МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

АДМИНИСТРИРОВАНИЕ И БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль ***Администрирование и безопасность операционных систем***	**Код модуля** № 1138284 УП № 5433, в. 4, № 6323, в. 4
Образовательная программа ***Информационная безопасность телекоммуникационных систем***	**Код ОП** ***10.05.02***
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки ***Информационная безопасность***	**Код направления и уровня подготовки** 10.05.02/01.01
Уровень подготовки ***Специалитет***	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: ***№1426 16 ноября 2016 г***

Екатеринбург, 2017

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Бакланов Валентин Викторович	к.т.н., доцент	доцент	Радиоэлектроники и связи	
2	Виноградова Нина Сергеевна	-	Старший преподаватель	Радиоэлектроники и связи	
3	Авдеев Денис Викторович	-	Старший преподаватель	Радиоэлектроники и связи	

Руководитель модуля Н.С. Виноградова

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Председатель учебно-методического совета В.Г. Коберниченко
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль Н.С. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ «АДМИНИСТРИРОВАНИЕ И БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

1.1. Объем модуля, 8 з.е.

1.2. Аннотация содержания модуля

Модуль относится к вариативной части образовательной программы (выбор вуза).

Изучаются структура, задачи и функциональные компоненты универсальных операционных систем Windows, Linux и MacOSX. Основное внимание уделено подсистемам обеспечения безопасности ОС, в частности, ограничению и разграничению доступа в систему, администрированию учетных записей пользователей, защите целостности системных программ и данных, созданию изолированной программной среды и др. Рассматриваются сетевые функции ОС, резервирование и восстановление данных, парольные системы и безопасность интерактивного режима.

Особое внимание уделено формированию у обучаемых исследовательских и практических навыков, которые отрабатываются в ходе многочисленных лабораторных работ. Предусмотрено выполнение и защита проектной работы.

1. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Очная форма обучения

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		**Семестр изучения**	**Объем времени, отведенный на освоение дисциплин модуля**							
			Аудиторные занятия, час.				**Самостоятельная работа, включая все виды текущей аттестации, час.**	**Промежуточная аттестация (зачет, экзамен), час.**	**Всего по дисциплине**	
			Лекции	**Практические занятия**	**Лабораторные работы**	**Всего**			**Час.**	**Зач. ед.**
1.	(ВВ) Безопасность операционных систем	7	34		34	68	76	экз	144	4
2.	(ВВ) Операционные системы	6, 7	17		34	51	57	зачет	108	3
3.	(ВВ) Проект по модулю	7					36	ПМ	36	1
			51		**68**	**119**	**169**		**288**	**8**

Заочная форма обучения не предусмотрена

2. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	*Криптографические методы защиты информации* *Информационные технологии* *Методы и языки программирования*
3.2.	**Кореквизиты**	*Безопасность вычислительных сетей* *Защита электронного документооборота* *Программно-аппаратные средства защиты информации*

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

3.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля	Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля	Универсальные компетенции (УОК, УОПК,УПК), формируемые при освоении модуля для нескольких ОП
	РО-05 Способность обеспечивать в рамках эксплуатационной деятельности защищенность и функциональность инфотелекоммуникационных систем, производить их администрирование и профилактику работоспособности	ПК-14 способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем ПК-15 способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания ПСК-10.5 способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи ПКД-5 способность восстанавливать работоспособность систем защиты при сбоях и нарушении функционирования ПКД-6 способность обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи ПКД-7 способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищённые	

		операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации ПКД-8 способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение ПКД-9 способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищённые операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации ПКД-10 способность разрабатывать и анализировать модели угроз, обеспечивать защищенность и стабильность функционирования файловых систем, а также реализовывать процесс восстановления информации в случае повреждения их целостности	

4.2 Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ПК-14	ПК-15	ПСК-10.5	ПКД-5	ПКД-6	ПКД-7	ПКД-8	ПКД-9	ПКД-10
1	(ВВ) Безопасность операционных систем	*	*		*		*	*		*
2	(ВВ) Операционные системы			*		*			*	*
3	(ВВ) Проект по модулю	*	*	*	*	*	*	*	*	*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю:
Не предусмотрен

5.2. Форма промежуточной аттестации по модулю:

В ходе выполнения курсового проекта по модулю студенты закрепляют знания, умения и навыки защиты компьютерной информации на уровне операционных систем, практического администрирования защищенных операционных систем, закрепляют знания о реализации защитных механизмов в современных операционных системах.

5.3. Фонд оценочных средств для проведения промежуточной аттестации по модулю (Приложение 1)

ПРИЛОЖЕНИЕ 1
к рабочей программе модуля

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

Система критериев оценивания результатов обучения в рамках модуля опирается на три уровня освоения: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю
Не предусмотрен

5.3.2.2. Перечень примерных тем итоговых проектов по модулю

- *Анализ защитных механизмов операционных систем семейства Windows*
- *Анализ защитных механизмов операционных систем семейства Linux*
- *Анализ защитных механизмов операционных систем семейства Android*
- *Анализ защитных механизмов операционных систем семейства MacOS*

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль ***Администрирование и безопасность операционных систем***	**Код модуля** № 1138284 (в справочнике модулей ЕТСУ) УП №№ 5433, в. 4, № 6323, в. 4
Образовательная программа ***Информационная безопасность телекоммуникационных систем***	**Код ОП** ***10.05.02.65.01.01***
Направление подготовки ***Информационная безопасность***	**Код направления и уровня подготовки** ***10.05.02***
Уровень подготовки ***специалитет***	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: ***№1426 16 ноября 2016 г***

