МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Моисеев Виктор Игоревич**
Лунегов Игорь Владимирович

Рабочая программа дисциплины

СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Код УМК 81654

Утверждено
Протокол №4
от «24» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Сети и системы передачи информации

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в вариативную 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 **Сети и системы передачи информации** у обучающегося должны быть сформированы следующие компетенции:

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

ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности

ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем

ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы

ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем

ПК.22 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

ПК.28 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы

ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы

ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

ПК.4 способность проводить анализ защищенности автоматизированных систем

ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы

ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

4. Объем и содержание дисциплины

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	7
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	0
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Экзамен (7 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Сети и системы передачи информации. Первый семестр
Курс дает студентам основные представления о передаче и преобразовании информации в системах передачи информации. Курс дает студентам знания, умения и навыки для планирования, построения и эксплуатации сетей передачи информации

Входной контроль
До изучения данной дисциплины студентами должны быть изучены дисциплины "Основы операционных систем", "Программирование", "Английский язык".

1. Уровни модели OSI.
Примеры протоколов работающих на разных уровнях. Связи между уровнями. Прямые и обратные зоны DNS. MTU и фрагментация на разных уровнях.

2. Основы конфигурирования коммутаторов и маршрутизаторов на базе операционной системы Cisco IOS.
Архитектура маршрутизатора/коммутатора: Management/Control/Data plane.

3. Протокол IPv4. Адресация в протоколе IPv4, распределение подсетей, маски переменной длины. Типы вещания: unicast, broadcast, multicast, anycast. MTU и фрагментация. Инструменты для мониторинга и поиска неполадок в IPv4. Белые/серые адрес
Протокол IPv4. Адресация в протоколе IPv4, распределение подсетей, маски переменной длины. Типы вещания: unicast, broadcast, multicast, anycast. MTU и фрагментация. Практика по настройке IPv4 и поиску неполадок с использованием штатных средств ОС и анализатора пакетов WireShark.

4. Процесс и принципы маршрутизации по назначению. Рекурсивный просмотр таблицы маршрутизации. Метрика, административная дистанция. Процесс построения таблицы маршрутизации. Маршрутизация по политике.
Практика по настройке IPv4 и поиску неполадок с использованием штатных средств ОС и анализатора пакетов WireShark.
Процесс и принципы маршрутизации по назначению. Рекурсивный просмотр таблицы маршрутизации. Метрика, административная дистанция, область видимости маршрута. Процесс построения таблицы маршрутизации. Маршрутизация по политике.

6. Динамическая маршрутизация. Основные принципы. Механизмы блокировки циклов. Редистрибьюция маршрутов. Протоколы OSPF, EIGRP, BGP. Автономная система. Настройка протокола OSPF для корневой зоны на маршрутизаторе с Cisco IOS.
Динамическая маршрутизация. Основные принципы. Механизмы блокировки циклов. Редистрибьюция маршрутов. Протоколы OSPF, EIGRP, BGP. Автономная система.
Практика. Настройка протокола OSPF для нескольких зон на маршрутизаторе с Cisco IOS и MikroTik RouterOS.

7. Процесс и принципы работы коммутатора. Механизмы блокировки циклов. Протокол STP. Настройка STP на коммутаторах Cisco. MTU и фрагментация на L2. Архитектура маршрутизатора/коммутатора: Management/Control/Data plane.
Процесс и принципы работы Ethernet-коммутатора. Механизмы блокировки циклов. Протокол STP, разновидности и альтернативы.
Практика. Настройка STP на коммутаторах Cisco и MikroTik. MTU и фрагментация на L2.

8. Виртуальные локальные сети. VLAN на базе протокола 802.1q. Порты доступа и магистральные (транк). Маршрутизация между VLAN на маршрутизаторах и L3-коммутаторах.

Сабинтерфейсы маршрутизатора. Настройка VLAN на коммутаторах и маршрутизатор
Виртуальные локальные сети. VLAN на базе протокола 802.1q. Порты доступа и магистральные. Маршрутизация между VLAN на маршрутизаторах и L3-коммутаторах. Сабинтерфейсы маршрутизатора.
Практика. Настройка VLAN на коммутаторах и маршрутизаторах. Практика по настройке VLAN на Cisco IOS и MikroTik RouterOS.

