# *«Безопасность вычислительных сетей»*

**по направлению 10.03.01 «Информационная безопасность»**
**(профиль «Безопасность автоматизированных систем»)**

**Общая трудоемкость дисциплины** составляет 5 зачетных единиц.(180 часов)

**Форма контроля**: экзамен 7 семестр.

Предполагаемые семестры: 7

**Цель**

- получение знаний и навыков работы, необходимых для разработки и эксплуатации автоматизированных систем;
- в изучение принципов построения информационных систем и принципов организации информационных систем в соответствии с требованиями по защите информации.

**Задачами курса** является изучение принципов построения информационных систем, основ администрирования вычислительных сетей, методов технической защиты информации, принципов организации информационных систем в соответствии с требованиями по защите информации.

**Учебная дисциплина *«Безопасность вычислительных сетей»*** является самостоятельным элементом в системе подготовки специалиста, относится к циклу Б1.В. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- принципы построения, проектирования и эксплуатации автоматизированных информационных систем.

В дисциплине «Безопасность вычислительных сетей» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- комплексное обеспечение информационной безопасности автоматизированных систем;
- интегрированные информационные системы в управлении.

**Краткое содержание дисциплины:**

Анализ и планирование безопасности вычислительной сети (ВС), средства защиты вычислительных сетей, безопасность уровня сетевых операционных систем, безопасность уровня сетевого взаимодействия, обеспечение безопасности сетевых приложений, использование стандартных средств Microsoft Windows 2000 Server для внедрения средств защиты локальной сети, особенности защиты информации в глобальных сетях.

**В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):**

ПК-4: Способность администрировать подсистемы информационной безопасности объекта защиты.

ПК-7: Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

В результате изучения дисциплины бакалавр должен:

**Знать:**

- принципы построения информационных систем;
- основы администрирования вычислительных сетей;

- принципы организации информационных систем в соответствии с требованиями по защите информации;
- эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы.

**Уметь:**

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.

**Владеть:**

- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- навыками выявления и уничтожения компьютерных вирусов;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- методами технической защиты информации.