МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор-
проректор по ОД
И.Г. Гайрабеков
_____
«22» 06 2025г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки

10.03.01 *«Информационная безопасность»*

Направленность (профиль)

«*Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*»

Квалификация

Бакалавр

Год начала подготовки – 2025

Грозный – 2025

1. Цели и задачи дисциплины

Целью изучения дисциплины является ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которыми подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программам; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации.

Задача дисциплины: ознакомить студентов с тенденциями развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а также с нормативными документами и методами защиты компьютерной информации.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Основы информационной безопасности» относится к Блоку 1 части, формируемой участниками образовательных отношений учебного плана. Для изучения курса требуется освоение следующих дисциплин: «Информатика», «Теоретические основы информатики.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ОП	**Индикаторы достижения**	**Планируемые результаты обучения по дисциплине (ЗУВ)**
Общепрофессиональные		
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1. Знать: роль информации в современном обществе, основы информационных технологий и информационной безопасности. ОПК-1.2. Уметь: применять информационные технологии и основы информационной безопасности для обеспечения объективных потребностей личности, общества и государства. ОПК-1.3. Владеть навыками использования информационных технологий и основ информационной безопасности для обеспечения	Знать: роль информации в современном обществе, основы информационных технологий и информационной безопасности. Уметь: применять информационные технологии и основы информационной безопасности для обеспечения объективных потребностей личности, общества и государства. Владеть навыками использования информационных технологий и основ информационной безопасности для обеспечения

	объективных потребностей личности, общества и государства.	объективных потребностей личности, общества и государства.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-6.1. Знать: основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.2. Уметь: организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.3.Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю .	Знать: основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Уметь: организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю .
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы	ОПК-6.1. Знать: основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.2. Уметь: организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской	Знать: основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Уметь: организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской

по техническому и экспортному контролю	Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.3. Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю .	Федерации, Федеральной службы по техническому и экспортному контролю. Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю .
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;	ОПК-2.3.1. Знать: локальные нормативные акты, стандарты информационной безопасности и меры по обеспечению безопасности объекта защиты ОПК-2.3.2. Уметь: разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты ОПК-2.3.3.Владеть: методами обеспечения безопасности объекта защиты	Знать: локальные нормативные акты, стандарты информационной безопасности и меры по обеспечению безопасности объекта защиты Уметь: разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты Владеть: методами обеспечения безопасности объекта защиты

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	**Всего часов/ зач. ед.**		**Семестры**	
			3	**3**
	ОФО	**ОЗФО**	**ОФО**	**ОЗФО**
Контактная работа (всего)	**68/1,8**	**34/0,9**	**68/1,8**	**34/0,9**
В том числе:				
Лекции	34/0,9	17/0,4	34/0,9	17/0,4
Практические занятия	-	-	-	-
Семинары	-	-	-	-
Лабораторные работы	34/0,9	17/0,4	34/0,9	17/0,4
Самостоятельная работа (всего)	**76/2,1**	**110/3,1**	**76/2,1**	**110/3,1**
В том числе:				
Курсовая работа (проект)				
ИТР				
Рефераты				
Работа над проектом	20/0,7	36/1	20/0,7	36/1
И (или) другие виды самостоятельной работы:				

Подготовка к лабораторным работам		20/0,7	38/1,1	20/0,7	38/1,1
Подготовка к практическим работам					
Подготовка к зачету		36/1	36/1	36/1	36/1
Подготовка к экзамену					
Контроль		-	-	-	-
Вид отчетности		**зачет**	**зачет**	**зачет**	**зачет**
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**144**	**144**	**144**	**144**
	ВСЕГО в зач. единицах	**4**	**4**	**4**	**4**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	**Наименование раздела дисциплины по семестрам**	**Лекц. зан. часы**		**Лаб.зан. часы**		**Всего часов**	
		ОФО	**ОЗФО**	**ОФО**	**ОЗФО**	**ОФО**	**ОЗФО**
1.	Основные понятия защиты информации и информационной безопасности	10	5	10	5	20	10
2.	Структура политики безопасности организации	10	5	10	5	20	10
3.	Основные понятия криптографической защиты информации	14	7	14	7	28	14

5.2. Лекционные занятия

Таблица 4

№ п/п	**Наименование раздела дисциплины**	**Содержание раздела**
3 семестр		
1.	Основные понятия защиты информации и информационной безопасности	Защита информации. Эффективность защиты информации. Защита информации от НСД. Система защиты информации. Санкционированный доступ к информации.
2.	Структура политики безопасности организации	Обзор политики безопасности. Базовая политика безопасности. Процедуры безопасности
3.	Основные понятия криптографической защиты информации	Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования.

