

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Методы и средства криптографической защиты информации»

(наименование дисциплины)

10.03.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

(направленность (профиль) /специализация образовательной программы)

высшее образование – бакалавриат

(уровень образования)

бакалавр

(квалификация, присваиваемая по специальности или направлению подготовки)

очная

(форма обучения)

2021

(год набора)

1. Цель освоения дисциплины

Обучение основополагающим принципам защиты информации с помощью криптографических методов, грамотному выбору и применению средств криптографической защиты информации в программной и аппаратной реализации, а также ознакомление с перспективами развития синтеза и анализа современных криптографических систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть учебного плана, и реализуется на 3 курсе(-ах) в 6 семестре(-ах)

3. Компетенции, формируемые в результате освоения дисциплины

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

4. Общая трудоемкость дисциплины

4 зачетные единицы (144 академических часа(-ов))

5. Форма (формы) промежуточной аттестации обучающихся

Экзамен

6. Разделы (если имеются) и темы дисциплины

1. История криптографии.
2. Модели шифров
3. Криптографическая стойкость
4. Имитостойкость и помехоустойчивость шифров
5. Принципы построения криптографических алгоритмов
6. Синтез шифров
7. Схемы шифрования с открытыми ключами

8. Криптографические хэш-функции
9. Электронная цифровая подпись
10. Ключевые системы, криптографические протоколы
11. Особенности использования вычислительной техники в криптографии
12. Вопросы организации сетей засекретной связи
13. Перспективы развития криптографических систем

7. Автор(ы) рабочей программы

Шпичак С.А., к.т.н., доцент