5. Статическая маршрутизация. Маршрутизация по-умолчанию. Настройка маршрутов на маршрутизаторе с Cisco IOS. Маршрутизация по политике.
Практика. Статическая маршрутизация. Маршрутизация по-умолчанию. Плавающие маршруты. Маршрутизация по политике. Настройка маршрутов на маршрутизаторе с Cisco IOS и MikroTik RouterOS.

9. Списки контроля доступа (ACL). Правила создания и применения на интерфейсах в Cisco IOS. Варианты использования ACL.
Сетевая фильтрация. Списки контроля доступа (ACL). Правила создания и применения на интерфейсах в Cisco IOS. Варианты использования ACL.
Практика. Фильтрация в MikroTik RouterOS. Фильтрация в ОС Linux на примере iptables. Брандмауэр Windows.

10. Технология трансляции сетевых адресов NAT для IPv4. Назначение, принципы работы. Преимущества и недостатки. Настройка NAT на маршрутизаторе. Резервирование выхода в интернет через двух провайдеров. NAT для IPv6. NAT64/DNS64.
Технология трансляции сетевых адресов NAT для IPv4. Назначение, принципы работы. Преимущества и недостатки.
Практика. Настройка NAT на маршрутизаторах Cisco и MikroTik. Практика по резервированию выхода в интернет через двух провайдеров. NAT для IPv6. NAT64/DNS64.

11. Беспроводные сети. Популярные протоколы. Принципы построения WLAN, типовые топологии. Обеспечение безопасности передачи данных и проверки подлинности.
Беспроводные сети Wi-Fi. Принципы построения WLAN, типовые топологии. Правила планирования размещения точек доступа. Разбор типичных ошибок планирования Wi-Fi покрытия. Обеспечение безопасности передачи данных и проверки подлинности.
Практика. Мониторинг загруженности спектра WiFi.

13. Анализ производительности сети на базе протокола TCP. Характеричтики TCP: RTT, Rcv/Snd/Cng-wnd, DupAck, Reorder, LFN.
Практика. Комплексный поиск неисправности в работе сетевого приложения на базе протокола TCP с использованием анализатора пакетов WireShark. Анализ производительности сети на базе протокола TCP. Характеристики TCP: RTT, Rcv/Snd/cWnd, DupAck, LFN, нарушение порядка пакетов. Варианты реализаций TCP и современные альтернативы

14. Технологии передачи информации операторского уровня: MPLS, MPLS-VPN, VRF.
Рассматриваются архитектура операторских сетей, основные услуги, технологии MPLS и поддерживаемые услуги (L2VPN, L3VPN, VPWS, VPLS).

15. Архитектуры ВС. Tree-Tier, Leaf and Spine, Folded CLOS.
Рассматриваются популярные архитектуры построения ВС - городские сети, ЛВС, ЦОД. Tree-Tier, Leaf and Spine, Folded CLOS.

12. Протокол IPv6. Отличия от IPv4. Broadcast в протоколе IPv6. Настройка в Cisco IOS. Способы назначения адресов хостам. RA, SLAAC, PMTUD, DHCPv6. Автономная система.
Протокол IPv6. Отличия от IPv4. Способы назначения адресов хостам. RA, SLAAC, PMTUD, DHCPv6. Туннелирование.
Практика. Настройка IPv6 в Cisco IOS и MikroTik RouterOS.

16. Перспективные направления в развитии сетей. Программно-конфигурируемые сети. SDN, NFV/OVN, OpenFlow.
Рассматриваются аспекты реализации программно-конфигурируемых сетей, виртуализации сетевых функций, автоматизации развертывания сетевых услуг. Облачные технологии.

17. Мультикаст вещание в IP. IGMP, PIM.
Рассматриваются мультикаст-технологии. Практика по вещанию IPTV сигнала h.264 DVB.

18. Технологии Voice-over-IP. Технологии DVB-IP.
Рассматриваются технологии передачи голосовой информации в IP сетях, протоколы SIP, RTP. Технологии DVB-IP, протоколы MPEG-TS, видеокодек H.264.
Качество обслуживания (QoS) в контексте информационной безопасности. Архитектуры QoS. Защита от перегрузки канала. Применение политик ограничения на трафик.
Практика по защите критически важного трафика от потерь с помощью инструментов QoS. Элементы теории телетрафика. Элементы теории интервального анализа трафика. Использование системы конвейерного интервального анализа видеотрафика для оптимизации настроек QoS на коммутаторах и параметров кодека H.264.

