

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 26.09.2023 10:54:08
Уникальный программный ключ:
27e516f4c088deb62ba68945f4406e13fd454355

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 (лабораторный практикум)

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: **5**

Семестр: **9**

Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лабораторные работы	36	36	часов
2	Всего аудиторных занятий	36	36	часов
3	Всего (без экзамена)	36	36	часов
4	Общая трудоемкость	36	36	часов
		1.0	1.0	З.Е.

Зачёт: 9 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

ическая 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

- 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 (лабораторный практикум)» (ФТД.4) относится к блоку ФТД.4.

Предшествующими дисциплинами, формирующими начальные знания, являются: Теоретические основы компьютерной безопасности, Техническая защита информации.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Подготовка к сдаче и сдача государственного экзамена.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- 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;

В результате изучения дисциплины обучающийся должен:

- **знать** знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.
- **уметь** 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** 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
9 семестр
1 Технические средства добывания и инженерно-технической защиты информации