МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Черепанов Иван Николаевич**
Лунегов Игорь Владимирович

Рабочая программа дисциплины

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

Код УМК 68688

Утверждено
Протокол №4
от «24» июня 2021 г.

Пермь, 2021

1. Наименование дисциплины

Виртуальные частные сети

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем
направленность Безопасность открытых информационных систем

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Виртуальные частные сети** у обучающегося должны быть сформированы следующие компетенции:

10.05.03 Информационная безопасность автоматизированных систем (направленность : Безопасность открытых информационных систем)

ОПК.2 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Индикаторы

ОПК.2.3 Применяет на практике опыт решения задач с использованием базовых алгоритмов, анализа типов коммуникаций и интеграции различных типов программного обеспечения

ПК.1 Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты

Индикаторы

ПК.1.1 Проводит моделирование безопасности информационных систем

ПК.5 Способен анализировать уязвимости внедряемой системы защиты информации

Индикаторы

ПК.5.3 Строит модели угроз безопасности информации автоматизированной системы

4. Объем и содержание дисциплины

Специальность	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	11
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Виртуальные частные сети.Первый семестр

Основы VPN

Изучение диапазонов не лицензируемых частот.
Описание технологий прямого расширения спектра и модуляций определенных в стандарте 802.11
Проблема многолучевого распространения. Технология разнесенного приема

Архитектура VPN

Теория антенн
Ограничения по использованию антенн
Общие вопросы выбора и размещения антенн

Топологии виртуальных частных сетей

Особенности технологий в беспроводных локальных сетях
Канальные планы в диапазоне 2,4 и 5 ГГц
Реализация одновременной работы на разных скоростях передачи данныхи
Основы работы беспроводных полно-связанных (MESH) сетей

Правовые аспекты применения технологии VPN

Точки доступа, беспроводные мосты, антенны и вспомогательное оборудование
Клиентские адаптеры для подключения к беспроводным локальным сетям
Устройства управления контроля и обслуживания беспроводных локальных сетей
Особенности Точек доступа Enterprise класса

Основные протоколы и стандарты VPN

Использование беспроводных мостов и альтернативные способы решения задач
Функциональные роли оборудования в радио сети
Информация необходимая для расчета пролета между двумя беспроводными мостами

Маршрутизация, протоколы динамической маршртутизации

Описание утилит по настройке клиентских адаптеров
Установка и настройка утилиты Aironet Desktop Utility

Основы конфигурации сетей

Наладка автономных точек доступа
Настройка автономных точек доступа
Наладка и настройка беспроводных мостов

Безопасность VPN

Первоначальная безопасность в стандарте 802.11
Уязвимости безопасности в беспроводных локальных сетях
Решения компании Cisco Sytems по обеспечения безопасности в беспроводных локальных сетях
Настройка сервера Cisco Secure ACS для обеспечения аутентификации б беспроводных локальных сетях

Итоговое контрольное мероприятие

Итоговое контрольное мероприятие проводится в виде зачета, в письменной форме. Так же при ответе задаются дополнительные вопросы по всему курсе дисциплины. Вопросы к зачету:
1. Какое утверждение точно описывает Cisco IOS и зоны политики на основе брандмауэра?
2. При использовании Cisco IOS зоны политики на основе межсетевого экрана, какая политика применяется?

3. Какой тип пакета не может быть отфильтрован по исходящим ACL?
4. Какие зоны в основе политике брандмауэра определяется системой и распространяется на трафик, предназначенный для маршрутизатора или происходящих из роутера?
5. Какое утверждение правильно описывает тип фильтрации брандмауэра?
6. В дополнение к критериям, используемым расширенные ACL, какие условия используются CBAC для фильтрации трафика?
7. Какое утверждение описывает характеристики фильтрации пакетов и брандмауэры с отслеживанием состояния, как они относятся к модели OSI?
8. Какие три действия могут в основе Cisco IOS политики брандмауэра предпринять, если настроены с Cisco SDM?
9. Маршрутизатор имеет CBAC настроен и входящих ACL применяется к внешнему интерфейсу. Какие действия предпринимает маршрутизатор предпринять после входящего к исходящему трафику,и какая новая запись создается в таблице состояний?
10. Для брандмауэр с отслеживанием состояния, какая информация хранится в течение сессии динамическую таблицу?
11. При настройке зоны основе Cisco IOS политики брандмауэра, которые три действия могут быть применены к классу трафика?
12. Какие два параметры отслеживаются CBAC для трафика TCP, но не для трафика UDP?
13. Каков первый шаг в настройке зоны основе Cisco IOS политики брандмауэра с помощью интерфейса?
14. Какие две характеристики списка ACL?
15. Какой тип пакетов выходе сети организации должна быть заблокирован ACL?
16. Если включено ведение журнала для записи ACL, то как маршрутизатор пакетов фильтруется ACL?
17. Автоматическое получение IP-адреса.
18. Управляющие протоколы Интернета.
19. Тестирование TCP/IP.
20. Утилиты командной строки для работы с сетью.
21. Служба имен доменов.
22. Пространство имен домена.
23. Разрешение имени.
24. Прямой и обратный запросы.
25. Технологии беспроводных сетей.
26. Топологии беспроводных сетей.
27. Методы доступа к сети.
28. Сервисы.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Семенов, Ю. А. Алгоритмы телекоммуникационных сетей. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 757 с. — ISBN 978-5-4497-1634-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/120470

2. Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 с. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/87999.html

Дополнительная:

1. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 428 с. — ISBN 978-5-4497-0350-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/89464.html

