Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

ЗАЩИТА ОПЕРАЦИОННЫХ СИСТЕМ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»
_____ **Бурлов В.Г.**

Утверждаю
Председатель УМС _____ **И.И. Палкин**

Рекомендована решением
Учебно-методического совета
«11» июня 2019 г., протокол № 7

Рассмотрена и утверждена на заседании кафедры
«07» мая 2019 г., протокол № 5
Зав. кафедрой _____ **Завгородний В.Н.**

Авторы-разработчики:
_____ **Грызунов В.В.**

Санкт-Петербург, 2019

1. Цели освоения дисциплины

Целью освоения дисциплины «Защита операционных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий построения защищенных операционных систем, а также средств и методов обеспечения защиты информации в операционных системах.

Основные задачи дисциплины:

– изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности операционных систем;

– изучение средств и методов управления доступом в защищенных операционных системах;

– изучение средств и методов аутентификации пользователей в защищенных операционных системах;

– изучение средств и методов реализации аудита в защищенных операционных системах;

– изучение средств и методов интеграции защищенных операционных систем в защищенную сеть.

– формирование у студентов комплекса научных знаний о теоретических основах работы современных операционных систем и компьютерных сетей.

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита операционных систем» для направление подготовки 10.05.02 – Информационная безопасность телекоммуникационных систем по защите информации относится к вариативным дисциплинам Блока 1 Дисциплины (Модули) и является предметом по выбору Б1.В.ДВ.03.01

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика и программирование»,

«Операционные системы»,

«Основы информационной безопасности»,

«Информационные технологии».

Дисциплина «Защита операционных систем» является предшествующей для изучения следующих дисциплин: "Основы проектирования защищенных ТКС", "Сети и системы передачи данных", "Программно-аппаратные средства обеспечения ИБ".

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОК-8	способностью к самоорганизации и самообразованию
ОПК-5	способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач
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

В результате освоения компетенций в рамках дисциплины «Защита операционных систем» обучающийся должен:

Код компетенции	Результаты обучения
ОК-8	Знать − модели нарушителя и сферы их применения; − протоколы авторизации в ОС; − основные средства защиты сетевых и распределённых ОС; Уметь: − распознать существующие уязвимости в ОС; − сопоставить возможности существующих средств защиты информации (СЗИ) и возможности средств информационно-технических вторжений; − применить на практике основные существующие СЗИ; Владеть навыками: − организовать свою работу как специалиста в области информационной безопасности; − составить актуальную модель нарушителя безопасности ОС; − сформулировать цели информационной безопасности компании
ОПК-5	Знать − механизм функционирования виртуальных машин; − особенности защиты информации при использовании облачных вычислений; − типы кластеров; − контексты применения технологий разделения памяти Уметь: − применить на практике основные существующие СЗИ; − исследовать текущий уровень защиты ОС; − решить задачи по предоставлению защищённого удалённого доступа в ОС; Владеть навыками: − предположить последствия применения вновь возникающих средств ведения информационно-технических воздействий к ОС; − компоновать доступные СЗИ в единую систему, оптимальную для отражения представленной модели нарушителя
ПК-14	Знать − механизм функционирования виртуальных машин; − особенности защиты информации при использовании облачных

	вычислений; − контексты применения технологий разделения памяти; − виды резервного копирования; − подходы к балансировке нагрузки на ИВС; Уметь: − применить на практике основные существующие СЗИ; − исследовать текущий уровень защиты ОС; − решить задачи по предоставлению защищённого удалённого доступа в ОС; Владеть навыками: − предположить последствия применения вновь возникающих средств ведения информационно-технических воздействий к ОС; − компоновать доступные СЗИ в единую систему, оптимальную для отражения представленной модели нарушителя;
ПК-15	Знать − модели нарушителя и сферы их применения; − технологические и нетехнологические методы воздействия на персонал, эксплуатирующий средства вычислительной техники; − возможных рисках и инцидентах информационной безопасности; − алгоритм расчёта экономической эффективности систем защиты информации. Уметь: − решить задачи по предоставлению защищённого удалённого доступа в ОС; − разработать план резервного копирования данных; − оценить экономическую эффективность СЗИ; Владеть навыками: − наладить инструментальный мониторинг безопасности ОС; сформулировать цели информационной безопасности компании

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Защита операционных систем» сведены в таблице.

