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

Техническая защита информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	16	16	часов
3	Лабораторные работы	20	20	часов
4	Всего аудиторных занятий	64	64	часов
5	Самостоятельная работа	44	44	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 7 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов:

- по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях;
- по вопросам анализа защищенности автоматизированных систем;
- по вопросам проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- по вопросам участия в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем;
- по вопросам участия в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
- по вопросам проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки информации.

1.2. Задачи дисциплины

– дать основы: выявление на объекте информатизации или в выделенном помещении технических каналов утечки информации; оценка уровня шумов/информативных сигналов/помех; оценка соответствия объекта информатизации или выделенного помещения требованиям по безопасности от утечки информации по техническим каналам

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» (Б1.Б.06.06) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности, Управление средствами защиты информации, Физика.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

– ПК-3 способностью проводить анализ защищенности автоматизированных систем;

– ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

– ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем;

– ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;

– ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;

В результате изучения дисциплины обучающийся должен:

– **знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам

– **уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации

– **владеть** методами и средствами выявления угроз безопасности автоматизированным

системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
7 семестр
1 Концепция инженерно-технической защиты информации
2 Теоретические основы инженерно-технической защиты информации
3 Физические основы защиты информации
4 Технические средства добывания и инженерно-технической защиты информации
5 Организационные основы инженерно-технической защиты информации
6 Методическое обеспечение инженерно-технической защиты информации