АННОТАЦИЯ

Дисциплины

Б1.О.32 «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Специальность – *10.05.03* «*Информационная безопасность автоматизированных систем*»

Квалификация (степень) выпускника – *специалист по защите информации*

Специализация – *Безопасность автоматизированных систем на железнодорожном транспорте*

**1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина относится к обязательной части блока 1 «Дисциплины (модули)».

**2. Цель и задачи дисциплины**

Целью изучения дисциплины является формирование у обучающихся способности использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Для достижения цели дисциплины решаются следующие задачи:

* формирование о обучающихся знаний о криптографических методах, алгоритмах, протоколах, используемых для защиты информации в автоматизированных системах;
* формирование у обучающихся умений, связанных с разработкой и анализом программных моделей средств криптографической защиты информации;
* формирование у обучающихся навыков использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач.

**3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующих компетенций, сформированность которых, оценивается с помощью индикаторов достижения компетенций:

| Компетенция | Индикатор компетенции |
| --- | --- |
| ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности | ОПК-10.1.1. Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| ОПК-10.2.1. Умеет разрабатывать и анализировать программные модели средств криптографической защиты информации |
| ОПК-10.3.1. Имеет навыки использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач |

В рамках изучения дисциплины осуществляется практическая подготовка обучающихся к будущей профессиональной деятельности. Результатом обучения по дисциплине является формирования у обучающихся практических навыков.

* использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач.

**4. Содержание и структура дисциплины**

1. Общие сведения о криптографии.

2. Симметричные криптосистемы.

3. Асимметричные криптосистемы.

4. Криптографические протоколы.

5. Средства криптографической защиты информации.

**5. Объем дисциплины и виды учебной работы**

Объем дисциплины – 7 зачетных единиц (252 часа), в том числе:

лекции – 64 часа;

лабораторные работы – 80 часов;

самостоятельная работа – 68 часов.

Форма контроля знаний – экзамен в 5 семестре, зачет в 6 семестре.