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 ОПЕРАЦИОННЫХ СИСТЕМ

Код УМК 80850

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

Пермь, 2023

1. Наименование дисциплины

Защита операционных систем

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 операционных систем** у обучающегося должны быть сформированы следующие компетенции:

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

ПК.1 Способен к развитию коммутационных подсистем и сетевых платформ, сетей передачи данных, транспортных сетей и сетей радиодоступа, спутниковых систем связи

Индикаторы

ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи

ПК.1.3 Осуществляет развитие сетей и систем 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.5.1 Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных

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

Индикаторы

ПК.9.1 Применяет на практике знания теоретических основ администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих

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)

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	5,6
Объем дисциплины (з.е.)	12
Объем дисциплины (ак.час.)	432
Контактная работа с преподавателем (ак.час.), в том числе:	204
Проведение лекционных занятий	68
Проведение практических занятий, семинаров	136
Самостоятельная работа (ак.час.)	228
Формы текущего контроля	Защищаемое контрольное мероприятие (12) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (5 семестр) Экзамен (6 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

1 семестр

В данном разделе курса формируются знания по основным компонентам ОС.

Многопоточные приложения в ОС

Формируются знания по компонентам многопоточных приложений. Рассматриваются следующие вопросы: средства разработки многопоточных приложений, основные принципы построения многопоточных приложений, подходы к решению проблем разработки многопоточных приложений, средства и методы защиты многопоточных приложений.

Критические секции и объекты в ОС

Формируются знания по критическим секциям и объектам в ОС. Рассматриваются следующие вопросы: средства разработки критических секций и объектов в ОС, основные принципы построения приложений на основе критических секций и объектов в ОС, подходы к решению проблем разработки приложений с использованием критических секций и объектов в ОС, средства и методы защиты критических секций и объектов в ОС.

Мьютексы в ОС

Формируются знания по работе мьютексов в ОС. Рассматриваются следующие вопросы: средства разработки мьютексов в ОС, основные принципы построения приложений на основе мьютексов в ОС, подходы к решению проблем разработки приложений с использованием мьютексов в ОС, средства и методы защиты мьютексов в ОС.

Семафоры с ОС

Формируются знания по работе семафоров в ОС. Рассматриваются следующие вопросы: средства разработки семафоров в ОС, основные принципы построения приложений на основе семафоров в ОС, подходы к решению проблем разработки приложений с использованием семафоров в ОС, средства и методы защиты семафоров в ОС.

События в ОС

Формируются знания по работе событий в ОС. Рассматриваются следующие вопросы: средства разработки событий в ОС, основные принципы построения приложений на основе событий в ОС, подходы к решению проблем разработки приложений с использованием событий в ОС, средства и методы защиты событий в ОС.

Итоговое контрольное мероприятие

Проверка знаний студентов, полученных в результате освоения курса.

2 семестр

В данном разделе курса формируются знания и навыки по построению защищенной распределенной инфраструктуры.

Введение

Основные положения, описания, моменты, связанные с распределенными ОС. Рассматриваются основные понятия, связанные с защитой ОС в доменных структурах.

Классические модели безопасности, Профили защиты и задания безопасности

Изучение классических моделей безопасности применяемых в ОС: мандатная модель, игровая модель, модель Бибопа, модель Белла-Лаппадула. Профили защиты и задания безопасности согласно положениям ФСТЭК и ГОСТ.

Принципы безопасности сетевых ОС, Логические уровни безопасности
Рассматриваются основные принципы безопасности сетевых ОС. Рассматриваются следующие вопросы: архитектура сетевых ОС, встроенные средства безопасности в ОС, внешние средства безопасности ОС и их способы интеграции в систему.

Управление учетными записями, Управление разрешениями на доступ к ресурсам
Рассматриваются оснастки ОС по управлению: учетными записями, разрешениями на доступ к ресурсам. Рассматриваются вопросы применения данных оснасток для работы с распределенными ОС.

Аутентификация Kerberos, Объекты групповых политик
Рассматриваются оснастки ОС по управлению: аутентификацией с помощью протокола Kerberos, объектами групповых политик. Рассматривается алгоритм работы протокола Kerberos, история развития, возможности применения. Рассматриваются вопросы создания групповой политики и ее реализации.