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Авдеев Денис Викторович	-	Старший преподаватель	Радиоэлектроники и связи	
2	Бакланов Валентин Викторович	К.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля Н.С. Виноградова

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Председатель учебно-методического совета В.Г. Коберниченко
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению защитных механизмов, реализованных в современных универсальных операционных системах Windows*, Linux, FreeBSD, Mac OS X.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- ПК-14 - способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем;
- ПК-15 - способность проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания;
- ПКД-5 - способность восстанавливать работоспособность систем защиты при сбоях и нарушении функционирования;
- ПКД-7 - Способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищённые операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПКД-8 - способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение;
- ПКД-10 - способность разрабатывать и анализировать модели угроз, обеспечивать защищенность и стабильность функционирования файловых систем, а также реализовывать процесс восстановления информации в случае повреждения их целостности.

В результате освоения дисциплины студент должен:

Знать:

- угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии;
- основные принципы защиты компьютерной информации в операционных системах;
- виды и стратегии резервирования информации;
- программную архитектуру распространенных файловых систем FAT, NTFS, EXT*FS, UFS;
- методы исследования, поиска и восстановления информации на носителях с файловыми системами FAT, NTFS, EXT*FS, UFS;
- методику восстановления данных в поврежденных файловых системах и на поврежденных машинных носителях;
- механизмы защиты информации от несанкционированного доступа, встроенные в операционные системы Windows*, Linux, FreeBSD, Mac OS X;
- основные принципы администрирования операционных систем.

Уметь:

- выполнять функции администратора операционных систем;
- осуществлять планирование и создание учетных записей пользователей и рабочих групп, выполнять разграничение доступа к ресурсам компьютерных систем средствами ОС;
- производить основные настройки операционных систем, обеспечивающие требуемый

уровень безопасности компьютерной информации;
- настраивать политику аудита, анализировать события, регистрируемые в журнальных файлах;
- настраивать сетевую инфраструктуру распространенных операционных систем;
- выполнять сбор информации о сетевом трафике, производить его анализ с целью оптимизации и обеспечения безопасности компьютерной сети;
- осуществлять управление сетевыми узлами с помощью средств системных служб и протокола SNMP;
- использовать стандартные сетевые утилиты операционных систем с целью диагностики и поиска неисправностей в сети;
- выполнять резервирование системной информации и данных;
- выполнять автоматическое и «ручное» восстановление системной информации, удаленных и испорченных данных;

Владеть (демонстрировать навыки и опыт деятельности):
- профессиональной терминологией в области информационной безопасности;
- методами и средствами сбора информации о сетевом трафике;
- навыками защиты информационных систем;
- навыками настройки операционных систем.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*7*
1.	**Аудиторные занятия**	68	68	68
2.	Лекции	34	34	34
3.	Практические занятия			
4.	Лабораторные работы	34	34	34
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	76	10,2	76
6.	**Промежуточная аттестация**	Э	2,33	Э
7.	**Общий объем по учебному плану, час.**	144	80,53	144
8.	**Общий объем по учебному плану, з.е.**	4		4

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Общие принципы безопасности операционных систем**	Ключевые элементы программной архитектуры операционных систем (ОС), определяющие защиту компьютерной информации и безопасность ЭВМ. Архитектура многозадачной сетевой операционной системы. Уровень ядра и уровень приложений. Объекты ядра. Аппаратно–зависимый программный слой. Защищенные файловые системы. Владение файловыми объектами и права доступа к ним. Изменение разрешений на доступ к файлам. Размещение элементов файловой системы на дисковом пространстве. Типовые файловые системы. Структура и назначение метаданных файлов. Понятие политики разграничения доступа в компьютерных системах. Одноуровневая и многоуровневая модели разграничения доступа, их достоинства и недостатки. Реализация технологии разграничения доступа в операционных системах. Модель безопасности и ее архитектура. Администрирование учетных записей пользователей. Группы пользователей. Права и привилегии пользователей и групп. Управление системной политикой безопасности. Стратегия предоставления прав на доступ к ресурсам. Хранение парольной информации. Алгоритм сетевой аутентификации. Обеспечение безопасности при удаленном доступе. Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС. Безопасность системных данных. Способы защиты системных файлов от незаконной модификации. Управление памятью. Механизмы виртуальной памяти. Создание и уничтожение процессов. Управление процессами и контроль над ними. Реализация многозадачного и многопоточного режимов. Механизмы системных вызовов. Защита на уровне межпроцессного взаимодействия. Сокрытие процессов. Реализация защитных требований на уровне командной оболочки. Защита программного обеспечения от незаконной модификации. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора.
2	**Защита компьютерной информации в операционных системах**	Ключевые элементы программной архитектуры ОС, влияющие на защиту информации. Базовые понятия. Основные отличия операционных систем Linux и FreeBSD.

