

МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

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

Рабочая программа дисциплины

БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Код УМК 94159

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

Пермь, 2020

1. Наименование дисциплины

Безопасность распределенных вычислительных сетей

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 **Безопасность распределенных вычислительных сетей** 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.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.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.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	8
Объем дисциплины (з.е.)	5
Объем дисциплины (ак.час.)	180
Контактная работа с преподавателем (ак.час.), в том числе:	70
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	42
Самостоятельная работа (ак.час.)	110
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (8 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Безопасность распределенных вычислительных сетей

Дисциплина "Безопасность распределенных вычислительных сетей" имеет целью обучить студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

Входной контроль

Входной контроль имеет целью оценить навыки и знания студентов, необходимые для успешного освоения данной дисциплины. На входной контроль выносятся базовые знания и навыки работы со службами сети Интернет, активным и пассивным оборудованием ВС, навыки конфигурирования основных сетевых сервисов в ОС Linux, Windows, RouterOS, Cisco IOS.

Раздел 1. Информационная безопасность в сетях передачи данных

Информационная безопасность – цели и задачи. Архитектуры открытых сетей, корпоративных сетей, сетей операторов связи, центров обработки данных. Стандарты по информационной безопасности и безопасности сетей. Обзор стандарта ISO IEC 27002:2005. Уязвимости политические, технологические, конфигурационные. Политика безопасности. Классификация угроз и типы атак. Технологии и инструменты анализа сети и потоков данных. Распространенные протоколы и их технологические уязвимости. Защищенные аналоги популярных протоколов

Раздел 2. Контроль доступа к сети

Контроль доступа к сети

Технологии аутентификации, авторизации и учета при доступе к сетевым ресурсам. Службы и протоколы проверки подлинности и контроля доступа. Методы проверки подлинности. Принципы работы систем RADIUS, TACACS+, Kerberos.

Защита уровня доступа

Защита топологии второго уровня. Идентифицирующий (перехватывающий) прокси – реализации, уязвимости. Защищенность сетевой инфраструктуры и защищенность пользователя. Контроль выделения IP-адресов и учет. Защита служебных протоколов DHCP и ARP. Сети хранения данных и безопасность.

IPv4 + IPv6 first-hop-security.

Контроль доступа на уровне порта

Набор стандартов 802.1x в применении к проводным и беспроводным сетям. Проверка подлинности на порту устройства. Ограничение прав доступа на порту. Изолирование портов доступа. Уязвимости изолирования портов. Применение 802.1x совместно с VoIP. Уязвимость протоколов передачи голоса и видео по IP

Раздел 3. Виртуальные частные сети и их защита

Технологии построения виртуальных каналов в открытых сетях. Технологии защиты виртуальных каналов. Протоколы туннелей. Технологии и протоколы VLAN, MPLS, GRE, PPTP, L2TP, PPPoE. Обзор протоколов набора стандартов IPSec. Защита транспортная и туннельная. Протоколы AH и ESP. Анонимность в сети Интернет. Правовые вопросы применения шифрования данных

Раздел 4. Инспекция потоков данных: межсетевое экранирование и системы обнаружения и предотвращения вторжений

Межсетевое экранирование

Межсетевые экраны. Списки контроля доступа – принципы реализации и правила применения.

Персональные межсетевые экраны. Списки доступа на порту, виртуальном интерфейсе, VLAN.

Объектные списки доступа. Межсетевой экран с контролем состояние подключений. Контекстный

контроль доступа. Инспектирование потоков трафика.

Системы обнаружения и предотвращения вторжений

Архитектура систем обнаружения и предотвращения вторжений. Глубокая инспекция пакетов. Типовые способы анализа потоков данных. Эвристические алгоритмы. Классификация потоков трафика.

Контроль классифицированных потоков. Распознавание приложений. Ассиметричные потоки данных

Раздел 5. Технологии обеспечения непрерывности работы сети

Непрерывность бизнеса, надежность, отказоустойчивость

Резервирование различных уровней сетевой топологии и инфраструктуры. Точки отказа.