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. Буцык, С. В. Вычислительные системы, сети и телекоммуникации : учебное пособие по дисциплине «Вычислительные системы, сети и телекоммуникации» для студентов, обучающихся по направлению 09.03.03 Прикладная информатика (уровень бакалавриата) / С. В. Буцык, А. С. Крестников, А. А. Рузаков ; под редакцией С. В. Буцык. — Челябинск : Челябинский государственный институт культуры, 2016. — 116 с. — ISBN 978-5-94839-537-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/56399.html

2. Фейт Сидни TCP/IP:Архитектура.Протоколы.Реализация (включая IP версии и IP SECURITY)/Сидни Фейт.-М.:Лори,2000, ISBN 5-85582-072-6.-424.

Дополнительная:

1. Хант Крейг Персональные компьютеры в сетях TCP/IP:Руководство администратора сети/Крейг Хант.-Киев:Изд.гр.BHV,1997, ISBN 5-7733-0019-2.-384.

2. Рогозин М. В. Лесные экосистемы и геобиологические сети:монография/М. В. Рогозин.-Пермь,2016, ISBN 978-5-7944-2717-2.-1. https://elis.psu.ru/node/358578

3. Широкополосные беспроводные сети передачи информации/РАН, Ин-т пробл. передачи информ..-М.:Техносфера,2005, ISBN 5-94836-049-0.-592.-Библиогр.: с. 579-591

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.ipspace.net/Main_Page ipSpace.net
https://dyn.com/blog/ Dyn Research

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

Образовательный процесс по дисциплине **Сети и системы передачи информации** 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.
Интернет с возможностью получения BGP full-view с route-серверов, Центр обработки данных ПГНИУ, лабораторный стенд Академии Cisco, лабораторный стенд MikroTik

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, практические 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 компьютерном классе кафедры радиоэлектроники и защиты информации с техническим оснащением, представленным в паспорте класса.
Для практических занятий - ПК, с установленной ОС windows или linux, оборудованные сетевыми адаптерами ethernet 10/100/1000.
Для лабораторных занятий:

ПК, с интерфейсом RS232, - 3шт.
Коммутаторы Cisco Catalyst 2960 - 3 шт.
Маршрутизаторы Cisco 2811 - 3 шт.
Точки доступа WiFi Ubiquity AirGrid - 2 шт.
IP-Телефоны Cisco 7911 - 3 шт.
Патч-корды UTP5 - 2м, - 6 шт.
Кабельный тестер Fluke DTX-1800.
Кроссировочный нож, обжимка на коннектор RJ45 (8P8C).
Коннекторы RJ45(8P8C) - 20шт.
Патч панель EIA/TIA-568B на 16 портов.
Витая пара UTP Cat5 - 10м. Маршрутизаторы MikroTik hAP lite RB941-2nD - 10 шт. Сварочный аппарат Fujikura FSM-18S. Оптические патч-корды LC-LC MM 15м - 3 шт.

Самостоятельная работа.
Аудитория для самостоятельной работы, в том числе помещения Научной библиотеки ПГНИУ,оснащенные компьютерной техникой с возможностьюподключения 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
Сети и системы передачи информации