	Linux и FreeBSD	Файл как универсальный объект ОС. Виды файлов. Права доступа к файлам. Основные команды, позволяющие работать с файлами. Действия над обычными файлами: создание, копирование, перемещение, удаление. Работа с каталогами. Создание и изменение разрешений на доступ к файлам. Использование «жестких» и символических ссылок. Дополнительные атрибуты файлов, поддерживаемые в ОС Linux. Работа со специальными файлами устройств. Загрузчики операционных систем LILO, GRUB. Обеспечение защиты от НСД при загрузке ОС. Вход в систему в однопользовательском режиме. Загрузка ПК с LiveCD с целью устранения неполадок. Архитектура файловых систем ext*fs и ufs*. Размещение элементов файловой системы на дисковом пространстве. Назначение и структура суперблока, описателей групп блоков, карт битовых полей, индексных дескрипторов, журнала транзакций. Структура индексного дескриптора регулярного файла, каталога, символической ссылки. Работа с устройствами дисковой и полупроводниковой памяти. Создание, изменение и удаление дисковых разделов. Отображение информации о дисковых разделах и файловых системах. Форматирование разделов и создание файловых систем. Конфигурационный файл /etc/fstab. Монтирование устройств и дисковых разделов с различными файловыми системами. Размещение файловых систем на дисковом пространстве. Монтирование разделов памяти с различными файловыми системами. Установление дисковых квот. Восстановление логически удаленных или поврежденных файлов. Последовательность логического удаления файлов в файловых системах ext*fs и ufs*. Виды повреждений файловой системы. Утилиты для работы с поврежденными файловыми системами. Возможности дисковых редакторов типа Linux Disk Editor и отладчиков файловых систем для восстановления утерянной компьютерной информации. Особенности восстановления файлов в различных файловых системах. Использование записей из журнальных файлов. Блочное копирование информации с поврежденных машинных носителей с помощью утилиты dd. Ключевые аргументы командной строки. Сетевое копирование с использованием утилиты netcat. Атрибуты процесса. Файловая система /proc как «зеркало» процессов. Переменные окружения. Создание и уничтожение процессов, изменение их приоритетов. Способы автоматического запуска и остановки программ. Периодически запускаемые процессы. Запуск и остановка программ в интерактивном и фоновом режимах. Средства взаимодействия между процессами. Перенаправление ввода/вывода. Терминальный режим и консольные атаки. Вывод информации о процессах. Наблюдение за процессами и контроль производительности системы. Признаки камуфляжа несанкционированно выполняемых процессов. Программные возможности сокрытия процессов. Использование возможностей командных оболочек

		при решении штатных задач администрирования. Типовой синтаксис команд. Запуск программ в фоновом режиме. Запуск нескольких команд, в т.ч. по условию. Командные файлы. Перенаправление ввода и вывода. Конвейеры. Управление операционной системой в многотерминальном режиме. Работа с файловым менеджером Midnight Commander. Пользователи и их виды. Группы пользователей. Учетные записи пользователей и работа с ними. Изменение, редактирование, удаление и временное блокирование учетных записей. Конфигурационные файлы group, passwd, master.passwd, shadow, login.defs. Временные отметки и признаки паролей. Смена паролей. Процедура регистрации и ее безопасность. Смена пользователей. Предоставление эффективных прав доступа. Использование механизма SUDO. Практические задачи на разграничение доступа и их решения. Предоставление пользователям временных прав суперпользователя. Распространенные атаки на права администратора системы. Исследование учетных записей пользователей. Обнаружение неавторизованных учетных записей пользователей и групп. Копирование и запись данных. Архивация и резервирование. Сетевые возможности операционных систем. Контроль и настройка сетевых интерфейсов. Разведка узлов компьютерной сети и сетевых служб. Методы сканирования узлов ЛВС. Возможности утилиты nmap. Режимы открытого и скрытного сканирования. Перехват и анализ сетевого трафика с помощью утилиты tcpdump. Задание условий фильтрации трафика. Особенности настройки и проверки работоспособности узлов беспроводных сетей. Уязвимости алгоритмов криптографической защиты. Наблюдение и аудит в ОС Linux и FreeBSD. Сбор информации об опасных файловых объектах. Поиск необычных и скрытых файлов и каталогов. Наблюдение за процессами и пользователями. Отслеживание взаимосвязей между субъектами, процессами и объектами. Аудит событий и его безопасность. Системные протоколы, их расположение и заполнение. Источники, потребители и уровни значимости сообщений. Защита системы протоколирования событий. Основные ошибки и просчеты в администрировании компьютерных сетей под управлением операционных систем Linux и FreeBSD. Анализ настроек безопасности UNIX-систем.
3	**Защита компьютерной информации в операционных системах семейства Windows**	Реализация технологии разграничения доступа в ОС Windows *. Объекты и субъекты доступа. Права и методы доступа. Дескриптор защиты. Дискреционный список контроля доступа. Системный список контроля доступа. Структура маркера доступа. Процесс проверки подлинности при входе в систему. Стратегия предоставления прав на доступ к ресурсам. Защита данных средствами разрешений файловой системы NTFS. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows*. Методы идентификации и аутентификации

		пользователей, применяемые в ОС Windows*. Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS. Структура зашифрованного файла. Создание ключа и сертификата агента восстановления. Хранение парольной информации. Анализ уязвимости паролей пользователей. Алгоритмы локальной и сетевой аутентификации. Механизмы криптографической защиты данных на логических разделах и съемных носителях информации, реализованные в ОС Windows 7. Технология BitLocker. Создание замкнутой программной среды с помощью функции AppLocker. Организация файловой системы NTFS. Основные свойства файловой системы NTFS. Структура MFT. Стандартные атрибуты файлов и каталогов в NTFS. Основные операции над объектами файловой системы. Резидентные и нерезидентные атрибуты. Потоки. Структура каталогов. Размещение файловой системы на дисковом пространстве. Разграничение доступа в ОС Windows*. Планирование и создание учетных записей пользователей и рабочих групп. Разграничение доступа к ресурсам. Разрешения доступа к общим папкам. Получение доступа к пользовательским данным с правами администратора. Структура системного реестра ОС Windows*. Редактирование реестра. Разделы и настройки системного реестра, определяющие политику безопасности. Использование реестра для настройки параметров ОС. Утилиты администрирования реестра с интерфейсом командной строки. Анализ и настройка политики безопасности. Анализ параметров безопасности. Рекомендуемые права пользователей. Управление системной политикой безопасности. Политика учетных записей. Разработка шаблона политики безопасности. Анализ и настройка политики безопасности с применением шаблонов. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора. Настройки журнала аудита. Анализ и восстановление данных на логических разделах NTFS. Подключение машинных носителей с NTFS-разделами. Восстановление главной загрузочной записи. Восстановление таблицы разделов и загрузочного сектора. Приемы и программное обеспечение для «ручного» восстановления удаленных файлов на NTFS-разделах. Возможности автоматизированного восстановления удаленных файлов. Анализ сетевых служб Windows*. Анализ сетевых компьютеров с использованием стандартных сетевых команд. Анализ сетевых узлов с использованием программ-сканеров портов. Анализ возможности сетевого подключения к файловым ресурсам Windows*. Использование инструментальных средств аудита безопасности компьютерных систем.
4	**Особенности защиты компьютерной**	Создание, изменение и удаление учетных записей пользователей. Регистрация в системе и