Уровень освоения компетенции	**Результат обучения**	**Результат обучения**	**Результат обучения**	**Результат обучения**
	ОК-8: Знать, уметь, владеть	ОПК-5: Знать, уметь, владеть	ОПК-14: Знать, уметь, владеть	ПК-15: Знать, уметь, владеть
минимальный	слабо ориентируется в терминологии и содержании	слабо ориентируется в терминологии и содержании	слабо ориентируется в терминологии и содержании	слабо ориентируется в терминологии и содержании
	не выделяет основные идеи	не выделяет основные идеи	не выделяет основные идеи	не выделяет основные идеи
	допускает грубые ошибки	допускает грубые ошибки	допускает грубые ошибки	допускает грубые ошибки
базовый	Способен выделить основные идеи текста, работает с критической литературой	Способен выделить основные идеи текста, работает с критической литературой	Способен выделить основные идеи текста, работает с критической литературой	Способен выделить основные идеи текста, работает с критической литературой
	Способен показать основную идею в развитии	Способен показать основную идею в развитии	Способен показать основную идею в развитии	Способен показать основную идею в развитии
	Знает основные рабочие категории,	Знает основные рабочие категории,	Знает основные рабочие категории,	Знает основные рабочие категории,

	однако не ориентируется в их специфике	однако не ориентируется в их специфике	однако не ориентируется в их специфике	однако не ориентируется в их специфике
продвинутый	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению
	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа
	Может дать критический анализ современным проблемам в заданной области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 8 зачетных единицы, 288 часов.

Объем дисциплины (*модуля*) *по видам учебных занятий в академических часах*)

Объём дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоёмкость дисциплины	**288**
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	**98**
в том числе:	
лекции	**42**
Практические занятия	**56**
семинарские занятия	
Самостоятельная работа (СРС) – всего:	**190**
в том числе:	
курсовая работа	
контрольная работа	
Вид промежуточной аттестации (зачет/экзамен)	**экзамен**

4.1. Структура дисциплины

Очная форма обучения

№ п/п	**Раздел и тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Занятия в активной и интерактивной форме, час.**	**Формируемые компетенции**
			Лекции	**Лаборат.**	**Самост. работа**			
1	Введение. Иерархическая модель ИВС. Общие подходы к обеспечению ИБ ОС	**9**	2	-	10	Кейс-задача.	2/2	ОК-8, ОПК-5, ПК-14, ПК-15
2	Модели нарушителя	**9**	4	4	12	Кейс-задача.	8/4	ОК-8, ОПК-5, ПК-14, ПК-15
3	Модели безопасности	**9**	4	4	14	Кейс-задача.	8/4	ОК-8, ОПК-5, ПК-14, ПК-15
4	Криптографические методы защиты ОС	**9**	4	4	14	Кейс-задача.	8/4	ОК-8, ОПК-5, ПК-14, ПК-15
5	Авторизация в ОС	**9**	4	6	12	Кейс-задача.	10/4	ОК-8, ОПК-5, ПК-14, ПК-15
6	Средства защиты сетевых и распределённых ОС	**9**	6	6	14	Кейс-задача.	12/6	ОК-8, ОПК-5, ПК-14, ПК-15
7	Удалённый доступ к ОС	**9**	4	4	12	Кейс-задача.	8/4	ОК-8, ОПК-5, ПК-14, ПК-15