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы	знать основы программных и программно-аппаратных средств используемых для защиты информационной системы	**Неудовлетворител** Отсутствие знаний основ программных и программно-аппаратных средств используемых для защиты информационной системы **Удовлетворительн** Общие, но не структурированные знания основ программных и программно-аппаратных средств используемых для защиты информационной системы **Хорошо** Сформированные, но содержащие отдельные пробелы знания основ программных и программно-аппаратных средств используемых для защиты информационной системы **Отлично** Хорошо сформированные знания основ программных и программно-аппаратных средств используемых для защиты информационной системы
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	уметь настраивать внешний брандмауэр, в соответствии с политикой безопасности предприятия	**Неудовлетворител** Отсутствие умений по защите внутренней сети от внешних угроз **Удовлетворительн** Частично сформированные умения по настройке внешних брандмауэров, в соответствии с политикой безопасности предприятия **Хорошо** В целом успешные, но содержащие отдельные пробелы умения по настройке внешних брандмауэров, в соответствии с политикой безопасности предприятия **Отлично**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Полностью сформированное умение по настройке внешних брандмауэров, в соответствии с политикой безопасности предприятия
ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	владеть методами защиты информационной системы от внешних вторжений	**Неудовлетворител** Отсутствие навыков защиты информационной системы от внешних вторжений **Удовлетворительн** Частично сформированные навыки владения методами эффективной защиты информационной системы от внешних вторжений **Хорошо** Сформированные, но содержащие отдельные пробелы, навыки владения методами эффективной защиты информационной системы от внешних вторжений **Отлично** Полностью сформированные навыки владения методами эффективной защиты информационной системы от внешних вторжений
ПК.28 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы	знать программно-аппаратные средства и уметь применять их для обеспечения защиты информационной системы	**Неудовлетворител** Не знает и не умеет применять программно-аппаратные средства для обеспечения защиты информационной системы **Удовлетворительн** частично сформированные знания и умения применять программно-аппаратные средства для обеспечения защиты информационной системы **Хорошо** Сформированные, но имеющие пробелы в знании и в целом успешное умение применять программно-аппаратные средства для обеспечения защиты информационной системы **Отлично** Хорошо сформированные знания и умения применять программно-аппаратные средства для обеспечения защиты информационной системы
ПК.22	владеть навыками	**Неудовлетворител**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	администрирования компьютерной сети предприятия	**Неудовлетворител** Отсутствие навыков сетевого администрирования **Удовлетворительн** Частично сформированные навыки администрирования компьютерной сети предприятия **Хорошо** В целом успешные, но содержащие отдельные пробелы навыки администрирования компьютерной сети предприятия **Отлично** Полностью сформированные навыки администрирования компьютерной сети предприятия
ПК.4 способность проводить анализ защищенности автоматизированных систем	знать риски информационной безопасности на предприятии, уметь выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности, владеть навыками проведения анализа защищенности автоматизированных систем	**Неудовлетворител** отсутствие знания рисков информационной безопасности на предприятии, отсутствие умения выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности, отсутствие навыков проведения анализа защищенности автоматизированных систем **Удовлетворительн** частично сформированные знания рисков информационной безопасности на предприятии, частично сформированные умения выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности, частично сформированные навыки проведения анализа защищенности автоматизированных систем **Хорошо** сформированные, но содержащие пробелы знания рисков информационной безопасности на предприятии, сформированные, но содержащие пробелы умения выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности, сформированные, но содержащие пробелы навыки проведения анализа защищенности автоматизированных систем

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично полностью сформированные знания рисков информационной безопасности на предприятии, сформированные умения выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности, сформированные навыки проведения анализа защищенности автоматизированных систем
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	уметь корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий	**Неудовлетворител** отсутствие умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий **Удовлетворительн** частично сформированные умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий **Хорошо** сформированные, но содержащие пробелы умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий **Отлично** полностью сформированные умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий
ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы	знать место анализа рисков в общей системе обеспечения информационной безопасности, уметь оценивать информационные риски в автоматизированных системах, владеть методами количественной и качественной оценки информационных рисков	**Неудовлетворител** отсутствие знания место анализа рисков в общей системе обеспечения информационной безопасности и умения оценивать информационные риски в автоматизированных системах, отсутствие владения методами количественной и качественной оценки информационных рисков **Удовлетворительн** частично сформированные знания место анализа рисков в общей системе обеспечения информационной безопасности и умения оценивать информационные риски в

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн автоматизированных системах, частично сформированное владение методами количественной и качественной оценки информационных рисков **Хорошо** сформированные, но содержащие пробелы знания место анализа рисков в общей системе обеспечения информационной безопасности и умения оценивать информационные риски в автоматизированных системах, сформированное, но содержащие пробелы владение методами количественной и качественной оценки информационных рисков **Отлично** полностью сформированные знания место анализа рисков в общей системе обеспечения информационной безопасности,полностью сформированные умения оценивать информационные риски в автоматизированных системах, полностью сформированное владение методами количественной и качественной оценки информационных рисков
ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем	владеть навыками анализа защищенности информационной системы с использованием специализированного оборудования	**Неудовлетворител** отсутствие владение навыками анализа защищенности информационной системы с использованием специализированного оборудования **Удовлетворительн** частично сформированное владение навыками анализа защищенности информационной системы с использованием специализированного оборудования **Хорошо** сформированное, но содержащее пробелы владения навыками анализа защищенности информационной системы с использованием специализированного оборудования **Отлично** полностью сформированное владение навыками анализа защищенности информационной системы с использованием