	информации в операционной системе Mac OS X	выход из нее. Включение и использование учетной записи суперпользователя **root**. Виды паролей: пароль учетной записи, пароль администратора, мастер-пароль, пароль суперпользователя. Выбор паролей с помощью **Password Assistant**. Пароли в виде «связки ключей». Сброс и обновление паролей. Аппаратный пароль **Firmware Password**. Работа с файлами. Надежное удаление файлов. Права доступа к файлам. Запрет изменений файлов. Особенности файловой системы **hfsplus**. Структура файлов. Восстановление поврежденных файлов. Использование механизма SUDO для предоставления пользователям дополнительных прав. Системные настройки безопасности. Шифрование пользовательских данных с помощью **FileVault**. Включение и выключение механизма шифрования. Недостатки режима шифрования. Контроль за режимом изоляции программной среды. Системная защита от вредоносных программ и сетевых атак. Загрузка операционной системы в однопользовательском режиме. Защита компьютеров Apple от непосредственного доступа. Экранная заставка. Контроль рабочего места с помощью видеорегистрации. Настройка средств сетевой защиты Mac OS X 10.6. Особенности регистрации системных событий. Расположение и безопасность журналов аудита.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 8
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																								
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*				
1	Общие принципы безопасности операционных систем		**9**	4		5	6	3	1		2													3	1		Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
2	Защита компьютерной информации в операционных системах Linux и FreeBSD		**20**	10		10	18	9	4		5		4	1										5	1					
3	Защита компьютерной информации в операционных системах семейства Windows		**22**	10		12	19	10	3		7		4	1										5	1					
4	Особенности защиты компьютерной информации в операционной системе Mac OS X		**17**	10		7	15	6	3		3		4	1										5	1					
	Всего (час), без учета промежуточной аттестации:	**126**	**68**	**34**		**34**	58	23	6		17		12	12										**18**	**18**					
	Всего по дисциплине (час.):	**144**	**68**					В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Исследование файловых объектов с правами пользователя	3
1	2	Исследование архитектуры файловых систем ext*fs	2
2	3	Восстановление данных программными средствами ОС Linux	2
2	4	Исследование процессов в ОС Linux	2
2	5	Исследование сетевых возможностей ОС Linux	2
2	6	Исследование беспроводной сети WiFi под управлением ОС Linux	2
2	7	Наблюдение и аудит в ОС Linux	2
3	8	Основы администрирования ОС Windows *	2
3	9	Использование реестра для настройки параметров ОС Windows *	2
3	10	Ручное восстановление данных на разделах FAT и NTFS	2
3	11	Аудит событий безопасности ОС Windows	2
3	12	Применение стандартных механизмов защиты ОС Windows 7	2
3	13	Применение механизма защиты шифрования файлов в ОС Windows 7 с использованием шифрующей файловой системы EFS. Применение механизма защиты BitLocker.	2
4	14	Исследование защитных механизмов операционной системы Mac OS X 10.6	7
		Всего:	**34**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Реализация политики разграничения доступа средствами ОС Linux.*
- *Настройка политики безопасности ОС Windows *.*
- *Настройка Родительского контроля в Mac OS X 10.6.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

- *Модель безопасности и ее архитектура.*
- *Ключевые элементы программной архитектуры ОС Linux, влияющие на защиту информации.*
- *Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows*.*
- *Системные настройки безопасности ОС Mac OS X.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Общие принципы безопасности операционных систем				*	*							
2.Защита компьютерной информации в операционных системах Linux и FreeBSD				*	*							
3.Защита компьютерной информации в операционных системах семейства Windows				*	*							
4.Особенности защиты компьютерной информации в операционной системе Mac OS X				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007 .— 136 с. 90 экз.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.

9.1.2.Дополнительная литература

3. Олифер В. Г. Сетевые операционные системы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер .— 2-е изд. — Москва [и др.] : Питер, 2008 .— 669 с. 10 экз.
4. Уайт К. Основы обслуживания Mac OS X. Руководство по обслуживанию и разрешению проблем Mac OS X 10.5 / Кевин М. Уайт ; [пер. с англ. О. Труфанова] .— Москва : ЭКОМ, 2009 .— 592 с. 1 экз
5. Пог.Д. Mac OS X Leopard. Основное руководство / Дэвид Пог ; [пер. с англ. С. Маккавеева] .— Санкт-Петербург ; Москва : Символ-Плюс, 2008 .— 880 с. 1 экз.
6. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с. 10 экз.
7. Ивановский С. Операционная система Linux: Сборник часто задаваемых вопросов и ответов на них / С. Ивановский .— М. : Познавательная книга плюс, 2001 .— 224 с. 1 экз.
8. Робачевский А.М. Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский .— Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002 .— 514 с. 9. экз.