8	Журналирование событий безопасности	**А**	1	2	10	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
9	Защита виртуальных машин, супервизоров и гипервизоров	**А**	1	2	10	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
10	Защита облачных вычислений	**А**	1	2	8	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
11	Кластеры	**А**	1	4	10	Кейс-задача.	5/2	ОК-8, ОПК-5, ПК-14, ПК-15
12	Разделение памяти	**А**	1	2	10	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
13	Системы хранения данных	**А**	2	2	8	Кейс-задача.	4/2	ОК-8, ОПК-5, ПК-14, ПК-15
14	Системы резервного копирования	**А**	1	2	10	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
15	Методы балансировки нагрузки	**А**	1	2	10	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
16	Особенности защиты мобильных ОС	**А**	1	2	8	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
17	Защита ОС на уровне персонала	**А**	2	4	8	Кейс-задача.	6/2	ОК-8, ОПК-5, ПК-14, ПК-15
18	Система управления безопасностью ОС	**А**	1	2	8	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
19	Заключение. Обоснование трат на защиту ОС	**А**	1	2	2	Кейс-задача.	3/2	ОК-8, ОПК-5, ПК-14, ПК-15
	ИТОГО		42	56	120		98/52	

4.2. Содержание разделов дисциплины

4.2.1 Введение. иерархическая модель ИВС. Общие подходы к обеспечению ИБ ОС

Основные определения. Уровни ИВС. Компенсационная и возможностная модель защиты ОС. Терминальная и структурная модели ОС. Подходы к обнаружению атак на ОС.

4.2.2 Модели нарушителя

Дестабилизирующие факторы, воздействующие на информацию. Возможности и ограничения нарушителя. Защищаемые ресурсы.

4.2.3 Модели безопасности

Принципы построения систем безопасности ОС. Модели разграничения доступа. Политика изолированной программной среды.

4.2.4 Криптографические методы защиты ОС

Место криптографических средств в защите ОС. Инфраструктура открытых ключей.

Защита ключевых элементов ОС и данных пользователя с помощью криптографии.

4.2.5 Авторизация в ОС

Основные понятия. Методы и протоколы авторизации в ОС.

4.2.6 Средства защиты сетевых и распределённых ОС

Особенности сетевых и распределённых ОС. Firewall, VPN, VLAN, NAT.

4.2.7 Удалённый доступ к ОС

Задачи, протоколы и средства обеспечения удалённого доступа. Безопасность удалённого доступа.

4.2.8 Журналирование событий безопасности

Назначение журналирования. Противоречия, возникающие в процессе журналирования, и способы их разрешения. Дифференциальный и интегральный алгоритмы наблюдения. Паттерны информационно-технических атак и вторжений. Анализ и расследование инцидентов Протоколы и системы журналирования. DLP-системы. Honey net.

4.2.9 Защита виртуальных машин, супервизоров и гипервизоров

История виртуализации. Уровни абстракции виртуализации. Hosting. Специфика угроз в виртуальной среде.

4.2.10 Защита облачных вычислений

Основные определения. История развития. Способы доставки приложений. Стратегии перевода в облако. Cloud-based бизнес-модели. Угрозы, атаки при использовании облаков.

4.2.11 Кластеры

Понятие кластера. Типы кластеров. Особенности защиты кластеров.

4.2.12 Разделение памяти

Организация защиты ресурсов при использовании разделяемой памяти. Распределённые файловые системы и их безопасность.

4.2.13 Системы хранения данных

Центр обработки данных, система хранения данных, сеть хранения данных. Характеристики, используемые протоколы, организация защиты.

4.2.14 Системы резервного копирования

Назначение и способы применения систем резервного копирования. Методы резервного копирования. Проблемы резервного копирования и восстановления из резервных копий.

4.2.15 Методы балансировки нагрузки

Постановка задачи. Виды нагрузок. Методы и инструменты балансировки нагрузки.