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично специализированного оборудования
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	владеть навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств	**Неудовлетворител** отсутствие владение навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств **Удовлетворительн** частично сформированное владение навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств **Хорошо** сформированное, но содержащие пробелы владение навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств **Отлично** полностью сформированное владение навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств
ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	Знать методы синтеза и анализа проектных решений по обеспечению безопасности АС, уметь выполнять синтез и анализ предполагаемых решений, владеть навыками принятия решений на основе синтеза и анализа АС	**Неудовлетворител** отсутствие знание методов синтеза и анализа проектных решений по обеспечению безопасности АС и умение выполнять синтез и анализ предполагаемых решений,отсутствие владение навыками принятия решений на основе синтеза и анализа АС **Удовлетворительн** частично сформированное знание методов синтеза и анализа проектных решений по обеспечению безопасности АС, частично сформированное умение выполнять синтез и анализ предполагаемых решений, частично сформированное владение навыками принятия решений на основе синтеза и анализа АС **Хорошо** сформированное, но содержащие пробелы знания методов синтеза и анализа

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо проектных решений по обеспечению безопасности АС, сформированное, но содержащие пробелы умения выполнять синтез и анализ предполагаемых решений, сформированное, но содержащие пробелы владения навыками принятия решений на основе синтеза и анализа АС **Отлично** полностью сформированное знание методов синтеза и анализа проектных решений по обеспечению безопасности АС, полностью сформированное умение выполнять синтез и анализ предполагаемых решений,полностью сформированное владение навыками принятия решений на основе синтеза и анализа АС
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	знать виды угроз для информационной системы,уметь строить модели угроз, вероятности их реализации и определять степень защищенности автоматизированной системы	**Неудовлетворител** отсутствие знания видов угроз для информационной системы, отсутствие умения строить модели угроз, вероятности их реализации и определять степень защищенности автоматизированной системы **Удовлетворительн** частично сформированное знание видов угроз для информационной системы, частично сформированное умение строить модели угроз, вероятности их реализации и определять степень защищенности автоматизированной системы **Хорошо** сформированное, но содержащие пробелы знания видов угроз для информационной системы, сформированное, но содержащие пробелы умения строить модели угроз, вероятности их реализации и определять степень защищенности автоматизированной системы **Отлично** полностью сформированное знание видов угроз для информационной системы, полностью сформированное умение строить модели угроз, вероятности их реализации и определять степень защищенности автоматизированной системы

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем	знать требования к формировании политик ИБ автоматизированных систем, уметь составлять нормативные документы, определяющие безопасность информации, владеть навыками администрирования АС	**Неудовлетворител** не знает требования к формировании политик ИБ автоматизированных систем, не умеет составлять нормативные документы, определяющие безопасность информации, не владеет навыками администрирования АС **Удовлетворительн** частично сформированные знания требований к формировании политик ИБ автоматизированных систем, частично сформированные умения составлять нормативные документы, определяющие безопасность информации, частично сформированные навыки администрирования АС **Хорошо** сформированные, но содержащие пробелы знания требований к формировании политик ИБ автоматизированных систем, сформированные, но содержащие пробелы умения составлять нормативные документы, определяющие безопасность информации, сформированные, но содержащие пробелы навыки администрирования АС **Отлично** сформированные знания требований к формировании политик ИБ автоматизированных систем, сформированные умения составлять нормативные документы, определяющие безопасность информации, сформированные навыки администрирования АС
ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций	знать требования по регламенту обеспечения ИБ АС, уметь разрабатывать методические материалы по обслуживанию систем безопасности АС	**Неудовлетворител** не знает требований по регламенту обеспечения ИБ АС, не умеет разрабатывать методические материалы по обслуживанию систем безопасности АС **Удовлетворительн** частично сформированные знания требований по регламенту обеспечения ИБ АС, частично сформированные умения разрабатывать методические материалы по обслуживанию систем безопасности АС **Хорошо**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
и других организационно-распорядительных документов в сфере профессиональной деятельности		**Хорошо** сформированные, но содержащие пробелы знания требований по регламенту обеспечения ИБ АС, сформированные, но содержащие пробелы умения разрабатывать методические материалы по обслуживанию систем безопасности АС **Отлично** полностью сформированные знания требований по регламенту обеспечения ИБ АС, сформированные умения разрабатывать методические материалы по обслуживанию систем безопасности АС
ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	знать составные элементы системы управления информационной безопасностью автоматизированной системы, владеть навыками проектирования системы управления информационной безопасностью предприятия	**Неудовлетворител** не знает составные элементы системы управления информационной безопасностью автоматизированной системы, не владеет навыками проектирования системы управления информационной безопасностью предприятия **Удовлетворительн** частично сформированные знания составных элементов системы управления информационной безопасностью автоматизированной системы, частично сформированные навыки проектирования системы управления информационной безопасностью предприятия **Хорошо** сформированные, но содержащие пробелы знания составных элементов системы управления информационной безопасностью автоматизированной системы, сформированные но содержащие пробелы навыки проектирования системы управления информационной безопасностью предприятия **Отлично** сформированные знания составных элементов системы управления информационной безопасностью автоматизированной системы, сформированные навыки проектирования системы управления информационной безопасностью предприятия