9.2.Методические разработки

1. Синадский Н.И. Безопасность операционных систем. УМК, 2007. Метаданные ресурса №7029

9.3.Программное обеспечение

ОС Linux, Windows, Mac OS X

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*7,1-7*	*20*
Домашняя работа №2	*7,1-15*	*20*
Домашняя работа №3	*7,1-15*	*20*
Контрольные работы №1-4	*7,1-15*	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение лабораторных работ	*7,1-15*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с наличием Дисциплины и ее аналогов, по которым возможно тестирование, на портале СМУДС УрФУ, возможно тестирование в рамках НТК.

ПРИЛОЖЕНИЕ 3

к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.
2. Методы и средства защиты информации в системах с проводными линиями. Типы проводных линий. Виды угроз, создаваемых проводными линиями. Оценка степени паразитных связей в линиях и уровней паразитных излучений, создаваемых проводными линиями.
3. Паразитные каналы утечки информации в телефонных системах и телефонных кабелях. Акустоэлектрические преобразования в телефонных аппаратах при опущенной трубке. Оценка уровней сигналов и уровней помех в телефонных линиях. Оценка реальности образования канала утечки. Защита от утечки с использованием диодных устройств типа «Гранит», «Корунд» и других. Особенности работы этих устройств в современных электронных аппаратах.
4. Применение генераторов шума для закрытия канала утечки за счет акустоэлектрического преобразования. Виды зашумления телефонных линий с целью закрытия каналов утечки информации.
5. Высокочастотное навязывание в телефонных системах. Механизмы взаимодействия акустического сигнала с высокочастотным сигналом навязывания. Оценка реальности канала утечки за счет высокочастотного навязывания. Оценка чувствительности метода.
6. Преднамеренно созданные каналы утечки по проводным линиям. Включение закладных устройств с передачей информации по проводам. Маскировка сигналов путем использования занятых проводных линий: радиотрансляционных сетей,

телефонных линий, сетей электропитания и других. Возможности и методы выделения сигналов в проводных линиях от помех. Компенсация помех. Адаптивные автокомпенсаторы.

7. Аппаратура выделения информации методом ВЧ навязывания, возможности и методы обеспечения высокой чувствительности. Меры борьбы с ВЧ навязыванием. Аппаратура контроля за утечкой информацией по каналам ВЧ навязывания.
8. Закладные устройства в системах с проводными коммуникациями. Устройства съема речевой информации в телефонных линиях. Методы подключения устройств. Использование диктофонов. Методы защиты от описанных закладных устройств. Аппаратура контроля и защиты от утечки информации по проводным линиям. Недостатки существующей аппаратуры.
9. Электрические характеристики и принцип работы городских телефонных линий. Возможные способы подключения закладных устройств к телефонным линиям. Количественные характеристики возмущений, вносимых закладными устройствами, и оценка возможности обнаружения закладных устройств. Примеры построения телефонных радио ретрансляторов (закладных устройств) с питанием от телефонных линий и оценка степени их влияния на параметры телефонных линий.
10. Методы защиты телефонных (и других проводных) линий от утечки информации через закладные устройства, параллельные телефоны и другими путями:
11. Способы реализации данных методов. Достоинства и недостатки. Проблемы реализации.
12. Применение фильтров для борьбы с утечкой информации по проводным линиям. Требования к характеристикам фильтров. Фильтры, предназначенные для защиты от утечки информации по сети 220 В. Особенность сетевых фильтров. Проектирование сетевых фильтров. Схемная реализация фильтров: независимые фазные фильтры; связанные фильтры. Реализация индуктивных и емкостных элементов сетевых фильтров. Ограничения, накладываемые на характеристики фильтров эксплуатационными требованиями.
13. Включение фильтров. Синфазные и противофазные сигналы и наводки в фильтрах. Заземление фильтров. Фильтры, предназначенные для защиты от мощных импульсных помех и преднамеренных воздействий. Меры защиты других проводных линий: провода пожарной и охранной сигнализаций, провода линий оповещения, городская трансляционная сеть, кабели компьютерных сетей, другие проводные линии.
14. Каналы утечки информации образованные электромагнитным излучением. Утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Виды каналов утечки за счет ПЭМИН. Основные средства (обработки конфиденциальной информации). Образование каналов утечки за счет наводок с основных средств на вспомогательные. Определение количественных характеристик цепей паразитных связей. Паразитные емкостная, индуктивная и связи.
15. Закладные устройства, использующие радиоканал. Средства индивидуальной радиосвязи: сотовые телефоны, бесшнуровые телефонные аппараты, пейджеры и другие.
16. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Возможности современной радиоэлектроники по построению закладных устройств.
17. Проблемы обнаружения и борьбы с закладными устройствами (ЗУ). Обеспечение энергетической скрытности (ЗУ). Потенциал радиоканала. Оценка эффективности антенн передатчиков и радиоприемников. Оценка минимальной мощности передатчиков (ЗУ). Оценка пороговой чувствительности радиоприемников.

