АННОТАЦИЯ

Дисциплины

*Б1.В.02 «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»*

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

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

Специализация – *Безопасность автоматизированных систем на транспорте*

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

Дисциплина относится к обязательной части/части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)». (*вариативная часть)*

**2. Цель и задачи дисциплины**

Целью изучения дисциплины является расширение и углубление профессиональной подготовки для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности и специализацией «Информационная безопасность автоматизированных систем на транспорте»

Для достижения цели дисциплины решаются следующие задачи:

- изучение основных угроз безопасности информации и моделей нарушителя в информационных системах;

- изучение основных принципов формирования политики безопасности в информационных системах;

- изучение базовых моделей разграничения доступа компьютерной системы

- изучение основных принципов антивирусной защиты автоматизированных систем.

**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 |
| --- | --- |
| ПК-1. Тестирование систем защиты информации автоматизированных систем | ПК-1.1.3. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| ПК-1.1.4. Знает основные меры по защите информации в автоматизированных системах |
| ПК-1.3.3. Имеет навыки выявления основных угроз безопасности информации в автоматизированных системах |
| ПК-2. Разработка проектных решений по защите информации в автоматизированных системах | ПК-2.1.5. Знает принципы формирования политики информационной безопасности в автоматизированных системах |
| ПК-2.2.2. Умеет определять типы субъектов доступа и объектов доступа, являющихся объектами защиты |
| ПК-2.2.3. Умеет определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе |
| ПК-2.3.1. Имеет навыки разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах |

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

- ПК-1.3.3. Имеет навыки выявления основных угроз безопасности информации в автоматизированных системах

- ПК-2.3.1. Имеет навыки разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах

**4. Содержание и структура дисциплины**

1 Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем

2 Основные виды моделей разграничения доступа

3 Антивирусная защита автоматизированных систем

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

Объем дисциплины – 4 зачетные единицы (144 час.), в том числе:

лекции – 32 час.

практические занятия – 48 час.

самостоятельная работа – 60 час.

Форма контроля знаний – зачет, курсовой проект