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы	знать виды средств защиты информации и средств контроля защищенности автоматизированной системы, уметь проектировать средства защиты информации и средства контроля защищенности автоматизированной системы	**Неудовлетворител** не знает виды средств защиты информации и средств контроля защищенности автоматизированной системы, не умеет проектировать средства защиты информации и средства контроля защищенности автоматизированной системы **Удовлетворительн** частично сформированные знания видов средств защиты информации и средств контроля защищенности автоматизированной системы, частично сформированные умения проектировать средства защиты информации и средства контроля защищенности автоматизированной системы **Хорошо** сформированные, но содержащие пробелы знания видов средств защиты информации и средств контроля защищенности автоматизированной системы, сформированные, но содержащие пробелы умения проектировать средства защиты информации и средства контроля защищенности автоматизированной системы **Отлично** полностью сформированные знания видов средств защиты информации и средств контроля защищенности автоматизированной системы, сформированные умения проектировать средства защиты информации и средства контроля защищенности автоматизированной системы
ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности	знать принципиальные схемы технических средств защиты, уметь настраивать технические средства для работы, владеть навыками управления техническими средствами защиты информации	**Неудовлетворител** не знает принципиальные схемы технических средств защиты, не умеет настраивать технические средства для работы, не владеет навыками управления техническими средствами защиты информации **Удовлетворительн** частично сформированные знания принципиальных схем технических средств защиты, частично сформированные умения

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн настраивать технические средства для работы, частично сформированные навыки управления техническими средствами защиты информации **Хорошо** сформированные, но содержащие пробелы знания принципиальных схем технических средств защиты, сформированные, но содержащие пробелы умения настраивать технические средства для работы, сформированные, но содержащие пробелы навыки управления техническими средствами защиты информации **Отлично** полностью сформированные знания принципиальных схем технических средств защиты, сформированные умения настраивать технические средства для работы, сформированные навыки управления техническими средствами защиты информации
ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности	владеть навыками разработки компонентов автоматизированных систем	**Неудовлетворител** не владеет навыками разработки структурных компонентов автоматизированных систем **Удовлетворительн** частично сформированные навыки разработки структурных компонентов автоматизированных систем **Хорошо** сформированные, но содержащие пробелы навыки разработки структурных компонентов автоматизированных систем **Отлично** полностью сформированные навыки разработки структурных компонентов автоматизированных систем

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Вариативная часть

Вид мероприятия промежуточной аттестации : Экзамен
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 48 до 60
«неудовлетворительно» / «незачтено» менее 48 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Входной контроль **Входное тестирование**	- диагностика неисправностей ПК и популярных ОС, понимание технических текстов на английском языке- знание устройства ПК на уровне опытного пользователя- понимание бизнес задач, решаемых компьютерными сетями- навыки работы с популярными службами сети Интернет - понимание терминологии языков программирования, основных единиц измерения, навыки программирования на одном языке или построения алгоритмов

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.4 способность проводить анализ защищенности автоматизированных систем **ПК.6** способность проводить анализ рисков информационной безопасности автоматизированной системы **ПК.9** способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем **ПК.29** способность администрировать подсистему информационной безопасности автоматизированной системы	5. Статическая маршрутизация. Маршрутизация по-умолчанию. Настройка маршрутов на маршрутизаторе с Cisco IOS. Маршрутизация по политике **Письменное контрольное мероприятие**	- понимание специальных терминов,- характеристики и алгоритмы работы основных протоколов передачи данных- навыки чтения структурных схем сетей передачи данных- знание основных сетевых сервисов