Управление доступом в систему и правами пользователей, Управление ресурсами и доступом к ним
Рассматриваются оснастки ОС по управлению: доступом в систему и правами пользователей, ресурсами и доступа к ним. Рассматриваются вопросы настройки и разграничения прав и ресурсов пользователей ОС.

Отказоустойчивые системы
Рассматриваются возможные варианты по построению отказоустойчивых систем. Рассматриваются вопросы: построения класстеров, отказоустойчивые массивы данных, бесперебойное питание, Blade-массивы.

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. Чекмарев А. Н. Windows 2000 и Windows Server 2003. Администрирование серверов и доменов.:[для администраторов локальных сетей и специалистов по информ. технологиям]/А. Н. Чекмарев.-СПб.:БХВ-Петербург,2006, ISBN 5-94157-260-3.-1104.

2. Байдачный, С. С. .NET Framework 2.0. Секреты создания Windows-приложений / С. С. Байдачный. — 2-е изд. — Москва : СОЛОН-Пресс, 2016. — 520 c. — ISBN 5-98003-245-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/90354

3. Кариев, Ч. А. Разработка Windows-приложений на основе Visual C# : учебное пособие / Ч. А. Кариев. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 978 c. — ISBN 978-5-4497-0909-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/102057.html

Дополнительная:

1. Курячий, Г. В. Операционная система UNIX : учебное пособие / Г. В. Курячий. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 258 c. — ISBN 978-5-4497-0670-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/97557

2. Microsoft Windows 2000 Professional:Учеб. курс MCSA/MCSE. Сертификационный экзамен 70-210: Офиц. пособие Microsoft для самостоят. подготовки/Гл. ред. А. И. Козлов; Пер. с англ. под общ. ред. А. И. Иванова.-3-е изд..-М.:Рус. Редакция,2003, ISBN 5-7502-0246-1.-672.

3. Власов, Ю. В. Администрирование сетей на платформе MS Windows Server : учебное пособие / Ю. В. Власов, Т. И. Рицкова. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 622 c. — ISBN 978-5-4497-0649-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/97536.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.intuit.ru/studies/courses/631/487/info Современные операционные системы

https://studizba.com/lectures/10-informatika-i-programmirovanie/330-lekcii-po-ossio/ Лекции по ОССиО

https://www.intuit.ru/studies/courses/10471/1078/info Введение во внутреннее устройство Windows

https://www.ibm.com/developerworks/ru/library/l-linux-kernel/ Анатомия ядра Linux

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

Образовательный процесс по дисциплине **Защита операционных систем** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice».
Специализированное программное обеспечение: Windows, Linux.

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

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектором и т.д.); экран для проектора, маркерная или меловая доска, компьютер/ноутбук.
Для лабораторных работ требуется аудитория Лаборатории программно-аппаратных средств: аппаратные и программные средства определены паспортом лаборатории.
Для самостоятельной работы требуется аудитория помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета и с доступом к ЭБС.

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 операционных систем

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

ПК.1

Способен к развитию коммутационных подсистем и сетевых платформ, сетей передачи данных, транспортных сетей и сетей радиодоступа, спутниковых систем связи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи	Знает основы систем связи и операционных систем. Умеет делать выборку необходимого ПО и аппаратного обеспечения в информационных системах и системах передачи данных. Владеет навыками работы с информационными системами.	**Неудовлетворител** Не знает основы систем связи и операционных систем. Не умеет делать выборку необходимого ПО и аппаратного обеспечения в информационных системах и системах передачи данных. Не владеет навыками работы с информационными системами. **Удовлетворительн** Знает основы систем связи и операционных систем. Не умеет делать выборку необходимого ПО и аппаратного обеспечения в информационных системах и системах передачи данных. Не владеет навыками работы с информационными системами. **Хорошо** Знает основы систем связи и операционных систем. Умеет делать выборку необходимого ПО и аппаратного обеспечения в информационных системах и системах передачи данных. Не владеет навыками работы с информационными системами. **Отлично** Знает основы систем связи и операционных систем. Умеет делать выборку необходимого ПО и аппаратного обеспечения в информационных системах и системах передачи данных. Владеет навыками работы с информационными системами.
ПК.1.3 Осуществляет развитие сетей и систем связи	Знает основы сетей передачи данных. Умеет работать с типовыми проектами по развитию систем передачи данных. Владеет навыками выбора технологий для	**Неудовлетворител** Не знает основы сетей передачи данных. Не умеет работать с типовыми проектами по развитию систем передачи данных. Не владеет навыками выбора технологий для развития систем передачи данных.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	развития систем передачи данных.	**Удовлетворительн** Знает основы сетей передачи данных. Не умеет работать с типовыми проектами по развитию систем передачи данных. Не владеет навыками выбора технологий для развития систем передачи данных. **Хорошо** Знает основы сетей передачи данных. Умеет работать с типовыми проектами по развитию систем передачи данных. Не владеет навыками выбора технологий для развития систем передачи данных. **Отлично** Знает основы сетей передачи данных. Умеет работать с типовыми проектами по развитию систем передачи данных. Владеет навыками выбора технологий для развития систем передачи данных.