2. Лабораторный практикум по дисциплине Методы и средства защиты информации в компьютерных сетях / составители А. Г. Симонян, Т. Б. К. Режеб. — Москва : Московский технический университет связи и информатики, 2015. — 58 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/61742.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://compress.ru/ ежемесячный компьютерный журнал «КомпьютерПресс
https://ru.bmstu.wiki/ Национальная библиотека им. Н. Э. Баумана
https://www.intuit.ru/ Национальный открытый университет ИНТУИТ

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Виртуальные частные сети** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
Перечень используемого программного обеспечения:
- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Plaer";
- программа просмотра интернет контента (браузер) "Google Chrome"

Дополнительно в рамках курса будут применяться технологии сетевого обмена данными по средствам стека протоколов TCP/IP, алгоритмы симметричного и асимметричного шифрования, протоколы вирутальных частных сетей (PPTP, L2TP, TLS, IPSec)

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия, групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской.

Лабораторные занятия проводятся в Компьютерном классе кафедры радиоэлектроники и защиты информации с техническим оснащением, указанным в паспорте.

Аудитория для самостоятельной работы: компьютерный класс кафедры радиоэлектроники и защиты информации ,в том числе помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Виртуальные частные сети

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.2

Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.2.3 Применяет на практике опыт решения задач с использованием базовых алгоритмов, анализа типов коммуникаций и интеграции различных типов программного обеспечения	знать методы проектирования и эксплуатации виртуальных частных сетей	**Неудовлетворител** Отсутствие знаний проектирования и эксплуатации виртуальных частных сетей **Удовлетворительн** Общие, но не структурированные знания методов проектирования и эксплуатации виртуальных частных сетей **Хорошо** Сформированные, но содержащие отдельные пробелы знания методов проектирования и эксплуатации виртуальных частных сетей **Отлично** Сформированные систематические знания методов проектирования и эксплуатации виртуальных частных сетей

ПК.1

Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.1.1 Проводит моделирование безопасности информационных систем	Знать методы разработки политики информационной безопасности открытых информационных систем. Уметь создавать, анализировать, разрабатывать и реализовывать политики информационной безопасности открытых информационных систем Владеть навыками работы политиками информационной безопасности открытых информационных систем.	**Неудовлетворител** Отсутствие знаний по разработке и реализации политики информационной безопасности открытых информационных систем **Удовлетворительн** Общие, но не структурированные знания по разработке и реализации политики информационной безопасности открытых информационных систем **Хорошо** Сформированные, но содержащие отдельные пробелы знания по разработке и реализации политики информационной безопасности открытых информационных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Сформированные систематические знаний по разработке и реализации политики информационной безопасности открытых информационных систем

ПК.5

Способен анализировать уязвимости внедряемой системы защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.3 Строит модели угроз безопасности информации автоматизированной системы	Знать методы построения моделей угроз информационной безопасности автоматизированной системы, типам угроз и методикам управления рисками	**Неудовлетворител** Отсутствие знаний по методам построения моделей угроз информационной безопасности автоматизированной системы, типам угроз и методикам управления рисками **Удовлетворительн** Общие, но не структурированные знания по методам построения моделей угроз информационной безопасности автоматизированной системы, типам угроз и методикам управления рисками **Хорошо** Сформированные, но содержащие отдельные пробелы по методам построения моделей угроз информационной безопасности автоматизированной системы, типам угроз и методикам управления рисками **Отлично** Сформированные систематические знаний по методам построения моделей угроз информационной безопасности автоматизированной системы, типам угроз и методикам управления рисками

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 43 до 60
«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Основы VPN **Входное тестирование**	У студентов проверяются знания освоенных ранее дисциплин "Информатика", "Организация ЭВМ и систем".
ПК.1.1 Проводит моделирование безопасности информационных систем **ОПК.2.3** Применяет на практике опыт решения задач с использованием базовых алгоритмов, анализа типов коммуникаций и интеграции различных типов программного обеспечения	Топологии виртуальных частных сетей **Защищаемое контрольное мероприятие**	Знание методов проектирования и эксплуатации виртуальных частных сетей
	Безопасность VPN **Защищаемое контрольное мероприятие**	Знание методов инструментального мониторинга виртуальных частных сетей

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Проводит моделирование безопасности информационных систем **ОПК.2.3** Применяет на практике опыт решения задач с использованием базовых алгоритмов, анализа типов коммуникаций и интеграции различных типов программного обеспечения **ПК.5.3** Строит модели угроз безопасности информации автоматизированной системы	Итоговое контрольное мероприятие **Письменное контрольное мероприятие**	Знание архитектуры VPN, основных методов построение защищенных каналов связи

Спецификация мероприятий текущего контроля

Основы VPN

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
При тестировании студентами допущено ошибок менее 10%	81
При тестировании студентами допущено ошибок менее 30%	61
При тестировании студентами допущено ошибок менее 50%	41
При тестировании студентами допущено ошибок более 50%	0

Топологии виртуальных частных сетей

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
знание архитектуры VPN	10
Знание основ защищенного обмена информацией	10
знание топологий VPN	10

Безопасность VPN

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знание основных протоколы и стандарты VPN	10
умение конфигурировать защищенных сетей	10
знание протоколов динамической маршрутизации	10

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Умение проектирования Виртуальных сетей	10
Умения конфигурация VPN сервер на IPSec	10
Знание основных протоколов создания VPN	10
Знание асинхронных методов шифрования, инфраструктуры открытых колючей	5
Знание базовых архитектура виртуальных сетей	5