4.2.16 Особенности защиты мобильных ОС

Принципы построения мобильных ОС. Защищаемые ресурсы. Особенности модели нарушителя мобильных ОС. Интеграция мобильных устройств в корпоративные сети. Политика BOYD. Enterprise Mobility Management. Virtual DLP.

4.2.17 Защита ОС на уровне персонала

Цели и методы социальной инженерии. Технологические и нетехнологические методы воздействия на персонал. Пирамида нейрологических уровней. Аналоговое маркирование. Боевые фокусы языка. Работа с пресуппозициями. Методы защиты ОС на уровне персонала.

4.2.18 Система управления безопасностью ОС

Основные термины и определения системы управления безопасностью.

Понятие риска. Оценка, оценивание и управление рисками. Понятие инцидента. Управление инцидентами. Аудит. Тестирование систем защиты по методу чёрного и белого ящика.

4.2.19 Заключение. Обоснование трат на защиту ОС

Подведение итогов. Экономическая эффективность систем защиты ОС, Защита ОС как инструмент увеличения доходности бизнеса.

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
1	1	Рассчитать время жизни антивируса	Кейс-задача 1	ОК-8, ОПК-5, ПК-14, ПК-15
2	2	Исследовать защищённость ОС	Кейс-задача 2	ОК-8, ОПК-5, ПК-14, ПК-15
3	3	Составить матрицу доступа согласно политике безопасности и настроить разграничение доступа	Кейс-задача 3	ОК-8, ОПК-5, ПК-14, ПК-15
4	4	Получить несанкционированный доступ к учётной записи суперпользователя	Кейс-задача 4	ОК-8, ОПК-5, ПК-14, ПК-15
5	4	Создать сертификат ключа проверки подлинности электронной подписи со структурой квалифицированного сертификата, организовать обмен файлами, подписанными электронной подписью и зашифрованными	Кейс-задача 5	ОК-8, ОПК-5, ПК-14, ПК-15
6	5	Настроить двухфакторную авторизацию при входе в аккаунт ОС	Кейс-задача 6	ОК-8, ОПК-5, ПК-14, ПК-15
7	6	Настроить NAT, Firewall	Кейс-задача 7	ОК-8, ОПК-5, ПК-14, ПК-15
8	6	Настроить сетевой антивирус, IDS	Кейс-задача 8	ОК-8, ОПК-5, ПК-14, ПК-15
9	7	Настроить удалённый доступ к ОС по RDP, SSH	Кейс-задача 9	ОК-8, ОПК-5, ПК-14, ПК-15
10	8, 9	Организовать контроль над деятельностью пользователей посредством DLP	Кейс-задача 10	ОК-8, ОПК-5, ПК-14, ПК-15
11	10	Создать персональное облако	Кейс-задача 11	ОК-8, ОПК-5, ПК-14, ПК-15
12	11, 12	Настроить NFS	Кейс-задача 12	ОК-8, ОПК-5, ПК-14, ПК-15
13	13	Создать программный RAID-1	Кейс-задача 13	ОК-8, ОПК-5, ПК-14, ПК-15
14	14	Составить политику резервного копирования указанных данных и реализовать её	Кейс-задача 14	ОК-8, ОПК-5, ПК-14, ПК-15
15	15, 16	Настроить OpenVPN	Кейс-задача 15	ОК-8, ОПК-5, ПК-14, ПК-15

16	17	Трансформация убеждений, заявленных участниками, с помощью инструментов социальной инженерии	Творческое задание	ОК-8, ОПК-5, ПК-14, ПК-15
17	18, 19	Оценить риски ИБ, рассчитать экономический эффект от внедрения средств защиты информации	Кейс-задача 16	ОК-8, ОПК-5, ПК-14, ПК-15

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль проводится путём проверки выполнения творческого задания, кейс-задач. Кейс-задачи представлены в ФОС.

5.2. Методические указания по организации самостоятельной работы

Во время самостоятельной работы студенты знакомятся с существующими методами и инструментами обеспечения информационной безопасности ОС, методами социальной инженерии, возможными направлениями развития СЗИ и средств информационно- технических воздействий.

В перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Защита операционных систем» входит дополнительная литература и видеофильмы для самостоятельного изучения.

5.3. Промежуточный контроль: экзамен

Перечень вопросов к экзамену

1. Иерархическая модель информационно-вычислительной системы (ИВС).
2. Компенсационный и возможностный подходы к обеспечению безопасности ИВС.
3. Терминальная модель ИВС. Целенаправленные и случайные потоки нарушения информационной безопасности (ИБ)
4. Структурная модель ИВС. Защищаемые ресурсы.
5. Пространство состояний операционной системы (ОС). Подходы к обнаружению вторжений.
6. Понятие защищённой операционной системы (ОС). Подсистемы защищённой ОС.
7. Факторы, воздействующие на информацию. Классификация.
8. Показатели эффективности средства защиты информации. Расчёт времени жизни средства защиты информации.
9. Аспекты информационной безопасности. Понятия устойчивости, безопасности, защищённости, несанкционированного доступа.
10. Закладки уровня аппаратного обеспечения.
11. Закладки уровня программного обеспечения.
12. Принципы построения систем информационной безопасности ОС.
13. Модель дискреционного доступа (DAC).
14. Модель Белла-Лападулы.
15. Ролевая модель контроля доступа (RBAC).
16. Политика изолированной программной среды.

17. Способы нарушения информационной безопасности ОС. Матрица доступа.
18. Требования к защищенности автоматизированных систем. Задачи системы информационной безопасности ОС.
19. Простая электронная подпись. Назначение, сферы применения.
20. Усиленная неквалифицированная электронная подпись. Назначение, сферы применения.
21. Усиленная квалифицированная электронная подпись. Назначение, сферы применения.
22. Сертификат ключа проверки подлинности электронной подписи. Назначение, структура, жизненный цикл.
23. Протоколы аутентификации и авторизации. HTTP authentication.
24. Протоколы аутентификации и авторизации. Forms authentication.
25. Протоколы аутентификации и авторизации. Kerberos.
26. Протоколы аутентификации и авторизации. RADIUS. TACACS.
27. Аутентификация по сертификатам.
28. Аутентификация по одноразовым паролям.
29. Аутентификация по ключам доступа.
30. Аутентификация по токенам.
31. Протоколы удалённого доступа. Возможности и ограничения.
32. Основные проблемы, возникающие при организации удалённого доступа.
33. Сетевые и распределённые ОС. Назначение, особенности применения.
34. Средства защиты сетевых и распределённых ОС. Защита от вирусов.
35. Средства защиты сетевых и распределённых ОС. NAT.
36. Средства защиты сетевых и распределённых ОС. Firewall.
37. Средства защиты сетевых и распределённых ОС. VPN.
38. Средства защиты сетевых и распределённых ОС. VLAN.
39. Средства защиты сетевых и распределённых ОС. Организация DMZ.
40. Средства защиты сетевых и распределённых ОС. IDS, IPS.
41. Системы журналирования. Назначения и задачи.
42. Системы журналирования. Дифференциальный и интегральный алгоритмы наблюдения.
43. Системы журналирования. Паттерны информационно-технических атак и вторжений.
44. Системы журналирования. Анализ и расследование инцидентов.
45. DLP-системы. Назначение, сфера применения. Возможности и ограничения.
46. Honey Net. Назначение, сфера применения.
47. Технологии виртуализации. Назначение, решаемые задачи, история возникновения.
48. Уровни абстракции виртуализации.
49. V86 и HyperThreading.
50. Супервизор и гипервизор.
51. Способы обмена данными виртуальных машин и внешних устройств.
52. Паравиртуализация и полная виртуализация.
53. Виртуализация сетей.
54. Специфика угроз в виртуальной среде и защиты виртуальных машин.