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 основы администрирования систем передачи данных. Умеет осуществлять выбор методов и средств для администрирования систем передачи данных. Владеет навыками администрирования систем передачи данных.	**Неудовлетворител** Не знает основы администрирования систем передачи данных. Не умеет осуществлять выбор методов и средств для администрирования систем передачи данных. Не владеет навыками администрирования систем передачи данных. **Удовлетворительн** Знает основы администрирования систем передачи данных. Не умеет осуществлять выбор методов и средств для администрирования систем передачи данных. Не владеет навыками администрирования систем передачи данных. **Хорошо** Знает основы администрирования систем передачи данных. Умеет осуществлять выбор методов и средств для администрирования систем передачи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо данных. Не владеет навыками администрирования систем передачи данных. **Отлично** Знает основы администрирования систем передачи данных. Умеет осуществлять выбор методов и средств для администрирования систем передачи данных. Владеет навыками администрирования систем передачи данных.
ПК.9.1 Применяет на практике знания теоретических основ администрирования сетевых подсистем инфокоммуникационны х систем и/или их составляющих	Знает теоретические основы систем передачи данных. Умеет на практике применять способы и методы администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих.	**Неудовлетворител** Не знает теоретические основы систем передачи данных. Не умеет на практике применять способы и методы администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих. **Удовлетворительн** Знает частично теоретические основы систем передачи данных. Не умеет на практике применять способы и методы администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих. **Хорошо** Знает теоретические основы систем передачи данных. Умеет на практике применять часть способов и методов администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих. **Отлично** Знает теоретические основы систем передачи данных. Умеет на практике применять способы и методы администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих.
ПК.9.2 Проводит анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационны	Знает основы систем связи. Знает методики и средства администрирования информационных систем и систем передачи данных. Умеет проводить анализ необходимости и возможности	**Неудовлетворител** Не знает основы систем связи. Не знает методики и средства администрирования информационных систем и систем передачи данных. Не умеет проводить анализ необходимости и возможности создания и внедрения системы администрирования

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
х систем и /или их составляющих	создания и внедрения системы администрирования информационных систем и систем передачи данных.	**Неудовлетворител** информационных систем и систем передачи данных. **Удовлетворительн** Знает основы систем связи. Не знает методики и средства администрирования информационных систем и систем передачи данных. Не умеет проводить анализ необходимости и возможности создания и внедрения системы администрирования информационных систем и систем передачи данных. **Хорошо** Знает основы систем связи. Знает методики и средства администрирования информационных систем и систем передачи данных. Не умеет проводить анализ необходимости и возможности создания и внедрения системы администрирования информационных систем и систем передачи данных. **Отлично** Знает основы систем связи. Знает методики и средства администрирования информационных систем и систем передачи данных. Умеет проводить анализ необходимости и возможности создания и внедрения системы администрирования информационных систем и систем передачи данных.