Взаимодействие сети и обслуживающей инфраструктуры. Диспетчеризация, контроль параметров окружающей среды на узлах связи. Прогнозирование нагрузки и отказов. Двойные отказы.

Балансировка нагрузки и распределение нагрузки.

Резервирование в маршрутизации

Резервирование каналов доступа в Интернет. Политические и конфигурационные уязвимости протокола BGP. Протоколы резервирования и балансировки нагрузки шлюза: HSRP и GLBP. Организация каналов между устройствами одного уровня.

Резервирование в коммутации

Резервирование активных устройств и каналов. Защита топологии. Агрегирование каналов.

Резервирование восходящих каналов без потери пропускной способности. Виртуализация вышестоящих коммутаторов. Отслеживание состояния портов.

Качество обслуживания

Технологии обеспечения качества обслуживания (QoS). Прогнозируемые показатели отклика сети при больших нагрузках. Интегрированные и дифференцированные услуги. Реализация. Контроль предоставляемой полосы пропускания. Проверки соответствия соглашений об уровне сервиса

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. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 86 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/69405.html>
2. Аверченков В. И. Аудит информационной безопасности: Учебное пособие для вузов/Аверченков В. И..-Брянск:Брянский государственный технический университет,2012, ISBN 978-89838-487-6.-268. <http://www.iprbookshop.ru/6991>
3. Современные радиоэлектронные средства и технологии информационной безопасности : монография / В. А. Майстренко, А. А. Соловьев, М. Ю. Пляскин, А. И. Тихонов. — Омск : Омский государственный технический университет, 2017. — 356 с. — ISBN 978-5-8149-2554-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/78508.html>
4. Технические средства и методы защиты информации:учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность",090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем"/А. П. Зайцев [и др.] ; под ред. А. П. Зайцева, А. А. Шелупанова.-4-е изд., испр. и доп..-Москва:Горячая линия - Телеком,2012, ISBN 978-5-9912-0084-4.- 616.-Библиогр.: с. 608-609

Дополнительная:

1. Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем : учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. — 396 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/72158.html>
2. Безопасность ИТ:[Криптографические основы безопасности. Основы информационной безопасности. Протоколы безопасного сетевого взаимодействия. Стандарты информационной безопасности]/Интернет-Университет информационных технологий.-М.:Новый диск,2006.-1.

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<https://blog.ipspace.net/search/label/security> ipspace.net

<https://dyn.com/blog/category/security/> dyn research

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

Образовательный процесс по дисциплине **Безопасность распределенных вычислительных сетей** 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-образовательную 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 Player";
- программа просмотра интернет контента (браузер) "Google Chrome"

База знаний - k.psu.ru (вики, файлообмен, блог преподавателя).

Эмулятор Cisco PacketTracer.

Интернет с возможностью получения BGP full-view с route-серверов, Центр обработки данных ПГНИУ, лабораторный стенд Академии Cisco.

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.

Аудитория для лабораторных занятий.

Лабораторные занятия проводятся в компьютерном классе кафедры радиоэлектроники и защиты

информации, техническое оснащение которого представлено в паспорте компьютерного класса.

Для практических занятий - ПК, с установленной ОС windows или linux, оборудованные сетевыми адаптерами ethernet 10/100/1000.

Для лабораторных занятий:

Межсетевой экран Cisco ASA5520 - 2 шт.

Межсетевой экран Cisco PIX515E - 2 шт.

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.