55. Облачные вычисления. Назначение, решаемые задачи, история возникновения.
56. Способы доставки приложений до пользователя.
57. Бизнес-модели использования «облаков».
58. Угрозы и безопасность при использовании «облаков».
59. Кластеры. Назначение, решаемые задачи, история возникновения.
60. Ресурсы кластеров.
61. High-Availability cluster
62. NLB clusters
63. Computation\ High Performance Computing
64. Оценивание производительности кластерных систем.
65. Системы хранения. Назначение, решаемые задачи, история возникновения.
66. Центр обработки данных (ЦОД). Назначение, решаемые задачи, типовой состав.
67. Система хранения данных (СХД). Назначение, решаемые задачи, типовой состав, свойства.
68. Производительность систем хранения.
69. Консистентность данных (data consistency).
70. Варианты подключений СХД.
71. Система хранения, подключенная к сети (Network Attached Storage, NAS).
72. Сеть хранения данных (Storage Area Network, SAN).
73. Система хранения, подключенная к серверу (Server/Direct Attached Storage, SAS/DAS).
74. Защита операционных систем на уровне персонала. Назначение, решаемые задачи, инструменты.
75. Технологические методы социальной инженерии.
76. Виды воздействия на персонал.
77. Методы изменения поведения персонала.
78. Нейрологические уровни.
79. Фокусы языка. Намерение, другой результат, последствия.
80. Фокусы языка. Разделение, объединение, аналогия.
81. Фокусы языка. Переопределение, противоположный пример, иерархия критериев, метафрейм.
82. Фокусы языка. Изменение размеров фрейма, модель мира, стратегия реальности, применение к себе.
83. Резервное копирование и архивирование данных.
84. Методы резервного копирования.
85. Системы резервного копирования и их функции.
86. Проблемы систем резервного копирования и способы их решения.
87. Особенности модели нарушителя мобильных операционных систем.
88. Угрозы мобильных операционных систем.
89. Способы защиты мобильных операционных систем.
90. Bring Your Own Device (BYOD).
91. Mobile Device Management (MDM), Mobile Application Management (MAM), Enter- prise Mobility Management (EMM).
92. Системы управления информационной безопасностью (СУИБ).

Назначение, решаемые задачи.

93. Понятие риска. Оценка и оценивание риска. Факторы риска. Подходы к управлению рисками.
94. Управление инцидентами информационной безопасности (ИБ).
95. Типы тестирования ИБ. Аудит ИБ.

Примеры билетов

Кафедра Информационных технологий и систем безопасности
Дисциплина Защита операционных систем
Экзаменационный билет № 1

1) Закладки уровня программного обеспечения.
2) Фокусы языка. Намерение, другой результат, последствия.

Заведующий кафедрой_____/_____/

Кафедра Информационных технологий и систем безопасности
Дисциплина Защита операционных систем
Экзаменационный билет № 2

1) Honey Net. Назначение, сфера применения.
2) Особенности модели нарушителя мобильных операционных систем.

Заведующий кафедрой_____/_____/

Критерии выставления оценки:

- оценка «отлично»: экзаменуемый демонстрирует глубокие, исчерпывающие знания в объеме программы дисциплины, правильные уверенные действия по применению полученных знаний на практике, грамотное, логичное изложение материала при ответе;
- оценка «хорошо»: наличие твердых и достаточно полных знаний в объеме программы дисциплины, незначительные ошибки при освещении вопросов, правильные действия по применению полученных знаний на практике, четкое изложение материала при ответе;
- оценка «удовлетворительно»: наличие твердых знаний в объеме программы дисциплины, изложение ответов с ошибками, уверенно исправленными после дополнительных вопросов, необходимость в наводящих вопросах экзаменуемому, правильные действия по применению знаний на практике;
- оценка «неудовлетворительно»: при наличии грубых ошибок в ответах, непонимание сущности излагаемых вопросов, неумении применять знания на практике, неуверенности и неточности в ответах на дополнительные и наводящие вопросы.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Защита в операционных системах: Учебное пособие для вузов / В.Г. Проскурин. - М.: Гор. линия-Телеком, 2014. - 192 с.: ил.; 60x88 1/16. -

