МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Политов Александр Владимирович**

Рабочая программа дисциплины

ТРЕК "DEVOPS И АДМИНИСТРИРОВАНИЕ (ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ)"

Код УМК 100588

Утверждено
Протокол №1
от «28» июня 2024 г.

Пермь, 2024

1. Наименование дисциплины

Трек "Devops и администрирование (Защита компьютерных сетей)"

2. Место дисциплины в структуре образовательной программы

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

Направление подготовки: **01.03.02** Прикладная математика и информатика
направленность Инженерия программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Трек "Devops и администрирование (Защита компьютерных сетей)"** у обучающегося должны быть сформированы следующие компетенции:

01.03.02 Прикладная математика и информатика (направленность : Инженерия программного обеспечения)

ПК.3 Способность осуществлять теоретическое обобщение исходных данных, использовать современные математические модели и методы при решении задач моделирования в предметной области

Индикаторы

ПК.3.3 Исследует построенную математическую модель на соответствие проблемной ситуации, разрабатывает алгоритмы и оценивает эффективность их использования

ПК.5 Способен разрабатывать требования и проектировать программное обеспечение

Индикаторы

ПК.5.1 Собирает, систематизирует, выявляет взаимосвязи и документирует требования к компьютерному программному обеспечению, создавая или модифицируя математическую модель; оценивает время и трудоемкость их реализации

4. Объем и содержание дисциплины

Направление подготовки	01.03.02 Прикладная математика и информатика (направленность: Инженерия программного обеспечения)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	6
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	50
Проведение лекционных занятий	16
Проведение практических занятий, семинаров	34
Самостоятельная работа (ак.час.)	58
Формы текущего контроля	Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (6 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

Защита компьютерных 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.

Эссе

Необходимо написать эссе на заданную тематику по средствам и методам построения компьютерных сетей.

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. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/77317.html

3. 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. Пыхалов А. В. Методы и средства интеграции независимых баз данных в распределенных сетях TCP / IP:автореферат дис. ... канд. техн. наук : 05.13.11/А. В. Пыхалов.-Ростов-на-Дону,2012.-18.

2. 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

3. 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://www.intuit.ru/studies/courses/3688/930/lecture/16466 Основы компьютерных сетей
https://www.intuit.ru/studies/courses/3688/930/lecture/16466 Антивирусная защита компьютерных сетей
https://www.intuit.ru/studies/courses/13845/1242/lecture/27503 Безопасность информационных систем
https://www.intuit.ru/studies/courses/498/354/lecture/8442 Сетевая безопасность на основе серверных продуктов Microsoft

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

Образовательный процесс по дисциплине **Трек "Devops и администрирование (Защита компьютерных сетей)"** предполагает использование следующего 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;
- программы демонстрации видео материалов (проигрыватель);
- программа просмотра интернет контента (браузер)

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, лабораторный стенд Академии 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, 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, техническое оснащение которого представлено в паспорте компьютерного класса.

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
Трек "Devops и администрирование (Защита компьютерных сетей)"

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

ПК.3

Способность осуществлять теоретическое обобщение исходных данных, использовать современные математические модели и методы при решении задач моделирования в предметной области

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3.3 Исследует построенную математическую модель на соответствие проблемной ситуации, разрабатывает алгоритмы и оценивает эффективность их использования	Знать методы и модели защиты информации в компьютерных сетях, архитектуры сетей, стандарты и технологии анализа сети и потоков данных. Уметь анализировать построенные математические модели на соответствие проблемной ситуации, разрабатывать алгоритмы и оценивать их эффективность. Владеть навыками выявления уязвимостей и угроз в сетях, а также методами их устранения.	**Неудовлетворительно** Не знает методы и модели защиты информации в компьютерных сетях, архитектуры сетей, стандарты и технологии анализа сети и потоков данных. Не умеет анализировать построенные математические модели на соответствие проблемной ситуации, разрабатывать алгоритмы и оценивать их эффективность. Не владеет навыками выявления уязвимостей и угроз в сетях, а также методами их устранения. **Удовлетворительно** Знает методы и модели защиты информации в компьютерных сетях, архитектуры сетей, стандарты и технологии анализа сети и потоков данных. Не умеет анализировать построенные математические модели на соответствие проблемной ситуации, разрабатывать алгоритмы и оценивать их эффективность. Не владеет навыками выявления уязвимостей и угроз в сетях, а также методами их устранения. **Хорошо** Знает методы и модели защиты информации в компьютерных сетях, архитектуры сетей, стандарты и технологии анализа сети и потоков данных. Умеет анализировать построенные математические модели на соответствие проблемной ситуации, разрабатывать алгоритмы и оценивать их эффективность. Не владеет навыками выявления уязвимостей и угроз в сетях, а также методами их устранения. **Отлично** Знает методы и модели защиты информации в компьютерных сетях, архитектуры сетей, стандарты и технологии анализа сети и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично потоков данных. Умеет анализировать построенные математические модели на соответствие проблемной ситуации, разрабатывать алгоритмы и оценивать их эффективность. Владеет навыками выявления уязвимостей и угроз в сетях, а также методами их устранения.