18. Приборы для обнаружения электромагнитных излучений. Широкополосные индикаторы напряженности поля. Узкополосные сканирующие приемники. Проблемы, связанные с их применением. Принцип построения названных приборов. Проблемы построения сканирующих приемников. Обеспечение высокой избирательности по паразитным каналам приема. Обеспечение высокой скорости обзора широкого частотного диапазона.
19. Методы обнаружения закладных устройств и паразитных излучений с применением широкополосных индикаторов и сканирующих приемников. Мониторинг эфира. Акустическая завязка. Акустическая локация. Корреляционная обработка принятых сигналов. Проблемы, возникающие при обнаружении закладных устройств.
20. Закладные устройства, использующие сложные сигналы. Возможности реализации таких устройств на современной элементной базе. Возможности обнаружения таких устройств. Направление построения аппаратуры для обнаружения излучений со сложными сигналами.
21. Построение радиоканалов передачи данных (сообщений) с цифровой обработкой сигналов и с использованием сложных широкополосных несущих. Возможности и примеры построения радиопередатчиков со сложными сигналами. Микросхемы XE1202, AD9850. Построение радиоприемников сложных сигналов: с псевдослучайной перестройкой частоты. Проблемы синхронизации.
22. 20. Возможности и примеры построения радиоприемников приема сложных сигналов с фазовой манипуляцией. Построение устройств обработки сигналов на регистрах сдвига (цифровые корреляторы и согласованные фильтры). Использование ПАВ устройств (согласованные фильтры и конвольверы). Проблемы синхронизации.
23. Методы защиты от утечки информации через закладные устройства, использующие радиоканал, и ПЭМИ. Экранирование. Эффективность экранирования высокочастотного электромагнитного излучения сплошным металлическим экраном. Влияние щелей и отверстий. Эффективность экранирования сетчатым экраном.
24. Активные методы защиты. Эффективность зашумления широкополосным шумовым излучением. Эффективность зашумления ультразвуком.
25. Организованные каналы утечки (съема) информации – закладные устройства. Закладные устройства с проводными каналами передачи. Использование проводов сети 220 В и других проводных линий. Закладные устройства с радиоканалом. Диапазоны частот, мощность передатчиков, виды модуляции, виды сигналов, используемые в закладных устройствах.
26. Определение количественных характеристик цепей паразитных связей. Паразитные емкостная, индуктивная связи. Определение уровней наводок через паразитную емкость между приборами и проводниками. Определение уровней наводок за счет контуров с током (взаимной индуктивности). Излучение случайных антенн – электрических и магнитных диполей.
27. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Магнитные экраны на низких частотах. Магнитные экраны на высокой частоте. Поверхностный эффект и токи Фуко. Соотношения и количественные показатели степени экранирования электростатических и магнитных экранов.
28. Борьба с утечкой информации по техническим каналам. Методы обнаружения утечки информации за счет побочных излучений и излучений закладных устройств. Широкополосные индикаторы напряженности поля. Проблемы их применения. Сканирующие узкополосные приемники. Требования к характеристикам. Тактика применения. Проблемы использования.

29. Защита информации от утечки в телефонных каналах связи. Каналы утечки информации: прямой перехват переговоров путем подключения к телефонной линии; утечка информации по линии при положенной трубке за счет микрофонного эффекта и других акустоэлектрических преобразований; перехват информации при помощи закладных устройств (типы и способы подключения); перехват информации за счет высокочастотного навязывания. Методы борьбы с утечкой информации. Зашумление телефонной линии. Виды и способы зашумления.
30. Побочные электромагнитные излучения радиоэлектронных средств. Излучения гетеродинов радиоприемников. Излучения элементов компьютеров. Методика и аппаратура контроля уровня побочных излучений. Методика определения информативности побочных излучений.
31. Основные методы защиты информации техническими средствами. Охрана источников информации. Скрытие достоверной информации. Дезинформирование.
32. Методы локализации и обнаружения закладных устройств. Акустическое зондирование и определение дальности до закладного устройства. Корреляционная обработки акустических сигналов для локализации закладных устройств. Анализ уровня высших гармоник в излучении закладных устройств.
33. Нелинейные локаторы. Принцип действия. Проблемы применения.
34. Методика и аппаратура для измерения уровней наведенных сигналов из одних проводных линий в другие. Оценка (измерение) наведенных напряжений и токов в проводных линиях от электронных приборов (основных средств обработки конфиденциальной информации).
35. Методика и аппаратура наблюдения за радио излучениями в эфире с целью выявления каналов утечки информации за счет ПЭМИН и закладных устройств (мониторинг эфира). Требования к аппаратуре наблюдения. Обоснование возможности выявления каналов утечки информации. Характеристика возможностей поисковой программы «Филин».
36. Методика и аппаратура для измерения характеристик канала передачи сигналов по проводам сети 220 В. Проблемы, возникающие при использовании данного канала для передачи данных.
37. Методика измерения характеристик излучения проводных линий при помощи прибора ST 031P «Пирания». Приборы, необходимые для измерений. Сравнительные характеристики излучения проводных линий различных конструкций.
38. Методика измерения уровней излучения приборов и элементов приборов (например, печатных плат). Аппаратура, необходимая для проведения этих измерений.
39. Методика обнаружения и измерения уровней информативных паразитных излучений компьютеров. Методика оценки радиуса R2 (минимального расстояния до компьютера, на котором отношение сигнал/шум не превышает заданной величины). Аппаратура, с помощью которой можно сделать такие измерения.
40. Методика оценки эффективности зашумления паразитных излучений компьютера и зашумления излучения закладного устройства с радиоканалом. Аппаратура, необходимая для проведения измерений.
41. Методика определения мощности излучения закладных устройств и других источников. Экспериментальное определение дальности обнаружения излучения закладного устройства.
42. Поиск, локализация и обнаружение закладных устройств при помощи широкополосного индикатора напряженности поля «Пирания». Причины, ограничивающие возможности данного прибора. Пути его совершенствования.
43. Методика и аппаратура для наблюдения и измерения характеристик канала утечки информации за счет акусто-электрического преобразования в электронной

аппаратуре. Измерение паразитной частотной модуляции, возникающей в генераторе сигналов.

