Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ

по дисциплине

Б.1.1.18 «Техническая защита информации»

направления подготовки
10.03.01«Информационная безопасность»
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 3
семестр – 6
зачетных единиц – 3
часов в неделю – 3
всего часов – 108
в том числе:
лекции – 16
лабораторные занятия – 32
самостоятельная работа – 60
зачет – 6 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов методам, технологиям и применению специальных технических средств для защиты информации от ведения технической разведки.

Задачи изучения дисциплины:

– изучить общие принципы организации инженерно-технической защиты информации

– изучить основные методы ведения технической разведки и методы противодействия технической разведке, научиться определять преимущества и недостатки этих методов в рамках решения конкретных задач по защите информации

– получить практические навыки по организации комплексных работ по инженерно-технической защите информации

– научиться применять технические средства для проведения мероприятий по инженерно-технической защите информации

– научиться применять инструментальные средства для оценки эффективности мероприятий по противодействия технической разведке

2. Место дисциплины в структуре ООП ВО

Дисциплина «Техническая защита информации» относится к числу дисциплин базовой (общепрофессиональной) части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Физика» - знать физическую природу электромагнитных и акустических колебаний и волн, оптику, основы электромагнетизма, основы теории измерений

цикл математических дисциплин — знать и уметь применять методы анализа функций, основы интегрального и дифференциального исчисления, основы векторного анализа и алгебры, теорию вероятностей и мат. статистики, знать и уметь строить и анализировать математические модели объектов различной природы, а также использовать методы численного анализа для исследования построенных моделей

«Электроника и схемотехника», «Основы радиотехники» – знать основные средства и способы электромагнитной передачи информации, основы теории цепей, основы электродинамики и распространения радиоволн, основы теории радиопередающих и радиоприемных устройств.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ПК-1 - способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения

ПК-6 - способность использовать нормативные правовые акты в своей профессиональной деятельности

ПК-11 - способность разрабатывать и исследовать модели автоматизированных систем

ПК-13 - способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК-14 - способность проводить анализ рисков информационной безопасности автоматизированной системы

ПК-32 - способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите

ПК-33 - способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

Студент должен знать:

1. общие принципы организации инженерно-технической защиты конфиденциальной информации
2. основные технические каналы утечки информации и их свойства
3. физические и физико-технические основы реализации технических каналов утечки информации
4. математические модели, методы и подходы к описанию физических и физико-технических явлений, возникающих при реализации технических каналов утечки информации
5. возможности основных методов ведения технической разведки конфиденциальной информации
6. основные требования отраслевых и распорядительных нормативных документов по технической защите информации

Студент должен уметь:

1. оценивать степень опасности технических каналов утечки конфиденциальной информации
2. применять специальные технические средства для проведения мероприятий по инженерно-технической защите информации
3. оценивать степень опасности технических каналов утечки конфиденциальной информации

4. блокировать основные технические каналы утечки информации
5. проводить математическое моделирование и теоретический анализ технических каналов утечки информации

Студент должен владеть:

1. методиками и способами инструментальной оценки степени опасности технических каналов утечки конфиденциальной информации на объекте информатизации
2. методиками проведения инструментальной оценки эффективности мероприятий по блокированию основных технических каналов утечки информации.