МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное 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 2021 г.

Пермь, 2021

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)

ОПК.6 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

Индикаторы

ОПК.6.1 Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

ОПК.6.2 Осуществляет выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

ОПК.6.3 Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

ОПК.7 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Индикаторы

ОПК.7.2 Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации

ОПК.12 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

Индикаторы

ОПК.12.1 Организует диагностику и тестирование систем защиты информации автоматизированных систем

ОПК.12.2 Проводит анализ уязвимостей систем защиты информации автоматизированных систем

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

Индикаторы

ПК.1.1 Проводит моделирование безопасности информационных систем

ПК.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем

ПК.3 Способен управлять функционированием и защищенностью автоматизированных систем

Индикаторы

ПК.3.2 Устанавливает и настраивает программное обеспечение, необходимое для защиты автоматизированной системы от НСД

ПК.5 Способен анализировать уязвимости внедряемой системы защиты информации

Индикаторы

ПК.5.2 Проводит экспертизы состояния защищенности информации автоматизированных систем

ПК.5.3 Строит модели угроз безопасности информации автоматизированной системы

ОПСК.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить

верификацию данных в открытых информационных системах

Индикаторы

ОПСК.3.1 Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах

ОПСК.3.2 Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах

4. Объем и содержание дисциплины

Специальность	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	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.] ; 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. 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.-Москва: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-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"

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

ОПК.12

Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.12.1 Организует диагностику и тестирование систем защиты информации автоматизированных систем	Знает порядок организации диагностики и тестирования систем защиты информации в сетях передачи данных, умеет тестировать защищенность информационных сетей, владеет навыками обработки результатов тестирования	**Неудовлетворител** Не знает основные способы организации диагностики и тестирования систем защиты информации в сетях передачи данных, не умеет тестировать защищенность информационных сетей, не владеет навыками обработки результатов тестирования **Удовлетворительн** Знает некоторые способы организации диагностики и тестирования систем защиты информации в сетях передачи данных, умеет тестировать защищенность отдельных элементов информационных сетей **Хорошо** Знает основные способы организации диагностики и тестирования систем защиты информации в сетях передачи данных, умеет тестировать защищенность информационных сетей, владеет основными навыками обработки результатов тестирования **Отлично** Знает в полной мере порядок организации диагностики и тестирования систем защиты информации в сетях передачи данных, умеет тестировать защищенность информационных сетей, исчерпывающе владеет навыками обработки результатов тестирования
ОПК.12.2 Проводит анализ уязвимостей систем защиты информации автоматизированных	Умеет и владеет навыком проведения анализа уязвимостей систем защиты информации сетей передачи данных	**Неудовлетворител** Не умеет и не владеет навыком проведения анализа уязвимостей систем защиты информации сетей передачи данных **Удовлетворительн**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
систем		**Удовлетворительн** Умеет проводить основные моменты анализа уязвимостей систем защиты информации сетей передачи данных **Хорошо** Умеет и владеет основными навыками проведения анализа уязвимостей систем защиты информации сетей передачи данных **Отлично** Умеет и владеет в полной мере навыком проведения анализа уязвимостей систем защиты информации сетей передачи данных

ОПК.6

Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.6.1 Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Знает методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей, умеет применять научных подход в исследовании информационной безопасности СПД, владеет навыком обработки результатов исследований ИБ компьютерных сетей	**Неудовлетворител** Не знает методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей,не умеет применять научных подход в исследовании информационной безопасности СПД, не владеет навыком обработки результатов исследований ИБ компьютерных сетей **Удовлетворительн** Знает отдельные приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **Хорошо** Знает основные методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей, умеет применять научных подход в исследовании информационной безопасности СПД, владеет навыком обработки результатов исследований ИБ компьютерных сетей **Отлично** Знает в полной мере методы и приемы научных исследований при проведении разработок в области обеспечения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично безопасности компьютерных систем и сетей, умеет применять научных подход в исследовании информационной безопасности СПД, в полной мере владеет навыком обработки результатов исследований ИБ компьютерных сетей
ОПК.6.2 Осуществляет выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Умеет осуществлять выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**Неудовлетворител** Не умеет осуществлять выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **Удовлетворительн** Умеет осуществлять выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей, но не может в полной мере обосновать свой выбор **Хорошо** Умеет осуществлять выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей, и дает объяснение основных моментов выбора **Отлично** Умеет обоснованно осуществлять выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
ОПК.6.3 Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Умеет и владеет навыками применения методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных сетей	**Неудовлетворител** Не умеет и не владеет навыками применения методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных сетей **Удовлетворительн** Владеет отдельными навыками применения методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных сетей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо В основном умеет и владеет навыками применения методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных сетей **Отлично** В полной мере умеет и владеет навыками применения методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных сетей

ОПК.7

Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.7.2 Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации	Умеет применять методы и средства защиты информации в компьютерных сетях, а также методы и средства защиты информации от утечки по техническим каналам сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации	**Неудовлетворител** Не умеет применять методы и средства защиты информации в компьютерных сетях, а также методы и средства защиты информации от утечки по техническим каналам сетей и систем передачи информации при решении профессиональных задач **Удовлетворительн** Умеет применять отдельные и средства защиты информации в компьютерных сетях, а также методы и средства защиты информации от утечки по техническим каналам сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации **Хорошо** Умеет применять основные методы и средства защиты информации в компьютерных сетях, а также методы и средства защиты информации от утечки по техническим каналам сетей и систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации **Отлично** Умеет в полной мере применять методы и средства защиты информации в компьютерных сетях, а также методы и средства защиты информации от утечки по техническим каналам сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации

ОПСК.3

Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.3.1 Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах	Умеет обнаруживать и владеет навыками устранения нарушения правил разграничения доступа в компьютерных сетях	**Неудовлетворител** Не умеет обнаруживать и не владеет навыками устранения нарушения правил разграничения доступа в компьютерных сетях **Удовлетворительн** Умеет обнаруживать и владеет отдельными навыками устранения нарушения правил разграничения доступа в компьютерных сетях **Хорошо** Умеет обнаруживать и владеет основными навыками устранения нарушения правил разграничения доступа в компьютерных сетях **Отлично** Умеет в полной мере обнаруживать и владеет навыками устранения нарушения правил разграничения доступа в компьютерных сетях
ОПСК.3.2 Определяет источники и причины возникновения	Умеет определять источники и причины возникновения инцидентов безопасности в автоматизированных системах	**Неудовлетворител** Не умеет определять источники и причины возникновения инцидентов безопасности в автоматизированных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
инцидентов безопасности в автоматизированных системах		**Удовлетворительн** Умеет определять отдельные источники и причины возникновения инцидентов безопасности в автоматизированных системах **Хорошо** Умеет определять основные источники и причины возникновения инцидентов безопасности в автоматизированных системах **Отлично** Умеет в полной мере определять источники и причины возникновения инцидентов безопасности в автоматизированных системах

ПК.1

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем	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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично подсистемы ИБ АС. Владеет навыками решения оперативных задач ИБ АС.
ПК.1.1 Проводит моделирование безопасности информационных систем	Владеет навыком моделирования безопасности сетей передачи данных	**Неудовлетворител** Не владеет навыком моделирования безопасности сетей передачи данных **Удовлетворительн** Владеет отдельными навыками моделирования безопасности сетей передачи данных **Хорошо** Владеет основными навыками моделирования безопасности сетей передачи данных **Отлично** Владеет в полной мере навыком моделирования безопасности сетей передачи данных

ПК.5

Способен анализировать уязвимости внедряемой системы защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.2 Проводит экспертизы состояния защищенности информации 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.	**Неудовлетворител** не знает характеристики проектных решений по обеспечению безопасности СПД **Удовлетворительн** знает характеристики проектных решений по обеспечению безопасности СПД **Хорошо** знает характеристики проектных решений по обеспечению безопасности СПД, умеет составлять проектные решения по обеспечению безопасности СПД **Отлично** 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.
ПК.5.3 Строит модели угроз	Владеет навыком построения модели угроз безопасности	**Неудовлетворител** Не владеет навыками построения модели

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
безопасности информации автоматизированной системы	информации вычислительной сети	**Неудовлетворител** угроз безопасности информации вычислительной сети **Удовлетворительн** Владеет в отдельными навыками построения модели угроз безопасности информации вычислительной сети **Хорошо** Владеет в основными навыками построения модели угроз безопасности информации вычислительной сети **Отлично** Владеет в полной мере навыком построения модели угроз безопасности информации вычислительной сети

ПК.3

Способен управлять функционированием и защищенностью автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3.2 Устанавливает и настраивает программное обеспечение, необходимое для защиты автоматизированной системы от НСД	знает как устанавливать и настраивать программное обеспечение, необходимое для защиты СПД от НСД, умеет и владеет навыком настройки систем защиты сети	**Неудовлетворител** не знает как устанавливать и настраивать программное обеспечение, необходимое для защиты СПД от НСД, не умеет и не владеет навыком настройки систем защиты сети **Удовлетворительн** знает как устанавливать и настраивать отдельные элементы программного обеспечения, необходимого для защиты СПД от НСД **Хорошо** знает как устанавливать и настраивать программное обеспечение, необходимое для защиты СПД от НСД, умеет и владеет основными навыками настройки систем защиты сети **Отлично** В полной мере знает как устанавливать и настраивать программное обеспечение, необходимое для защиты СПД от НСД, в полной мере умеет и владеет навыком настройки систем защиты сети

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
ПК.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем **ОПСК.3.1** Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах **ОПСК.3.2** Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах **ОПК.6.2** Осуществляет выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **ОПК.6.3** Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **ОПК.7.2** Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации	Раздел 3. Виртуальные частные сети и их защита **Письменное 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
ОПК.12.2 Проводит анализ уязвимостей систем защиты информации автоматизированных систем		
ПК.1.1 Проводит моделирование безопасности информационных систем **ПК.3.2** Устанавливает и настраивает программное обеспечение, необходимое для защиты автоматизированной системы от НСД **ПК.5.3** Строит модели угроз безопасности информации автоматизированной системы **ОПК.6.1** Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Раздел 5. Технологии обеспечения непрерывности работы сети **Защищаемое контрольное мероприятие**	Знание анализируемые показатели безопасности сетей передачи данных. Умение анализировать характеристики и показатели сетей.Навыки оценки эффективности показателей безопасности сетей.
ПК.5.2 Проводит экспертизы состояния защищенности информации автоматизированных систем **ОПК.12.1** Организует диагностику и тестирование систем защиты информации автоматизированных систем	Раздел 5. Технологии обеспечения непрерывности работы сети **Итоговое контрольное мероприятие**	Политика безопасности ИБ СПД.Схема защищенной сети передачи данных. Результат анализа защищенности СПД и соответствия политике ИБ.

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 сетевыз протоколов	3

канального, сетевого и транспортного уровней	
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 самостоятельной 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	10

частной модели угроз.	
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