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

Объем дисциплины (модуля) **5 ЗЕТ (180 час)**

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ
ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты
:
:
:
:
:
:
:
:
:
ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
:
:
:
:
:
:
:
:
:
ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
:
:
:
:
:
:
:
:
:
ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
:
:
:
:
:
:

:
:
:
ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
:
:
:
:
:
:
:
:
:
ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
:
:
:
:
:
:
:
:
:
ПСК-1: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
:
:
:
:
:
:
:
:
:
ПСК-4: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
:
:
:
:
:
:
:
:
:
ПСК-6: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

:
:
:
:
:
:
:
:
:

В результате освоения дисциплины обучающийся должен

Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Уметь: осуществлять меры противодейтствия нарушениям сетевой безопасности с испольованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проетирования, 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 докмуентов.

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