44. Методика и аппаратура для оценки эффективности зашумления закладного устройства, включенного в телефонную линию, при использовании прибора КТЛ 400.
45. Характеристика методов обнаружения закладных устройств, включенных в телефонную линию, реализованных в приборе КТЛ 400 и других методов. Характеристика проблем, возникающих при решении данной задачи.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОПЕРАЦИОННЫЕ СИСТЕМЫ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Администрирование и безопасность операционных систем*	Код модуля № 1138284 (в справочнике модулей ЕТСУ) УП №№ 5433, в. 4, № 6323, в. 4
Образовательная программа ***Информационная безопасность телекоммуникационных систем***	**Код ОП** 10.05.02/01.01
Направление подготовки ***Информационная безопасность***	**Код направления и уровня подготовки** ***10.05.02.***
Уровень подготовки ***Специалитет***	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: ***№1426 16 ноября 2016 г***

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Авдеев Денис Викторович	-	Старший преподаватель	Радиоэлектроники и связи	

Руководитель модуля Н.С. Виноградова

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Председатель учебно-методического совета В.Г. Коберниченко
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ОПЕРАЦИОННЫЕ СИСТЕМЫ»

1.1.Аннотация содержания дисциплины

Изучаются основополагающие принципы построения и функционирования операционных систем. Подробно рассматривается архитектура современных операционных систем, назначение основных подсистем. При изучении внимание уделяется вопросам безопасности операционных систем, принципам построения пользовательского интерфейса.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- ПСК-10.5 - способность проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи;
- ПКД-6 - способность обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи;
- ПКД-9 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищённые операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПКД-10 - способность разрабатывать и анализировать модели угроз, обеспечивать защищенность и стабильность функционирования файловых систем, а также реализовывать процесс восстановления информации в случае повреждения их целостности.

В результате освоения дисциплины студент должен:

Знать:

- угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии;
- основные принципы защиты компьютерной информации в операционных системах;
- виды и стратегии резервирования информации;
- механизмы защиты информации от несанкционированного доступа, встроенные в операционные системы Windows и Linux;
- основные принципы администрирования операционных систем.

Уметь:

- выполнять функции администратора операционных систем;
- осуществлять планирование и создание учетных записей пользователей и рабочих групп, выполнять разграничение доступа к ресурсам компьютерных систем средствами ОС;
- производить основные настройки операционных систем, обеспечивающие требуемый уровень безопасности компьютерной информации;
- настраивать политику аудита, анализировать события, регистрируемые в журнальных файлах;
- настраивать сетевую инфраструктуру распространенных операционных систем.

Владеть (демонстрировать навыки и опыт деятельности):

- методикой сбора информации о сетевом трафике, и анализа с целью оптимизации и обеспечения безопасности компьютерной сети;
- навыками управления сетевыми узлами с помощью средств системных служб и протокола SNMP;

– навыками использования стандартных сетевых утилит операционных систем с целью диагностики и поиска неисправностей в сети.

1.4. Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)	
		Всего часов	**В т.ч. контактная работа (час.)***	*6*	*7*
1.	**Аудиторные занятия**	51	51	34	17
2.	Лекции	17	17	17	
3.	Практические занятия				
4.	Лабораторные работы	34	34	17	17
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	57	7,65	38	19
6.	**Промежуточная аттестация**	3,3	0,5	3	3
7.	**Общий объем по учебному плану, час.**	108	59,15	72	36
8.	**Общий объем по учебному плану, з.е.**	3		2	1

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Общие принципы безопасности операционных систем**	Ключевые элементы программной архитектуры операционных систем. Защищенные файловые системы. Модель безопасности и ее архитектура. Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС. Безопасность системных данных. Способы защиты системных файлов от незаконной модификации. Управление памятью. Механизмы виртуальной памяти. Создание и уничтожение процессов. Аудит событий безопасности.
2	**Защита компьютерной информации в операционных системах Linux**	Файл как универсальный объект ОС. Загрузчики операционных систем. Архитектура файловых систем. Атрибуты процесса. Использование возможностей командных оболочек при решении штатных задач администрирования. Пользователи и их виды. Копирование и запись данных. Архивация и резервирование. Сетевые возможности операционных систем. Наблюдение и аудит в ОС Linux. Основные ошибки и просчеты в администрировании компьютерных сетей под управлением операционных систем Linux. Анализ настроек безопасности UNIX-систем.
3	**Защита компьютерной информации в операционных системах семейства Windows**	Реализация технологии разграничения доступа в ОС Windows. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows. Разграничение доступа в ОС Windows. Структура системного реестра ОС Windows. Редактирование реестра. Анализ и настройка политики безопасности. Аудит событий безопасности. Анализ сетевых служб Windows. Использование инструментальных средств аудита безопасности компьютерных систем.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 6
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*				
1	Общие принципы безопасности операционных систем	**4**	**3**	3			**1**	**1**	1																		Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
2	Защита компьютерной информации в операционных системах Linux	**49**	**24**	7		17	**25**	**9**	3		6		**16**	1				1												
3	Защита компьютерной информации в операционных системах семейства Windows	**47**	**24**	7		17	**23**	**8**	3		5		**15**	1				1												
	Всего (час), без учета промежуточной аттестации:	**100**	**51**	**17**		**34**	**49**	**18**	**7**		**11**		**31**	**15**				**16**												
	Всего по дисциплине (час.):	**108**	**51**				**53**	В т.ч. промежуточная аттестация																			**8**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Исследование файловых объектов с правами пользователя	3
2	2	Реализация политики разграничения доступа средствами ОС Linux	2
2	3	Исследование процессов в ОС Linux	3
2	4	Исследование сетевых возможностей ОС Linux	3
2	5	Исследование беспроводной сети WiFi под управлением ОС Linux	3
2	6	Наблюдение и аудит в ОС Linux	3
3	7	Основы администрирования ОС Windows	4
3	8	Использование реестра для настройки параметров ОС Windows	4
3	9	Настройка политики безопасности ОС Windows. Аудит событий безопасности	3
3	10	Применение стандартных механизмов защиты ОС Windows	3
3	11	Применение механизма защиты шифрования файлов в ОС Windows с использованием шифрующей файловой системы EFS. Применение механизма защиты BitLocker.	3
		Всего:	**34**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Обеспечение безопасности при удаленном доступе.*
- *Сокрытие процессов.*
- *Настройка адекватной политики аудита.*
- *Разделение функций администратора и аудитора.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

