МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Безопасность сетей ЭВМ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **5, 6**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	6 семестр	Всего	Единицы
1	Лекции	18	18	36	часов
2	Практические занятия	8	8	16	часов
3	Лабораторные работы	28	36	64	часов
4	Всего аудиторных занятий	54	62	116	часов
5	Самостоятельная работа	54	82	136	часов
6	Всего (без экзамена)	108	144	252	часов
7	Подготовка и сдача экзамена	0	36	36	часов
8	Общая трудоемкость	108	180	288	часов
		3.0	5.0	8.0	З.Е.

Зачёт: 5 семестр
Экзамен: 6 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Обучить студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

1.2. Задачи дисциплины

- Дать основы:
- – архитектуры вычислительных сетей;
- – программно-аппаратных и технических средств создания сетей;
- – принципов построения сетей и управления ими;
- – использования программных и аппаратных технологий защиты сетей;
- – методологии проектирования, развертывания и сопровождения безопасных сетей;
- – обследования и анализа защищенных вычислительных сетей.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность сетей ЭВМ» (Б1.Б1.05.04) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность сетей ЭВМ, Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Безопасность сетей ЭВМ.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ;
- ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ;
- ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ;
- ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

В результате изучения дисциплины обучающийся должен:

- **знать** средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.
- **уметь** применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.
- **владеть** навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
5 семестр
1 Основные понятия информационных сетей
2 Основы построения современных локальных сетей
3 Средства реализации межсетевого взаимодействия
4 Перспективные направления развития и проблемы информационных сетей
6 семестр
5 Основные понятия информационной безопасности сетей ЭВМ
6 Технологии обеспечения безопасности в локальных сетях
7 Обеспечение безопасности межсетевого взаимодействия