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.5.1 Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите	Знает теоретические основы информационной безопасности информационных систем, нормативно-правовую базу по защите информации. Знает методы и средства по защите информации в системах передачи данных. Умеет	**Неудовлетворител** Не знает теоретические основы информационной безопасности информационных систем, нормативно-правовую базу по защите информации. Не знает методы и средства по защите информации в системах передачи данных. Не умеет применения на практике методы и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
информации, методы и средства по защите информации в системах передачи данных	применения на практике методы и средства по защите информации в системах передачи данных. Владеет навыками организации нормативно-правовой защиты информации в информационных системах.	**Неудовлетворител** средства по защите информации в системах передачи данных. Не владеет навыками организации нормативно-правовой защиты информации в информационных системах. **Удовлетворительн** Знает теоретические основы информационной безопасности информационных систем, нормативно-правовую базу по защите информации. Знает методы и средства по защите информации в системах передачи данных. Не умеет применения на практике методы и средства по защите информации в системах передачи данных. Не владеет навыками организации нормативно-правовой защиты информации в информационных системах. **Хорошо** Знает теоретические основы информационной безопасности информационных систем, нормативно-правовую базу по защите информации. Знает методы и средства по защите информации в системах передачи данных. Умеет применения на практике методы и средства по защите информации в системах передачи данных. Не владеет навыками организации нормативно-правовой защиты информации в информационных системах. **Отлично** Знает теоретические основы информационной безопасности информационных систем, нормативно-правовую базу по защите информации. Знает методы и средства по защите информации в системах передачи данных. Умеет применения на практике методы и средства по защите информации в системах передачи данных. Владеет навыками организации нормативно-правовой защиты информации в информационных системах.

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.11.1 Применяет на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Знает теоретические основы администрирования информационных систем. Знает основы информационной безопасности. Владеет навыками работы со средствами удаленного доступа к информационных системам. Умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).	**Неудовлетворител** Не знает теоретические основы администрирования информационных систем. Не знает основы информационной безопасности. Не владеет навыками работы со средствами удаленного доступа к информационных системам. Не умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Удовлетворительн** Знает теоретические основы администрирования информационных систем. Знает основы информационной безопасности. Не владеет навыками работы со средствами удаленного доступа к информационных системам. Не умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Хорошо** Знает теоретические основы администрирования информационных систем. Знает основы информационной безопасности. Владеет навыками работы со средствами удаленного доступа к информационных системам. Не умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов). **Отлично** Знает теоретические основы администрирования информационных систем. Знает основы информационной безопасности. Владеет навыками работы со средствами удаленного доступа к

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично информационных системам. Умеет применять на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : ИТС

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 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Многопоточные приложения в ОС **Защищаемое контрольное мероприятие**	Знания по теоретическим основам построения многопоточных приложений, умения и навыки по разработке и реализации механизмов многопоточных приложений.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Критические секции и объекты в ОС **Защищаемое контрольное мероприятие**	Знания по теоретическим основам построения приложений на основе критических секций и объектов, умения и навыки по разработке и реализации механизмов критических секций и объектов ОС.
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Мьютексы в ОС **Защищаемое контрольное мероприятие**	Знания по теоретическим основам построения приложений на основе мьютексов, умения и навыки по разработке и реализации механизмов мьютексов ОС.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Семафоры с ОС **Защищаемое контрольное мероприятие**	Знания по теоретическим основам построения приложений на основе семафоров, умения и навыки по разработке и реализации механизмов семафоров ОС.
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	События в ОС **Защищаемое контрольное мероприятие**	Знания по теоретическим основам построения приложений на основе событий, умения и навыки по разработке и реализации механизмов событий ОС.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Знает пройденный материал курса и умеет применить его на практике.

Спецификация мероприятий текущего контроля

Многопоточные приложения в ОС

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **16**
Проходной балл: **7**

Показатели оценивания	Баллы
Многопоточное приложение согласно поставленному заданию и правильный результат работы программы согласно поставленному заданию.	16

Критические секции и объекты в ОС

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **16**
Проходной балл: **7**

Показатели оценивания	Баллы
Приложение согласно поставленному заданию и правильный результат работы программы согласно поставленному заданию.	16

Мьютексы в ОС

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **16**
Проходной балл: **7**

Показатели оценивания	Баллы
Приложение согласно поставленному заданию и правильный результат работы программы согласно поставленному заданию.	16

Семафоры с ОС

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **16**
Проходной балл: **7**

Показатели оценивания	Баллы
Приложение согласно поставленному заданию и правильный результат работы программы согласно поставленному заданию.	16

События в ОС

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **16**
Проходной балл: **7**

Показатели оценивания	Баллы
Приложение согласно поставленному заданию и правильный результат работы программы согласно поставленному заданию.	16