ПК.5

Способен разрабатывать требования и проектировать программное обеспечение

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.1 Собирает, систематизирует, выявляет взаимосвязи и документирует требования к компьютерному программному обеспечению, создавая или модифицируя математическую модель; оценивает время и трудоемкость их реализации	Знать подходы к разработке требований и проектированию программного обеспечения, включая создание и модификацию математических моделей. Уметь собирать, систематизировать и документировать требования к программному обеспечению, оценивать временные и трудозатратные параметры их реализации. Владеть практическими навыками создания и адаптации математических моделей для различных типов проектов.	**Неудовлетворительно** Не знает подходы к разработке требований и проектированию программного обеспечения, включая создание и модификацию математических моделей. Не умеет собирать, систематизировать и документировать требования к программному обеспечению, оценивать временные и трудозатратные параметры их реализации. Не владеет практическими навыками создания и адаптации математических моделей для различных типов проектов. **Удовлетворительно** Знает подходы к разработке требований и проектированию программного обеспечения, включая создание и модификацию математических моделей. Не умеет собирать, систематизировать и документировать требования к программному обеспечению, оценивать временные и трудозатратные параметры их реализации. Не владеет практическими навыками создания и адаптации математических моделей для различных типов проектов. **Хорошо** Знает подходы к разработке требований и проектированию программного обеспечения, включая создание и модификацию математических моделей. Умеет собирать, систематизировать и документировать требования к программному обеспечению, оценивать временные и трудозатратные параметры их

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо реализации. Не владеет практическими навыками создания и адаптации математических моделей для различных типов проектов. **Отлично** Знает подходы к разработке требований и проектированию программного обеспечения, включая создание и модификацию математических моделей. Умеет собирать, систематизировать и документировать требования к программному обеспечению, оценивать временные и трудозатратные параметры их реализации. Владеет практическими навыками создания и адаптации математических моделей для различных типов проектов.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

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

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 46 до 60
«неудовлетворительно» / «незачтено» менее 46 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3.3 Исследует построенную математическую модель на соответствие проблемной ситуации, разрабатывает алгоритмы и оценивает эффективность их использования **ПК.5.1** Собирает, систематизирует, выявляет взаимосвязи и документирует требования к компьютерному программному обеспечению, создавая или модифицируя математическую модель; оценивает время и трудоемкость их реализации	Эссе **Защищаемое контрольное мероприятие**	знание средств и методов построения компьютерных сетей

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3.3 Исследует построенную математическую модель на соответствие проблемной ситуации, разрабатывает алгоритмы и оценивает эффективность их использования **ПК.5.1** Собирает, систематизирует, выявляет взаимосвязи и документирует требования к компьютерному программному обеспечению, создавая или модифицируя математическую модель; оценивает время и трудоемкость их реализации	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.
ПК.3.3 Исследует построенную математическую модель на соответствие проблемной ситуации, разрабатывает алгоритмы и оценивает эффективность их использования **ПК.5.1** Собирает, систематизирует, выявляет взаимосвязи и документирует требования к компьютерному программному обеспечению, создавая или модифицируя математическую модель; оценивает время и трудоемкость их реализации	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.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3.3 Исследует построенную математическую модель на соответствие проблемной ситуации, разрабатывает алгоритмы и оценивает эффективность их использования **ПК.5.1** Собирает, систематизирует, выявляет взаимосвязи и документирует требования к компьютерному программному обеспечению, создавая или модифицируя математическую модель; оценивает время и трудоемкость их реализации	Раздел 3. Виртуальные частные сети и их защита. Итоговый контроль **Итоговое контрольное мероприятие**	Политика безопасности ИБ СПД. Схема защищенной сети передачи данных. Результат анализа защищенности СПД и соответствия политике ИБ.

Спецификация мероприятий текущего контроля

Эссе

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **1**
Проходной балл: **.5**

Показатели оценивания	Баллы
Письменная работа по организации защищенной сети домашней/корпоративной.	1

Раздел 1. Информационная безопасность в сетях передачи данных

Продолжительность проведения мероприятия промежуточной аттестации: **22 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **33**
Проходной балл: **15**

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: **18 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **33**
Проходной балл: **15**

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: **20 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **33**
Проходной балл: **15**

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.	9
Студент создает политику безопасности сети передачи данных соответствующую требованиям законодательства и политики предприятия. Не менее 10 пунктов, согласно частной модели угроз.	9
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.	9
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.	6