5.3. Лабораторный практикум

Таблица 5

№ п/п	Наименование раздела	Наименование лабораторных работ
3 семестр		
1.	Основные понятия защиты информации и информационной безопасности	**Лабораторная работа №1.** Установка виртуальной Kali Linux
2.	Структура политики безопасности организации	**Лабораторная работа №2.** Работа в командной строке
3.	Основные понятия криптографической защиты информации	**Лабораторная работа №3.** Создание Exploit и payload **Лабораторная работа №4.** Фишинговая атака

5.4. Практические занятия (семинары) – не предусмотрены.

Таблица 6

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	**-**	**-**

6. Самостоятельная работа

Таблица 7

№№ п/п	Тематика докладов с презентациями
1	ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»
2	ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности»
3	ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3
4	ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
5	ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»
6	ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
7	ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»
8	ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий.

	Часть 1. Менеджмент сетевой безопасности»
9	ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»
10	ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»
11	Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
12	Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
13	Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
14	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
15	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
16	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
17	Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями «Оранжевой книги».
18	Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
19	Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
20	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями «Оранжевой книги».
21	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
22	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
23	Оценка защищенности ОС Windows XP Professional (NT, 2000) в соответствии со стандартами ISO.
24	Оценка защищенности ОС Linux в соответствии со стандартами ISO.
25	Сравнительный анализ антивирусных пакетов.

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. 1. Галатенко В.А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142285.html (дата обращения: 10.06.2025). — Режим доступа: для авторизир. пользователей.
2. Бондаренко И.С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137525/details (дата обращения: 10.06.2025). — Режим доступа: для авторизир. пользователей.

Бирюков А.А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 3-е изд. — Москва : ДМК Пресс, 2023. — 440 с. — ISBN 978-5-93700-219-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/159410/details (дата обращения: 10.06.2025). — Режим доступа: для авторизир. Пользователей

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

Вопросы к первой рубежной аттестации:

1. Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности
13. Процедуры безопасности

Образец билета к1-ой рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Основы информационной безопасности»
1-я рубежная аттестация
Группа: Семестр: 7
Билет №1.

Признаки классификации угроз
2. НСД к информации. Способы получения НСД

Преподаватель_____

Вопросы ко второй рубежной аттестации:

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования
4. Электронная цифровая подпись и функция хэширования
5. Аутентификация, авторизация и администрирование действий пользователей
6. Аутентификация на основе паролей
7. Угрозы безопасности ОС
8. Понятие защищенной ОС
9. Основные функции подсистемы защиты ОС
10. Разграничение доступа к объектам ОС
11. Аудит
12. Технология межсетевых экранов
13. Функции МЭ
14. Дополнительные возможности МЭ
15. Проблемы безопасности МЭ..

Образец билета ко второй рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Основы информационной безопасности»
2-я рубежная аттестация
Группа: Семестр: 7
Билет №1.

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования

Преподаватель_____

7.2. Вопросы к зачету

Основные понятия защиты информации и информационной безопасности

1. Базовые свойства информации применительно к ИБ
2. Идентификация, аутентификация, авторизация
3. Анализ угроз ИБ
4. Признаки классификации угроз
5. НСД к информации. Способы получения НСД
6. Общие критерии безопасности
7. Концепции общих критериев
8. Политика безопасности организации
9. Распределение ролей и обязанностей администраторов и пользователей сети

10. Структура политики безопасности
11. Уровни политики безопасности
12. Процедуры безопасности
13. Основные понятия криптографической защиты информации
14. Симметричные криптосистемы шифрования
15. Ассиметричные криптосистемы шифрования
16. Электронная цифровая подпись и функция хэширования
17. Аутентификация, авторизация и администрирование действий пользователей
18. Аутентификация на основе многоразовых паролей
19. Аутентификация на основе одноразовых паролей
20. Аутентификация на основе PIN-кода
21. Угрозы безопасности ОС
22. Понятие защищенной ОС
23. Основные функции подсистемы защиты ОС
24. Разграничение доступа к объектам ОС
25. Аудит
26. Технология межсетевых экранов
27. Функции МЭ
28. Дополнительные возможности МЭ

Образец билета к зачету:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Основы информационной безопасности»
Группа: Семестр: 7
Билет №1.

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования

Подпись преподавателя_____ Подпись заведующего кафедрой _____

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа №1. Установка виртуальной Kali Linux

Цель работы: Подготовка рабочей среды, ознакомление с Kali.