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Правильно решенные задания контрольного мероприятия.	20

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 46 до 60
«неудовлетворительно» / «незачтено» менее 46 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи	Введение **Защищаемое контрольное мероприятие**	Знания теоретических основ систем защиты ОС, умения и навыки в оперирование основными понятиями базовой модели ОС.
ПК.1.3 Осуществляет развитие сетей и систем связи **ПК.9.2** Проводит анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих	Классические модели безопасности, Профили защиты и задания безопасности **Защищаемое контрольное мероприятие**	Знания теоретических основ моделей безопасности, умения и навыки в области разработки профилей защиты и задания безопасности.
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Принципы безопасности сетевых ОС, Логические уровни безопасности **Защищаемое контрольное мероприятие**	Знания теоретических основ принципов безопасности ОС, умения и навыки применять теоретические знания принципов безопасности ОС на практике.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.9.1 Применяет на практике знания теоретических основ администрирования сетевых подсистем инфокоммуникационных систем и/или их составляющих **ПК.11.1** Применяет на практике знания теоретических основ администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Управление учетными записями, Управление разрешениями на доступ к ресурсам **Защищаемое контрольное мероприятие**	Знания по теоретическим основам разработки систем доступа к ресурсам в доменной структуре, умения и навыки использования теоретических знаний на практике.
ПК.1.3 Осуществляет развитие сетей и систем связи **ПК.9.2** Проводит анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих	Аутентификация Kerberos, Объекты групповых политик **Защищаемое контрольное мероприятие**	Знания по теоретическим основам разработки систем доступа к ресурсам в доменной структуре на уровне групповых политик локально и удаленно, с помощью протокола Kerberos, умения и навыки использования теоретических знаний на практике.
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.9.3** Осуществляет самостоятельную работу по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих	Управление доступом в систему и правами пользователей, Управление ресурсами и доступом к ним **Защищаемое контрольное мероприятие**	Знания по теоретическим основам разработки управления доступом в систему ОС, ресурсам, умения и навыки использования теоретических знаний на практике.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.3 Осуществляет развитие сетей и систем связи **ПК.9.3** Осуществляет самостоятельную работу по администрированию сетевых подсистем инфокоммуникационных систем и /или их составляющих **ПК.9.2** Проводит анализ возможности создания системы администрирования сетевых подсистем инфокоммуникационных систем и /или их составляющих	Отказоустойчивые системы **Защищаемое контрольное мероприятие**	Знания по теоретическим основам построения отказоустойчивых систем, умения и навыки применения теоретических знаний на практике.

Спецификация мероприятий текущего контроля

Введение

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Отчет по проведенному анализу.	5
Анализ доменной структуры согласно базовым принципам построения распределенных ОС.	5

Классические модели безопасности, Профили защиты и задания безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**
Проходной балл: **7**

Показатели оценивания	Баллы
Отчет по проведенному анализу.	10
Анализ конкретной доменной структуры согласно классическим моделям безопасности.	5

Принципы безопасности сетевых ОС, Логические уровни безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**
Проходной балл: **7**

Показатели оценивания	Баллы
Отчет по проделанной работе.	10
Собственная политика безопасности в доменной структуре на примере конкретной задачи.	5

Управление учетными записями, Управление разрешениями на доступ к ресурсам

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**
Проходной балл: **7**

Показатели оценивания	Баллы
Отчет по проделанной работе.	10
Собственная политика безопасности на уровне пользователей в доменной структуре на примере конкретной задачи.	5

Аутентификация Kerberos, Объекты групповых политик

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**
Проходной балл: **7**

Показатели оценивания	Баллы
Настройка протокола Kerberos для удаленной аутентификации пользователя.	8
Отчет по проделанной работе.	7

Управление доступом в систему и правами пользователей, Управление ресурсами и доступом к ним

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**
Проходной балл: **7**

Показатели оценивания	Баллы
Отчет по проделанной работе.	10
Собственная политика безопасности на уровне управления доступом в систему ОС, ресурсами ОС.	5

Отказоустойчивые системы

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**
Проходной балл: **7**

Показатели оценивания	Баллы
Отчет по проделанной работе.	10
Построить класстер на базе своего ПК.	5