

Б1.В.ДВ.04.02 Защита информационных процессов на транспорте

Объем дисциплины (модуля) 5 ЗЕТ (180 час)

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цель дисциплины: Формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.

Задачи дисциплины: Изучение основных аспектов деятельности по созданию, обеспечению функционирования и контролю эффективности комплексной системы защиты информации на предприятии. Изучение структуры комплексной системы защиты информации на предприятии. Обобщение основополагающих нормативно-правовых принципов организации системы защиты информации.

Изучение методов проведения анализа и управления информационными рисками предприятия.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ

ПК-2: Способен администрировать средства защиты информации прикладного и системного программного обеспечения

ПК-2.7: Способен выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности в области моделирования и анализа сложных естественных и искусственных систем

ПК-3: Способен устанавливать и настраивать средства защиты информации в автоматизированных системах

ПК-3.3: Знает основные меры по защите информации в автоматизированных системах

ПК-3.2: Владеет навыками установки и настройки средств защиты информации в автоматизированных системах

ПК-3.1: Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

ПК-4: Способен проводить работы по техническому обслуживанию защищенных технических средств защиты информации

ПК-4.3: Выполняет техническое обслуживание технических средств обработки информации в защищенном исполнении

ПК-4.2: Знает порядок аттестации объектов информатизации на соответствие требованиям безопасности информации

ПК-4.1: Знает проектную документацию на систему защиты объекта информатизации

ПК-5: Способен проводить мониторинг защищенности информации в автоматизированных системах

ПК-5.3: Анализирует недостатки в функционировании системы защиты информации автоматизированной системы

ПК-5.4: Применяет технические средства контроля эффективности средств защиты информации

ПК-5.1: Проводит мониторинг угроз безопасности информации в автоматизированных системах

ПК-5.2: Принимает меры защиты информации при выявлении новых угроз безопасности информации

ПК-6: Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах

ПК-6.1: Применяет руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

В результате освоения дисциплины обучающийся должен

Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
анализировать и оценивать угрозы информационной безопасности;
применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.

Владеть: методами и средствами выявления угроз безопасности автоматизированным системам;
методами формирования требований по защите информации;
методами анализа и формализации информационных процессов объекта и связей между ними;
методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Общие положения об информационной безопасности для телекоммуникационных систем

Раздел 2. ViPNet [Администратор] и его основные модули

Раздел 3. ViPNet [Координатор] и его основные модули
Раздел 4. ViPNet [Клиент] - характеристика и основные функции
Раздел 5. Типовые схемы применения технологии ViPNet