- *Перехват и анализ сетевого трафика с помощью утилиты tcpdump.*
- *Создание замкнутой программной среды с помощью функции AppLocker.*

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

Не предусмотрено

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Общие принципы безопасности операционных систем				*								
2.Защита компьютерной информации в операционных системах Linux					*			*				
3.Защита компьютерной информации в операционных системах семейства Windows				*				*				

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

9.1.1.Основная литература

1. Синицын С. В. Операционные системы : учебник для вузов / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин .— 3-е изд., стер. — Москва : Издательский центр "Академия", 2013 .— 296 с.
2. Робачевский А.М. Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский .— Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002 .— 514 с. 12 экз.

9.1.2.Дополнительная литература

1. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007 .— 136 с. 90 экз.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.
3. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с. 10 экз.

9.2.Методические разработки

1. Доросинский Л.Г., Зверева О.М. Операционные системы. УМК, 2007. Метаданные ресурса №6818

9.3.Программное обеспечение

ОС Linux, Windows

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

СЕМЕСТР VI

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа	*6,1-7*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,4		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение лабораторных работ	*6,1-15*	*80*
Расчетная работа	*6,1-7*	*20*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

СЕМЕСТР VII

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0		
Промежуточная аттестация по лекциям – 0 **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –1		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа	*7,1-7*	*20*
Расчетная работа	*7,1-7*	*20*
Выполнение лабораторных работ	*7,1-15*	*60*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0,4		
Промежуточная аттестация по лабораторным занятиям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0,6**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

1. Unix-подобные системы. ОС Linux.
2. Состав файла. Открытие файла в Unix-подобной системе.
3. Пользователи в Unix-подобной системе. Распределение идентификаторов пользователей. Суперпользователь.
4. Виды доступа в Unix-подобной системе. Особенности прав доступа к файлам и каталогам.
5. Категории пользователей по отношению к файлу в Unix-подобной системе. Варианты записи прав доступа.
6. Эффективные права в Unix-подобной системе. Маска доступа. Аттрибуты файловых систем ext*fs.
7. Жёсткие ссылки в Unix-подобной системе. Символические ссылки.
8. Группы пользователей в Unix-подобной системе. Создание группы. Хранение конфигурации.
9. Управление группами пользователей в Unix-подобной системе. Получение сведений о группах пользователя.
10. Хранение сведений о пользователе в Unix-подобной системе.
11. Механизм sudo в Unix-подобной системе. Хранение конфигурации.
12. Загрузка ОС Linux. Регистрация пользователей.
13. Управление процессами ОС. Виды процессов. Режимы процессов.
14. Идентификаторы процесса в Unix-подобной системе. Приоритет.
15. Наблюдение за процессами в Unix-подобной системе. Переменные окружения. Файловая система /proc.
16. Доступность ресурсов в Unix-подобной системе. Атаки на доступность. Управление службами.

17. Уровень выполнения в ОС Linux. Запуск по расписанию в Unix-подобной системе.
18. Командная оболочка в Unix-подобной системе. Завершение работы в системе.
19. Межпроцессное взаимодействие в Unix-подобной системе. Сигналы. Перенаправление потока. Каналы.
20. Терминальный режим в Unix-подобной системе. Обмен сообщениями.
21. Конфигурация сетевого интерфейса в Unix-подобной системе.
22. Использование протоколов ARP и ICMP в Unix-подобной системе.
23. Исследование сетевого окружения в Unix-подобной системе. Утилиты nmap, tcpdump и aircrack-ng.
24. Конфигурация безпроводного сетевого интерфейса в Unix-подобной системе. Виртуальные интерфейсы.
25. Аудит в Unix-подобной системе: системные журналы и управление протоколированием.
26. Аудит в Unix-подобной системе: уровни значимости и защита системы аудита.
27. Устройства в Unix-подобной системе. Защита устройств. Виртуальные устройства.
28. Монтирование в Unix-подобной системе. Хранение конфигурации.
29. Объекты доступа в ОС Windows. Субъекты доступа.
30. Стандартные и специфичные методы доступа в ОС Windows.
31. Список доступа в ОС Windows. Структура файла в файловой системе NTFS.
32. Идентификатор пользователя в ОС Windows. Взаимодействие с дескриптором защиты.
33. Контроль доступа в ОС Windows. Использование записей контроля доступа и маркеров доступа. Наследование разрешений.
34. Проверка подлинности при входе пользователя в ОС Windows.
35. Индивидуальные разрешения NTFS.
36. Стандартные разрешения NTFS для файлов и папок. Связь с индивидуальными разрешениями.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено