АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ»
по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Дисциплина «Виртуальные частные сети» является одной из составляющих общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования федерального государственного образовательного стандарта высшего профессионального образования по специальности "Информационная безопасность автоматизированных систем". Цель курса – ознакомление студентов с основными техническими средствами построения виртуальных частных сетей.

Задачи освоения дисциплины:

изучить основы построения виртуальных частных сетей (VPN);

рассмотреть различные варианты и схемы создания VPN;

ознакомиться со стандартными протоколами VPN и управлением криптографическими ключами в VPN.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Виртуальные частные сети» изучается в 7 семестре и относится к вариативной части дисциплин блока Б1, предназначенного для студентов, обучающихся по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика»; «Основы информационной безопасности», «Теория информации», «Техническая защита информации».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информатики и теории информации;

способность использовать нормативные правовые документы;

способность анализировать социально-значимые проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Компьютерные сети»; «Модели безопасности компьютерных систем»; «Безопасность операционных систем»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Криптографические методы защиты информации.

ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
1	2
ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий	**Знать:** основные характеристики современных виртуальных частных сетей **Уметь:** осваивать новые образцы программных, технических средств и информационных технологий, относящихся к виртуальным частным сетям **Владеть:** навыками освоения новых образцов программных, технических средств и информационных технологий, относящихся к виртуальным частным сетям
ПК-10 - способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:** основы электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов виртуальных частных сетей **Уметь:** применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов виртуальных частных сетей **Владеть:** навыками применения знаний в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов виртуальных частных сетей в сфере профессиональной деятельности
ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	**Знать:** Основы проектирования системы управления информационной безопасностью автоматизированной системы **Уметь:** проектировать системы управления информационной безопасностью автоматизированной системы **Владеть:** Навыками проектирования системы управления информационной безопасностью автоматизированной системы

1	2
ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**Знать:** основные контрольные проверки работоспособности применяемых средств защиты информации, относящиеся к виртуальным частным сетям (ВЧС) **Уметь:** проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации, относящиеся к виртуальным частным сетям **Владеть:** навыками проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации, относящихся к ВЧС
ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**Знать:** основные элементы инструментального мониторинга защищенности информации в ВЧС и типовые каналы утечки информации **Уметь:** проводить инструментальный мониторинг защищенности информации в ВЧС и выявлять каналы утечки информации **Владеть:** навыками проведения инструментального мониторинга защищенности информации в ВЧС
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**Знать:** основы организации разработки, внедрения, эксплуатации и сопровождения ВЧС с учетом требований информационной безопасности **Уметь:** организовывать разработку, внедрение, эксплуатацию и сопровождение ВЧС с учетом требований информационной безопасности **Владеть:** навыками организации разработки, внедрения, эксплуатации и сопровождения ВЧС с учетом требований информационной безопасности
ПК-24 - способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**Знать:** основы эффективного применения информационно-технологических ресурсов ВЧС с учетом требований информационной безопасности **Уметь:** применять информационно-технологические ресурсы ВЧС с учетом требований информационной безопасности **Владеть:** навыками применения информационно-технологических ресурсов ВЧС с учетом требований информационной безопасности

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 часа).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекционные занятия, интерактивный опрос в ходе лекций, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

При организации самостоятельной работы занятий используются образовательные технологии развивающего, проблемного и проектного обучения.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на лекциях, написание рефератов.

Промежуточная аттестация проводится в форме зачёта.