Теоретическая часть:

Kali Linux — это дистрибутив операционной системы Linux. Это одна из немногих систем, которая предназначена для специалистов информационной безопасности. В неё входит ряд утилит, которые созданы для тестирования уязвимостей. Kali редко используется как основная ОС, чаще всего она устанавливается как гостевая.

Система Kali Linux была разработана в 2013 году. Над ней работала команда из Offensive Security. За основу была взята структура Debian, а инструменты тестирования информационной безопасности были взяты из ОС BackTrack. Первый релиз был выпущен

13 марта 2013 года.

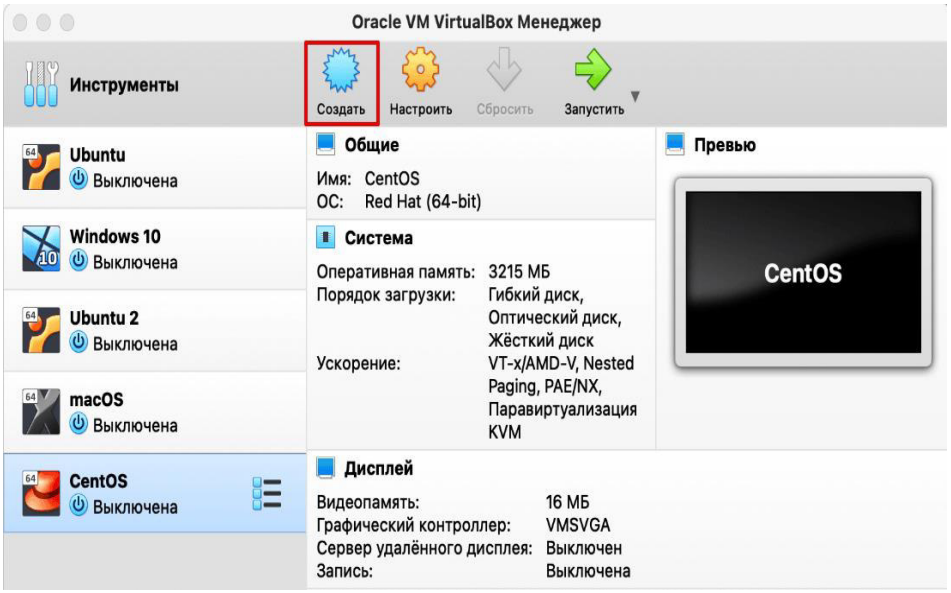
Практическая часть:

Установка Кали Линукс на виртуальную машину происходит в 3 этапа:

1. Создание виртуальной машины для Kali Linux.
2. Настройка виртуальной машины.
3. Установка ОС Kali Linux.

Этап 1. Создание виртуальной машины на VirtualBox

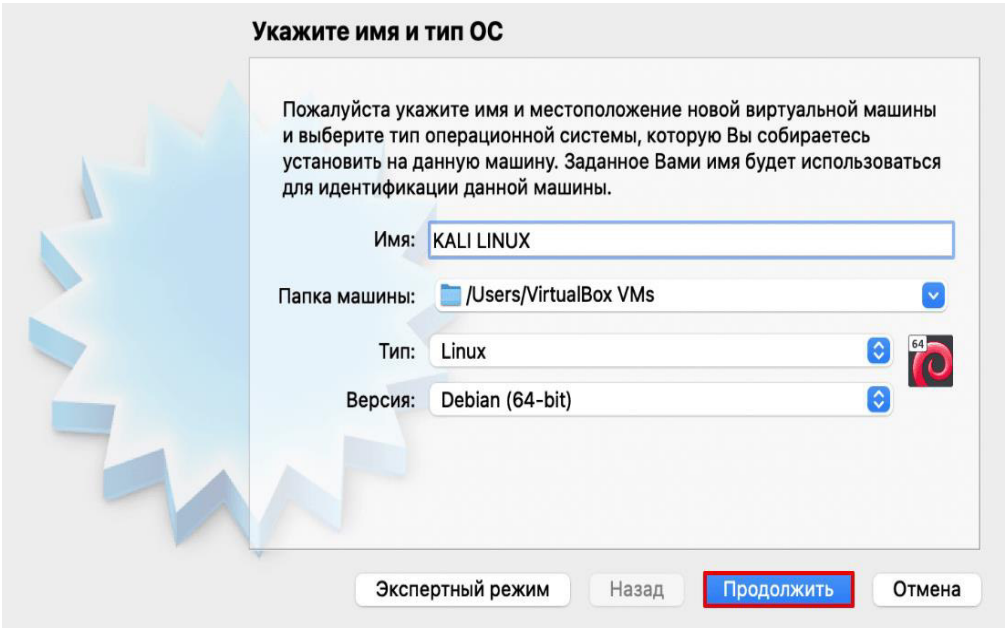
1. Скачайте ISO-образ Kali с официального сайта.
2. Запустите VirtualBox и нажмите Создать:



3. Введите имя виртуальной машины (любое).