(Специальность). ISBN 978-5-9912-0379-1
2. Гостев, И. М. Операционные системы: учебник и практикум для академического бакалавриата / И. М. Гостев. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2018. — 164 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-04520-8. — Режим доступа: www.biblio-online.ru/book/A14759F4-CD1C-441C-A929-64B9D29C6010.
3. Бабернов В. Системы резервного копирования.
4. Девянин П.Н. Модели безопасности компьютерных систем: Уч. пособие для студентов ВУЗов. — М.: Академия, 2005.
5. Котяшичев И. А., Бырылова Е. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. — 2015. — №6.4. — С. 30-34.

б) дополнительная литература:

1. Пелехатый М. М., Чекчурин Ю. А. Сертификационный курс НЛП-Практик, — М.: Твои книги, 2014. — 272 с.
2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
3. Грызунов В.В. Аналитическая модель целостной информационной системы // Доклады ТУСУР. – 2009. – № 1(19), ч.1. – С.226-230.
4. Руководящий документ Гостехкомиссии «Защита от НСД. Термины и определения».

в) программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

- windows 7
- office 2007
- dr Web
- Oracle VM VirtualBox GNU General Public License
- Ub-untu 17 GNU GPLv3
- OpenVAS GNU General Public License
- Wireshark GNU General Public License
- OpenVPN GNU General Public License

Интернет-ресурсы

- 10 самых мощных суперкомпьютеров мира. https://naked-science.ru/article/top/10-fastest-supercomputers
- 5 мифов о безопасности BYOD. http://www.devicelock.com/ru/articles/detail.html?ID=2558
- BYOD риски и преимущества. https://habrahabr.ru/sandbox/57695/
- NDMP – что это, и как использовать? http://blog.aboutnetapp.ru/archives/518
- SMB Multichannel в Windows Server 2012. https://habrahabr.ru/company/microsoft/blog/151451/
- Анализ современных технологий виртуализации. https://habrahabr.ru/company/centosadmin/blog/212985/

- Введение в Microsoft Cluster Service (MSCS) семейства Windows Server 2003. http://www.ishodniki.ru/art/art_progr/net/466.html
- Введение в облачные вычисления. http://www.intuit.ru/studies/courses/673/529/lecture/11917
- Глава 5. Технологии резервного копирования и восстановления данных. http://www.razlib.ru/kompyutery_i_internet/servernye_tehnologii_hranenija_dannyh_v_srede_windows_2000_windows_server_2003/p9.php
- Грызунов В.В. Определение наиболее важного узла в сети // Информост. - 2003. №2.- С. 58-59. http://www.rit.informost.ru/rit/2-2003/58.pdf
- Защита в виртуальной среде: чеклист угроз. https://habrahabr.ru/company/croc/blog/140044/
- Как защищать данные на мобильных сотрудников https://habrahabr.ru/company/croc/blog/199468/
- Как оценить риски информационной безопасности. http://www.jetinfo.ru/author/andrej-zakharov/risk-delo-popravimoe.
- Кластерные технологии СУБД Oracle. https://novinteh.com/nvt/misc/Oracle/RAC.pdf
- Новый поворот. https://www.osp.ru/pcworld/2012/07/13016652/
- Обзор систем резервного копирования и восстановления данных на мировом и российских рынках. https://www.anti-malware.ru/analytics/Technology_Analysis/Backup_systems
- Обзор систем хранения данных. https://www.olly.ru/node/135.
- Обзор способов и протоколов аутентификации в веб-приложениях. https://habrahabr.ru/company/dataart/blog/262817/
- Подходы к обеспечению безопасности в концепции BYOD https://www.anti-malware.ru/analytics/Technology_Analysis/BYOD_Security
- Построение процесса управления инцидентами. http://www.journal.ib-bank.ru/post/217
- Построение СУИБ: С чего начать? https://habrahabr.ru/post/233315/
- Работа с инцидентами информационной безопасности. https://habrahabr.ru/post/154405/
- Реализация мультипроцессорных кластеров высокой доступности (HACMP). http://www.intuit.ru/studies/professional_skill_improvements/2004/info
- Решения Microsoft для виртуализации ИТ-инфраструктуры предприятий. http://www.intuit.ru/studies/courses/2324/624/info
- Системы хранения данных: как выбирать?! https://habrahabr.ru/company/parallels/blog/239381/
- Собери сам: как мы сделали хранилище Amazon-style для небольших хостеров. https://habrahabr.ru/company/parallels/blog/162381/