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.11** способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности **ПК.12** способность разрабатывать политики информационной безопасности автоматизированных систем **ПК.15** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.18** способность проводить инструментальный мониторинг защищенности автоматизированных систем **ПК.22** способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	12. Протокол IPv6. Отличия от IPv4. Broadcast в протоколе IPv6. Настройка в Cisco IOS. Способы назначения адресов хостам. RA, SLAAC, PMTUD, DHCPv6. Автономная си **Письменное контрольное мероприятие**	- понимание специальных терминов,- характеристики и алгоритмы работы основных протоколов передачи данных- навыки чтения и создания структурных схем сетей передачи данных- навыки настройки основных сетевых сервисов

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **ПК.28** способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы **ПК.30** способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы		

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.4 способность проводить анализ защищенности автоматизированных систем **ПК.5** способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы **ПК.6** способность проводить анализ рисков информационной безопасности автоматизированной системы **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.9** способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем **ПК.10** способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности **ПК.11** способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности **ПК.12** способность разрабатывать политики информационной безопасности автоматизированных систем **ПК.13**	Итоговый контроль **Итоговое контрольное мероприятие**	Студент демонстрирует понимание специальных терминов, знает характеристики и алгоритмы работы основных протоколов передачи данных. Демонстрирует навыки чтения и создания структурных схем сетей передачи данных, навыки настройки основных сетевых сервисов. Ориентируется в перспективных технологиях развития сетей. Ориентируется в справочной информации и опубликованных стандартах. Способен предложить законченное архитектурное решение по созданию сети передачи данных с заданными характеристиками (включая активное, пассивное оборудование, кабельную систему).

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы **ПК.14** способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы **ПК.15** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.18** способность проводить инструментальный мониторинг защищенности автоматизированных систем **ПК.22** способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности **ПК.23** способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности		

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **ПК.28** способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы **ПК.29** способность администрировать подсистему информационной безопасности автоматизированной системы **ПК.30** способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы		

Спецификация мероприятий текущего контроля

Входной контроль

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
- понимание бизнес задач, решаемых компьютерными сетями- навыки работы с популярными службами сети Интернет	4

- диагностика неисправностей ПК и популярных ОС, понимание технических текстов на английском языке	2
- понимание терминологии языков программирования, основных единиц измерения, навыки программирования на одном языке или построения алгоритмов	2
- знание устройства ПК на уровне опытного пользователя	2

5. Статическая маршрутизация. Маршрутизация по-умолчанию. Настройка маршрутов на маршрутизаторе с Cisco IOS. Маршрутизация по политике

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **14**

Показатели оценивания	Баллы
Студент корректно сопоставляет значения минимум 8 специальных терминов из 16	8
Студент корректно описывает алгоритмы работы минимум 10 протоколов физического, канального, сетевого и транспортного уровней в любых комбинациях.	8
Студент корректно интерпретирует значение элементов структурной схемы СКС, физической, логической. Минимум 8 различных элементов.	8
Студент корректно настраивает 6 различных сетевых сервисов в заданной ОС	6

12. Протокол IPv6. Отличия от IPv4. Broadcast в протоколе IPv6. Настройка в Cisco IOS. Способы назначения адресов хостам. RA, SLAAC, PMTUD, DHCPv6. Автономная си

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **14**

Показатели оценивания	Баллы
Студент корректно интерпретирует значение элементов структурной схемы СКС, физической, логической. Минимум 8 различных элементов.	8
Студент корректно сопоставляет значения минимум 8 специальных терминов из 16	8
Студент корректно описывает алгоритмы работы минимум 10 протоколов физического, канального, сетевого и транспортного уровней в любых комбинациях.	8
Студент корректно настраивает 6 различных сетевых сервисов в заданной ОС	6

Итоговый контроль

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
Студент корректно называет и описывает не менее 4 перспективных направлений развития сетей ПД	6
Студент корректно настраивает работу не менее 6 различных сетевых сервисов на маршрутизаторе	6
Студент корректно создает структурную схему сети передачи данных с не менее 10 узлами, 5 единицами активного оборудования, 5 единицами пассивного оборудования.	6
Студент корректно описывает алгоритм работы не менее 10 протоколов физического, канального, сетевого уровней	6
Студент корректно интерпретирует значения 6 специальных терминов	6
Студент корректно интерпретирует раздел стандарта передачи данных из серии IEEE 802 или RFC Standards Track по выбору преподавателя и способен описать алгоритм реализации данного раздела стандарта	6
Студент предлагает законченное архитектурное решение по созданию СПД, включая СКС, активное оборудование, пассивное оборудование по заданным преподавателям входным требованиям	4