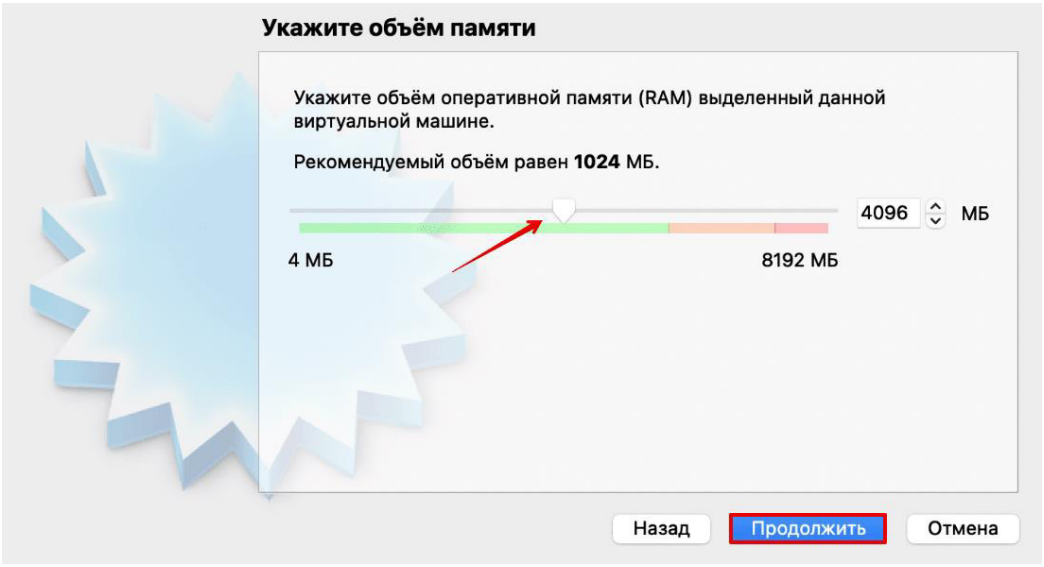
Так как Kali Linux разработана на основе Debian, в строке «Тип» выберите Linux. В строке «Версия» выберите Debian 64-bit и нажмите

Продолжить:

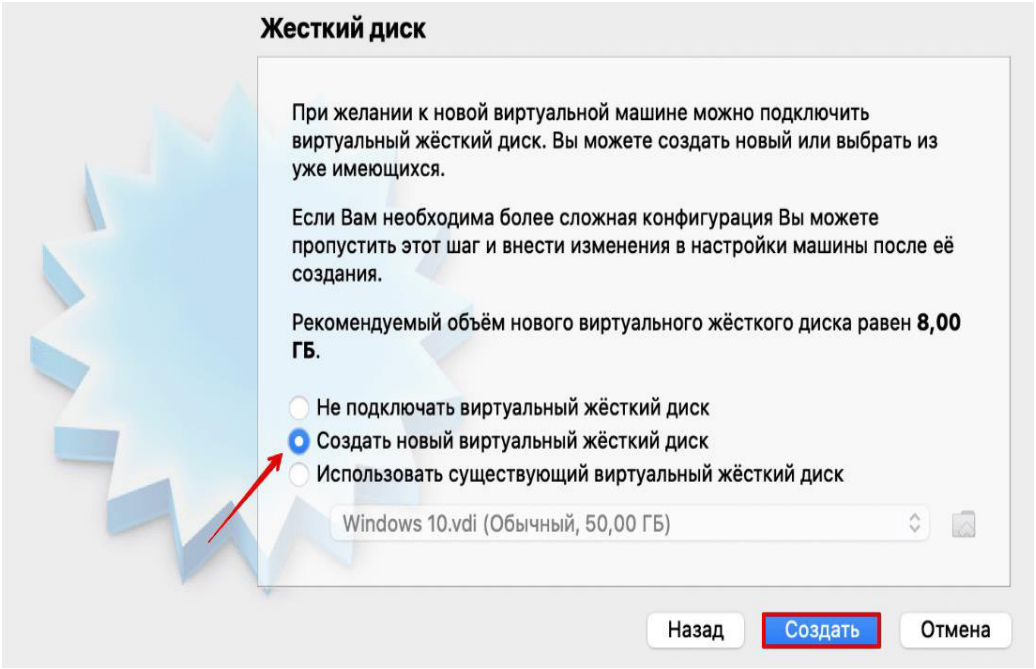


Чтобы выделить объём памяти для машины, сдвиньте ползунок вправо. Мы рекомендуем указать объём 4 ГБ, но если на вашем компьютере недостаточно