- Специфические угрозы в виртуальных средах. http://www.jetinfo.ru/jetinfo_arhiv/zaschita-virtualnykh-sred/spetsificheskie-ugrozy-v-virtualnykh-sredakh/2012
- Способы защиты мобильных устройств http://www.trn.ua/articles/7488/
- Технологии аппаратной виртуализации. http://www.ixbt.com/cm/virtualization-h.shtml
- Технологии и средства хранения и обработки данных. http://www.kp.ru/guide/sistemy-khranenija-dannykh.html
- Технологии построения и использования кластерных систем. http://www.intuit.ru/studies/courses/542/398/info

Информационно-справочные системы:

- https://biblio-online.ru – ЭБС Юрайт
- http://znanium.com – ЭБС Знаниум
- http://www.prospektnauki.ru – ЭБС Проспект науки
- http://elib.rshu.ru ЭБС ГидроМетеоОнлайн
- https://нэб.рф - Национальная электронная библиотека

Профессиональные базы данных

- База данных Web of Science
- База данных Scopus
- Электронно-библиотечная система elibrary

7. Методические указания для обучающихся по освоению дисциплины

Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практические и семинарские занятия	Закрепление знаний на практике. Уяснить задачу на занятие, поставленную преподавателем, активно принимать участие в её решении. При возникновении трудностей сначала попытаться решить с другими студентами, в случае неуспеха, обратиться к преподавателю
Самостоятельная работа	Изучение конспекта лекций, дополнительной литературы. Акцент делать на вопросы, не вошедшие в конспект лекций, на контекст применения изучаемого материала
Подготовка к зачёту	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.
Текущий контроль	Проверка текущего уровня усвоения материала. Точно и в срок выполнять практические задания

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень

программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Введение. Иерархическая модель ИВС. Общие подходы к обеспечению ИБ ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Модели нарушителя	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Модели безопасности	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Криптографические методы защиты ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web

	рационального воздействия; сочетание индивидуального и коллективного обучения	Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Авторизация в ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Средства защиты сетевых и распределённых ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Удалённый доступ к ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17

	коллективного обучения	OpenVAS Wireshark OpenVPN
Журналирование событий безопасности	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Защита виртуальных машин, супервизоров и гипервизоров	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Защита облачных вычислений	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Кластеры	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark

		OpenVPN
Разделение памяти	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Системы хранения данных	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Системы резервного копирования	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Методы балансировки нагрузки	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Особенности защиты	Чтение лекций с	https://biblio-online.ru

мобильных ОС	использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Защита ОС на уровне персонала	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Система управления безопасностью ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN
Заключение. Обоснование трат на защиту ОС	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Oracle VM VirtualBox Ub-untu 17 OpenVAS Wireshark OpenVPN

9. Особенности освоения ПРАКТИКИ для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Помещение для хранения и профилактического обслуживания учебного оборудования – укомплектовано специализированной мебелью для хранения оборудования и техническими средствами для его обслуживания.

Лаборатория – компьютерный класс с ЛВС связанной с интернетом и мультимедиа.