

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Защищенные информационные системы»

(наименование дисциплины)

10.04.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Организация и технологии защиты информации

(направленность (профиль) /специализация образовательной программы)

высшее образование – магистратура

(уровень образования)

Магистр

(квалификация, присваиваемая по специальности или направлению подготовки)

очно-заочная

(форма обучения)

2022

(год набора)

1. Цель освоения дисциплины

Цель освоения дисциплины – обучить студентов принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления. Знания и практические навыки, полученные из курса специальности будут применены при разработке курсовых и дипломных проектов.

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть учебного плана образовательной программы и реализуется на 2 курсе(-ах) в 4 семестре(-ах)

3. Компетенции, формируемые в результате освоения дисциплины

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

4. Общая трудоемкость дисциплины

5 зачетные единицы (180 академических часа(-ов))

5. Форма (формы) промежуточной аттестации обучающихся

Экзамен.

6. Разделы (если имеются) и темы дисциплины

Тема 1. Проблемы безопасности информационной безопасности

Тема 2. Основные понятия политики безопасности

Тема 3. Структура политики безопасности

Тема 4. Роль стандартов информационной безопасности

Тема 5. Международные стандарты информационной безопасности

Тема 6. Отечественные стандарты безопасности информационных технологий

Тема 7. Основные понятия и определения, используемые при описании моделей безопасности информационных систем

Тема 8. Математические модели дискреционного и мандатного разграничения доступа

Тема 9. Модели ролевого разграничения доступа

Тема 10. Проблемы применения моделей безопасности при построения защищенных информационных систем

Тема 11. Концепция глобального управления безопасностью

Тема 12. Функционирование системы управления средствами безопасности

Тема 13. Средства защиты информационных систем

Тема 14. Процесс оценки рисков и управления риском информационной безопасности

Тема 15. Программный инструмент для управления рисками ИБ

Тема 16. Обеспечения безопасности Web-серверов

7. Автор(ы) рабочей программы

Голембиовская О.М., к.т.н., доцент

Шинаков К.Е., к.т.н., доцент