Аудитория для самостоятельной работы, 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
Безопасность распределенных вычислительных сетей**

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

ПК.29

способность администрировать подсистему информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы	Знать структуру подсистемы информационной безопасности АС. Уметь администрировать подсистему ИБ АС. Владеть навыками решения оперативных задач ИБ АС.	Неудовлетворител Студент не может сформулировать структуру подсистемы информационной безопасности АС. Не знает приемы администрирования подсистемы ИБ АС. Студент не владеет навыками решения оперативных задач ИБ АС. Удовлетворительн Студент владеет специальной терминологией ИБ. Имеет представление об основных элементах подсистемы ИБ АС. Хорошо Студент демонстрирует понимание основных элементов подсистемы ИБ АС. Владеет специальной терминологией ИБ. Имеет представление о приемах администрирования ИБ АС. Отлично Студент демонстрирует знание структуры подсистемы информационной безопасности АС. Знает приемы администрирования подсистемы ИБ АС. Владеет навыками решения оперативных задач ИБ АС.

ПК.30

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.30 способность выполнять	Знать варианты реализации частных политик ИБ сетей	Неудовлетворител Студент не владеет терминологией.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	передачи данных. Уметь применять политики ИБ в системе передачи данных (СПД) Владеть навыками мониторинга безопасности СПД.	<p>Неудовлетворител Не знает вариантов применения частных политик ИБ в СПД.</p> <p>Удовлетворительн студент знаком с вариантами частных политик ИБ СПД. Владеет специальной терминологией.</p> <p>Хорошо студент знает назначение частных политик ИБ сетей передачи данных. студент знает варианты применения политик ИБ СПД. студент знает показатели мониторинга ИБ СПД.</p> <p>Отлично студент знает варианты реализации частных политик ИБ сетей передачи данных. студент умеет применять политики ИБ в СПД. студент владеет навыками мониторинга безопасности СПД.</p>

ПК.7

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	Знать анализируемые показатели безопасности сетей передачи данных. Уметь анализировать характеристики и показатели сетей. Владеть навыками оценки эффективности показателей безопасности сетей.	<p>Неудовлетворител Студент не знает показатели безопасности сетей передачи данных.</p> <p>Удовлетворительн Знает анализируемые показатели безопасности сетей передачи данных.</p> <p>Хорошо Знает анализируемые показатели безопасности сетей передачи данных. Умеет анализировать характеристики и показатели сетей.</p> <p>Отлично Знает анализируемые показатели безопасности сетей передачи данных. Умеет анализировать характеристики и показатели сетей. В совершенстве владеет навыками оценки эффективности показателей безопасности</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично сетей.

ПК.6

способность проводить анализ рисков информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы	знать основные составляющие рисков ИБ в сетях передачи данных. уметь анализировать риски ИБ системы передачи данных (СПД). владеть навыком анализа рисков ИБ по заданной схеме ИБ СПД.	Неудовлетворител Студент не знает основные риски ИБ сетей передачи данных. Удовлетворительн Студент знаком с основными рисками ИБ сетей передачи данных. Хорошо знает основные составляющие рисков ИБ в сетях передачи данных. умеет анализировать риски ИБ СПД. Отлично знает основные составляющие рисков ИБ в сетях передачи данных. умеет анализировать риски ИБ СПД. в совершенстве владеет навыком анализа рисков ИБ по заданной схеме ИБ СПД.

ПК.18

способность проводить инструментальный мониторинг защищенности автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем	знать требования к инструментальному мониторингу защищенности автоматизированных систем, уметь проводить инструментальный мониторинг защищенности автоматизированных систем владеть навыками проведения инструментального мониторинга защищенности автоматизированных систем	Неудовлетворител студент не знает требования к инструментальному мониторингу защищенности автоматизированных систем, не умеет проводить инструментальный мониторинг защищенности автоматизированных систем, не владеет навыками проведения инструментального мониторинга защищенности автоматизированных систем Удовлетворительн студент частично знает требования к

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительн инструментальному мониторингу защищенности автоматизированных систем</p> <p>Хорошо студент знает требования к инструментальному мониторингу защищенности автоматизированных систем, умеет проводить инструментальный мониторинг защищенности автоматизированных систем, владеет навыками проведения инструментального мониторинга защищенности автоматизированных систем</p> <p>Отлично студент знает требования к инструментальному мониторингу защищенности автоматизированных систем, умеет проводить инструментальный мониторинг защищенности автоматизированных систем, в совершенстве владеет навыками проведения инструментального мониторинга защищенности автоматизированных систем</p>

ПК.15

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно- аппаратных, криптографических и технических средств защиты информации	знать порядок проведения и требования к контрольным проверкам работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации в СПД, уметь проводить проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты	<p>Неудовлетворител не знает порядок проведения и требования к контрольным проверкам работоспособности и эффективности применяемых программно- аппаратных, криптографических и технических средств защиты информации в СПД,</p> <p>Удовлетворительн знает порядок проведения и требования к контрольным проверкам работоспособности и эффективности применяемых программно- аппаратных, криптографических и технических средств защиты информации в СПД,</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	информации в СПД владеть навыками проверки работоспособности и эффективности применяемых средств защиты информации в СПД	<p>Хорошо знает порядок проведения и требования к контрольным проверкам работоспособности и эффективности применяемых программно- аппаратных, криптографических и технических средств защиты информации в СПД, умеет проводить проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации в СПД</p> <p>Отлично знает порядок проведения и требования к контрольным проверкам работоспособности и эффективности применяемых программно- аппаратных, криптографических и технических средств защиты информации в СПД, умеет проводить проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации в СПД владеет навыками проверки работоспособности и эффективности применяемых средств защиты информации в СПД</p>

ПК.9

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	знать характеристики проектных решений по обеспечению безопасности СПД, уметь составлять проектные решения по обеспечению безопасности СПД, владеть навыками разработки проектных решений по обеспечению безопасности СПД.	<p>Неудовлетворител не знает характеристики проектных решений по обеспечению безопасности СПД,</p> <p>Удовлетворительн знает характеристики проектных решений по обеспечению безопасности СПД</p> <p>Хорошо знает характеристики проектных решений по обеспечению безопасности СПД, умеет составлять проектные решения по обеспечению безопасности СПД,</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Отлично</p> <p>знает характеристики проектных решений по обеспечению безопасности СПД, умеет составлять проектные решения по обеспечению безопасности СПД, в совершенстве владеет навыками разработки проектных решений по обеспечению безопасности СПД.</p>

ПК.5

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.5</p> <p>способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p>	<p>Знать типовые модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Уметь разрабатывать модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Владеть навыками оценки актуальности модели угроз данной СПД.</p>	<p>Неудовлетворител</p> <p>Не знает типовые модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Удовлетворительн</p> <p>Знает типовые модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Хорошо</p> <p>Знает типовые модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Умеет разрабатывать модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Отлично</p> <p>Знает типовые модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Умеет разрабатывать модели угроз и модели нарушителя информационной безопасности СПД.</p> <p>Владеет навыками оценки актуальности модели угроз данной СПД.</p>

ПК.12

способность разрабатывать политики информационной безопасности автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.12	знать требования к политике	Неудовлетворител

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
способность разрабатывать политики информационной безопасности автоматизированных систем	информационной безопасности автоматизированных систем и сетей передачи данных, уметь формулировать политику ИБ СПД.	<p>Неудовлетворител не знает требования к политике информационной безопасности автоматизированных систем и сетей передачи данных</p> <p>Удовлетворительн знает требования к политике информационной безопасности автоматизированных систем и сетей передачи данных</p> <p>Хорошо знает требования к политике информационной безопасности автоматизированных систем и сетей передачи данных, умеет формулировать политику ИБ СПД.</p> <p>Отлично знает требования к политике информационной безопасности автоматизированных систем и сетей передачи данных, умеет формулировать политику ИБ СПД. в совершенстве владеет навыками анализа соответствия СПД политике ИБ.</p>

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 (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций	Знать требования к нормативным и методическим материалам, регламентирующим работу по обеспечению информационной безопасности автоматизированных систем. Уметь разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.	<p>Неудовлетворител Не знает требований к нормативным и методическим материалам, регламентирующим работу по обеспечению информационной безопасности автоматизированных систем.</p> <p>Удовлетворительн Знает требования к нормативным и методическим материалам, регламентирующим работу по обеспечению информационной безопасности автоматизированных систем</p> <p>Хорошо</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
и других организационно- распорядительных документов в сфере профессиональной деятельности		<p>Хорошо</p> <p>Знает требования к нормативным и методическим материалам, регламентирующим работу по обеспечению информационной безопасности автоматизированных систем.</p> <p>Знает состав нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.</p> <p>Отлично</p> <p>Знает требования к нормативным и методическим материалам, регламентирующим работу по обеспечению информационной безопасности автоматизированных систем.</p> <p>Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.</p>

ПК.13

способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знать требования, предъявляемые к системе управления ИБ СПД. Способность создавать и реализовывать проект создания системы управления ИБ СПД.	<p>Неудовлетворител</p> <p>Не знает требования, предъявляемые к системе управления ИБ СПД.</p> <p>Удовлетворительн</p> <p>Частично сформированные знания требований, предъявляемые к системе управления ИБ СПД.</p> <p>Способен создавать проект создания системы управления ИБ СПД.</p> <p>Хорошо</p> <p>Знает требования, предъявляемые к системе управления ИБ СПД.</p> <p>Способен создавать и реализовывать проект создания системы управления ИБ СПД.</p> <p>Отлично</p> <p>Полностью сформированные знания требований, предъявляемые к системе</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично управления ИБ СПД. Способен создавать и реализовывать проект создания системы управления ИБ СПД.

ПК.14

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы	Знать требования, предъявляемые к средствам защиты информации. Знать требования, предъявляемые к средствам контроля защищенности информации. Способность создавать и реализовывать проект создания средства защиты информации. Способность создавать и реализовывать проект создания средства контроля защищенности информации.	Неудовлетворител Не знает требования, предъявляемые к средствам защиты информации. Не знает требования, предъявляемые к средствам контроля защищенности информации. Удовлетворительн Знает требования, предъявляемые к средствам защиты информации. Знает требования, предъявляемые к средствам контроля защищенности информации Хорошо Знает требования, предъявляемые к средствам защиты информации. Знает требования, предъявляемые к средствам контроля защищенности информации. Способен создавать проект создания средства защиты информации. Способен создавать проект создания средства контроля защищенности информации. Отлично Знает требования, предъявляемые к средствам защиты информации. Знает требования, предъявляемые к средствам контроля защищенности информации. Способен создавать и реализовывать проект создания средства защиты информации. Способен создавать и реализовывать проект создания средства контроля защищенности информации.

ПК.10

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности	Владеть навыками разработки элементов защищенных сетей передачи данных. Знать характеристики оборудования и протоколов, стандартов СКС, элементов защиты сети.	Неудовлетворител Не знает характеристик оборудования и протоколов, стандартов СКС, элементов защиты сети. не знает состав элементов защищенных сетей передачи данных. Удовлетворительн Знает состав элементов защищенных сетей передачи данных. Знает характеристики оборудования и протоколов, стандартов СКС, элементов защиты сети. Хорошо Владеть навыками разработки элементов защищенных сетей передачи данных. Знает характеристики оборудования и протоколов, стандартов СКС, элементов защиты сети Отлично Владеет навыками разработки элементов защищенных сетей передачи данных. Способен создать проект разработки элементов защищенной сети передачи данных. Знает характеристики оборудования и протоколов, стандартов СКС, элементов защиты сети.

ПК.11

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности	Владеет навыками разработки элементов сетей передачи данных. Знать характеристики оборудования и протоколов, стандартов СКС.	Неудовлетворител не знает терминологии. Не знает характеристик оборудования и протоколов, стандартов СКС. Удовлетворительн Владеет терминологией. Знает характеристик оборудования и протоколов, стандартов СКС. Хорошо

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> <p>Знаком с разработкой элементов сетей передачи данных. Знает характеристики оборудования и протоколов, стандартов СКС.</p> <p style="text-align: center;">Отлично</p> <p>В совершенстве владеет навыками разработки элементов сетей передачи данных. Полностью сформированные знания характеристики оборудования и протоколов, стандартов СКС.</p>

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

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 50 до 60

«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Входной контроль Входное тестирование	Проверяются базовые знания и навыки работы со службами сети Интернет, активным и пассивным оборудованием ВС, навыки конфигурирования основных сетевых сервисов в ОС Linux, Windows, RouterOS, Cisco IOS.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p> <p>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</p> <p>ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>	<p>Раздел 3. Виртуальные частные сети и их защита</p> <p>Письменное контрольное мероприятие</p>	<p>Знание вариантов реализаций частных политик ИБ сетей передачи данных.</p> <p>Применение политик ИБ в СПД.</p> <p>Владение навыками мониторинга безопасности СПД.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы</p> <p>ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы</p>	<p>Раздел 5. Технологии обеспечения непрерывности работы сети</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание анализируемые показатели безопасности сетей передачи данных.</p> <p>Умение анализировать характеристики и показатели сетей. Навыки оценки эффективности показателей безопасности сетей.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p> <p>ПК.12 способность разрабатывать политики информационной безопасности автоматизированных систем</p> <p>ПК.13 способность участвовать в проектировании системы управления информационной безопасностью</p>	<p>Раздел 5. Технологии обеспечения непрерывности работы сети</p> <p>Итоговое контрольное мероприятие</p>	<p>Политика безопасности ИБ СПД.Схема защищенной сети передачи данных.</p> <p>Результат анализа защищенности СПД и соответствия политике ИБ.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>автоматизированной системы ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности</p> <p>автоматизированной системы ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем</p> <p>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</p> <p>ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы</p> <p>ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы,</p>		

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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
Показатель БаллКорректная интерпретация алгоритма работы 3 сетевых протоколов канального, сетевого и транспортного уровней	3
Корректная интерпретация схемы ЛВС с подключением к Интернет	3
Корректная настройка 2 сетевых сервисов в Cisco IOS и RouterOS	2
Корректная настройка 2 сетевых сервисов в Linux и Windows	2

Раздел 3. Виртуальные частные сети и их защита

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

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

Проходной балл: **15**

Показатели оценивания	Баллы
Знание вариантов реализаций частных политик ИБ сетей передачи данных.	10
Студент адекватно распознает угрозы безопасности посредством мониторинга безопасности СПД	10
Правильно применяется политика ИБ в СПД.	10

Раздел 5. Технологии обеспечения непрерывности работы сети

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

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

Проходной балл: **15**

Показатели оценивания	Баллы
Знает не менее 10 показателей безопасности сетей передачи данных.	10
Студент корректно анализирует не менее 10 характеристик и показателей работы сетей передачи данных.	10
Корректно оценивает эффективность 10 реализованных мер ИБ заданной СПД	10

Раздел 5. Технологии обеспечения непрерывности работы сети

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **20**

Показатели оценивания	Баллы
Студент корректно проводит анализ защищенности сети передачи данных по заданной схеме или техническому заданию. Проводит анализ соответствия политике безопасности. Не менее 10 различных мер.	10
Студент создает техническое задание на модернизацию сети передачи данных с целью привести сеть в соответствие требованиям политики безопасности предприятия. Не менее 10 пунктов частной модели угроз.	10
Студент создает политику безопасности сети передачи данных соответствующую требованиям законодательства и политики предприятия. Не менее 10 пунктов, согласно частной модели угроз.	10
Студент создает архитектурный план защищенной сети передачи данных, соответствующей политике безопасности и техническому заданию. Не менее 10 единиц активного и пассивного оборудования, не менее 10 узлов сети.	10