Приложение
к рабочей программе модуля (дисциплины)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Код модуля	Модуль
1156866	*Безопасность операционных систем*

Екатеринбург, 2021

Оценочные материалы по модулю составлены авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*
3	Макарова Ольга Сергеевна	-	Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. СТРУКТУРА И ОБЪЕМ МОДУЛЯ *Безопасность операционных систем*

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1	Обеспечение безопасности операционных систем	*4 з.е./144 ч.*	*экзамен*
2	Операционные системы	*3 з.е./108 ч.*	*зачет*
	ИТОГО по модулю:	*7 з.е./252 ч.*	

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО МОДУЛЮ

2.1. Проект по модулю

Не предусмотрено

2.2. Интегрированный экзамен по модулю

Не предусмотрено

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 1

Модуль *Безопасность операционных систем*

Дисциплина Обеспечение безопасности операционных систем

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ *Безопасность операционных систем*

Таблица 1

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
1	**2**
– 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*	*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* *4* *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;*

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.*	*– 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.*

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

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 иняз. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Общие принципы безопасности операционных систем		**9**	4		5	6	3	1		2												3	1					
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**

2.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

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**

3. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

3.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

<table>
<tr><th colspan="4">Характеристика уровней достижения результатов обучения (индикаторов)</th></tr>
<tr><th rowspan="2">№ п/п</th><th rowspan="2">Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)</th><th colspan="2">Шкала оценивания</th></tr>
<tr><th colspan="2">Традиционная характеристика уровня</th><th>Качественная характеристика уровня</th></tr>
<tr><td>1.</td><td>Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет</td><td>Отлично (80-100 баллов)</td><td rowspan="2">Зачтено</td><td>Высокий (В)</td></tr>
<tr><td>2.</td><td>Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения</td><td>Хорошо (60-79 баллов)</td><td>Средний (С)</td></tr>
</table>

3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

4. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Спецификация теста в системе ОК УрФУ:

Для проведения промежуточной аттестации используется ОК УрФУ.

Структура тестовых материалов при использовании ОК УрФУ: Тест включает в себя 40 заданий, время выполнения – 60 минут. В структуре теста представлены вопросы по всем разделам изучения дисциплины.

4.1 Примерный перечень контрольных вопросов для подготовки к аттестации по дисциплине

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.

Раздел 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 2

Модуль *Безопасность операционных систем*

Дисциплина Операционные системы

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ *Операционные системы*

Таблица 6

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
1	**2**
– 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*

5. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

5.1. Распределение объема времени по видам учебной работы

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 иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Общие принципы безопасности операционных систем	**4**	**3**	3			**1**	**1**	1																					
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**

5.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 8

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**

6. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-

оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 9

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

3.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 10

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)

5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания	Нет результата

7. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Спецификация теста в системе ОК УрФУ:

Для проведения промежуточной аттестации используется ОК УрФУ.

Структура тестовых материалов при использовании ОК УрФУ: Тест включает в себя 40 заданий, время выполнения – 60 минут. В структуре теста представлены вопросы по всем разделам изучения дисциплины.

Примерный перечень контрольных вопросов для подготовки к аттестации по дисциплине

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.