МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Черников Арсений Викторович**
Челин Алексей Юрьевич

Рабочая программа дисциплины

ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ

Код УМК 93220

Утверждено
Протокол №1
от «28» августа 2023 г.

Пермь, 2023

1. Наименование дисциплины

Защита компьютерных сетей

2. Место дисциплины в структуре образовательной программы

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

Направление подготовки: **11.03.02** Инфокоммуникационные технологии и системы связи
направленность Инфокоммуникационные технологии в сервисах и услугах связи

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Защита компьютерных сетей** у обучающегося должны быть сформированы следующие компетенции:

11.03.02 Инфокоммуникационные технологии и системы связи (направленность : Инфокоммуникационные технологии в сервисах и услугах связи)

ПК.5 Способен к оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

Индикаторы

ПК.5.3 Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

ПК.9 Способен осуществлять администрирование сетевых подсистем инфокоммуникационных систем и /или их составляющих

Индикаторы

ПК.9.2 Проводит анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих

ПК.9.3 Осуществляет самостоятельную работу по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих

ПК.11 Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Индикаторы

ПК.11.1 Применяет на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

ПК.11.3 Осуществляет самостоятельно администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

ПК.12 Способен к проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы

Индикаторы

ПК.12.2 Анализирует существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы

ПК.12.3 Осуществляет самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы

4. Объем и содержание дисциплины

Направление подготовки	11.03.02 Инфокоммуникационные технологии и системы связи (направленность: Инфокоммуникационные технологии в сервисах и услугах связи)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	3
Объем дисциплины (з.е.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	102
Проведение лекционных занятий	34
Проведение лабораторных работ, занятий по иностранному языку	68
Самостоятельная работа (ак.час.)	114
Формы текущего контроля	Защищаемое контрольное мероприятие (3)
Формы промежуточной аттестации	Экзамен (3 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

1 семестр

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. Итоговый контроль

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.

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. Стохастические методы и средства защиты информации в компьютерных системах и сетях/М. А. Иванов [и др.] ; под ред. И. Ю. Жукова.-Москва:КУДИЦ-ПРЕСС,2009, ISBN 978-5-91136-068-9.-512.-Библиогр.: с. 504-510

2. 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.] ; ред.: А. П. Зайцев, А. А. Шелупанов.-4-е изд., испр. и доп..-Москва:Горячая линия - Телеком,2012, ISBN 978-5-9912-0084-4.-616.-Библиогр.: с. 608-609

Дополнительная:

1. 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 c. — ISBN 978-5-8149-2554-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/78508.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.intuit.ru/studies/courses/3688/930/lecture/16466 Основы компьютерных сетей
https://www.intuit.ru/studies/courses/13845/1242/lecture/27503 Безопасность информационных систем

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

Образовательный процесс по дисциплине **Защита компьютерных сетей** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующих 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:
- операционная система "ALT Linux"
- офисный пакет приложений "Libre office";
- программа просмотра интернет контента (браузер)
- VirtualBox
- GNS3
- PnetLab
- Eve-NG
- Cisco packet tracer
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 в компьютерном классе (лаборатории) с техническим оснащением, представленным в паспорте класса. Дополнительно для рабочего места преподавателя требуется оснащение презентационной техникой (проектор, экран для проектора, компьютер/ноутбук)
Требуемое ПО:

- операционная система "ALT Linux"
- офисный пакет приложений "Libre office";
- программа просмотра интернет контента (браузер)
- VirtualBox
- GNS3
- PnetLab
- Eve-NG
- Cisco packet tracer

Не менее 200 GB свободного дискового пространства на каждой рабочей станции.

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
Защита компьютерных сетей

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

ПК.11

Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.11.3 Осуществляет самостоятельно администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Знает средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Владеет навыками осуществления самостоятельного администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).	**Неудовлетворител** Не знает средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Не владеет навыками осуществления самостоятельного администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Удовлетворительн** Частично знает средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Не владеет навыками осуществления самостоятельного администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Хорошо** Знает средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Частично владеет навыками осуществления самостоятельного администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Отлично** Знает средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Владеет навыками осуществления самостоятельного администрирования средств обеспечения безопасности удаленного доступа (операционных систем и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично специализированных протоколов).
ПК.11.1 Применяет на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Знает теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).	**Неудовлетворител** Не знает теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Не умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Удовлетворительн** Частично знает теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Не умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Хорошо** Знает теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Частично умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Отлично** Знает теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). Умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и

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

ПК.9

Способен осуществлять администрирование сетевых подсистем инфокоммуникационных систем и /или их составляющих

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.9.3 Осуществляет самостоятельную работу по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих	Знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Владеет навыками осуществления самостоятельной работы по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих.	**Неудовлетворител** Не знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Не владеет навыками осуществления самостоятельной работы по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих. **Удовлетворительн** Частично знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Не владеет навыками осуществления самостоятельной работы по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих. **Хорошо** Знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Частично владеет навыками осуществления самостоятельной работы по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих. **Отлично** Знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Владеет навыками осуществления самостоятельной работы по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих.
ПК.9.2 Проводит анализ	Знает средства администрирования сетевых	**Неудовлетворител** Не знает средства администрирования

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
возможности создания системы администрирования сетевых подсистем инфокоммуникационны х систем и /или их составляющих	подсистем инфокоммуникационных систем и /или их составляющих. Умеет проводить анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих.	**Неудовлетворител** сетевых подсистем инфокоммуникационных систем и /или их составляющих. Не умеет проводить анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. **Удовлетворительн** Частично знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Не умеет проводить анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. **Хорошо** Знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Частично умеет проводить анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. **Отлично** Знает средства администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих. Умеет проводить анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих.

ПК.12

Способен к проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.12.2 Анализирует существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном	Знает методы и средства для проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Умеет анализировать существующие возможности контроля проведения	**Неудовлетворител** Не знает методы и средства для проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Не умеет анализировать существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
обеспечении инфокоммуникационной системы	регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы.	**Неудовлетворител** обеспечении инфокоммуникационной системы. **Удовлетворительн** Знает частично методы и средства для проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Не умеет анализировать существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. **Хорошо** Знает методы и средства для проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Частично умеет анализировать существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. **Отлично** Знает методы и средства для проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Умеет анализировать существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы.
ПК.12.3 Осуществляет самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	Знает нормативные документы по проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Умеет осуществлять самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы.	**Неудовлетворител** Не знает нормативные документы по проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Не умеет осуществлять самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. **Удовлетворительн** Частично знает нормативные документы по проведению регламентных работ на сетевых

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн устройствах и программном обеспечении инфокоммуникационной системы. Не умеет осуществлять самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. **Хорошо** Знает нормативные документы по проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Частично умеет осуществлять самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. **Отлично** Знает нормативные документы по проведению регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы. Умеет осуществлять самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы.

ПК.5

Способен к оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.3 Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления	Знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых	**Неудовлетворител** Не знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Не умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
безопасностью	устройств, администрируемой сети с помощью специальных средств управления безопасностью.	**Удовлетворительн** Частично знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Не умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Хорошо** Знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Частично умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Отлично** Знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.

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 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.5.3 Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью **ПК.12.2** Анализирует существующие возможности контроля проведения регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	Раздел 1. Информационная безопасность в сетях передачи данных **Защищаемое контрольное мероприятие**	Знание вариантов реализаций частных политик ИБ сетей передачи данных. Применение политик ИБ в СПД. Владение навыками мониторинга безопасности СПД.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.9.3 Осуществляет самостоятельную работу по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих **ПК.12.3** Осуществляет самостоятельное проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	Раздел 2. Контроль доступа к сети **Защищаемое контрольное мероприятие**	Знание анализируемые показатели безопасности сетей передачи данных. Умение анализировать характеристики и показатели сетей.Навыки оценки эффективности показателей безопасности сетей.
ПК.9.2 Проводит анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих **ПК.11.3** Осуществляет самостоятельно администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) **ПК.11.1** Применяет на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Раздел 3. Виртуальные частные сети и их защита. Итоговый контроль **Защищаемое контрольное мероприятие**	Политика безопасности ИБ СПД.Схема защищенной сети передачи данных. Результат анализа защищенности СПД и соответствия политике ИБ.

Спецификация мероприятий текущего контроля

Раздел 1. Информационная безопасность в сетях передачи данных

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **33**
Проходной балл: **13.8**

Показатели оценивания	Баллы
Студент корректно идентифицирует не менее 10 наиболее критичных угрозы безопасности СПД по заданной схеме, данным мониторинга и описаниям бизнес-процессов	11
Студент корректно создает частную политику ИБ СПД по 10 идентифицированным угрозам	11
Студент корректно реализует 10 мер из частной политики ИБ СПД	11

Раздел 2. Контроль доступа к сети

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **33**
Проходной балл: **13.8**

Показатели оценивания	Баллы
Знает не менее 10 показателей безопасности сетей передачи данных.	11
Студент корректно анализировать не менее 10 характеристик и показателей работы сетей передачи данных.	11
Корректно оценивает эффективность 10 реализованных мер ИБ заданной СПД	11

Раздел 3. Виртуальные частные сети и их защита. Итоговый контроль

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **34**
Проходной балл: **13.8**

Показатели оценивания	Баллы
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
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.	8
Студент корректно проводит анализ защищенности сети передачи данных по заданной схеме или техническому заданию. Проводит анализ соответствия политике безопасности. Не менее 10 различных мер.	8
Студент создает политику безопасности сети передачи данных соответствующую требованиям законодательства и политики предприятия. Не менее 10 пунктов, согласно частной модели угроз.	8