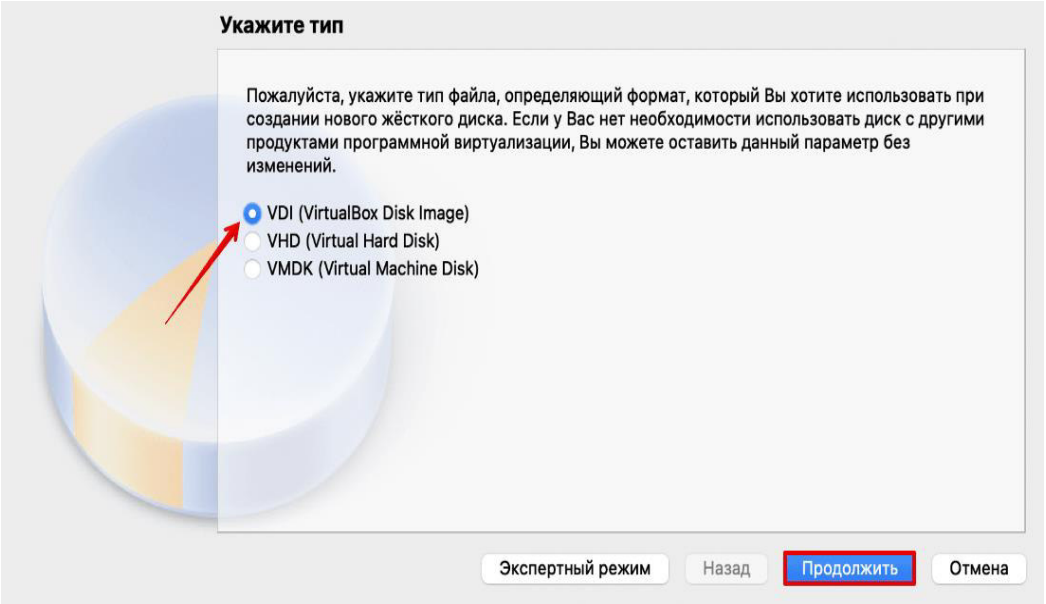
оперативной памяти, выбирайте 2-3 ГБ. Нажмите Продолжить:



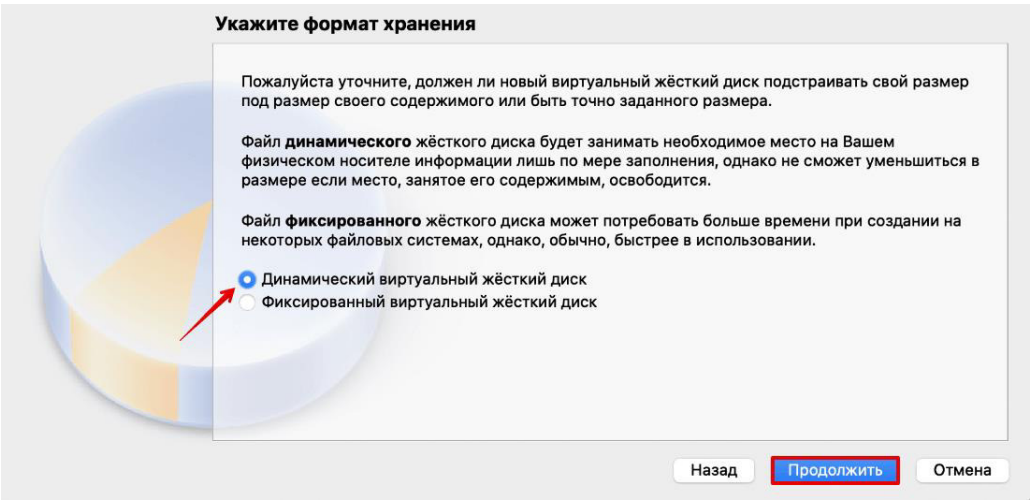
Выберите пункт Создать новый виртуальный жёсткий диск и кликните Создать:



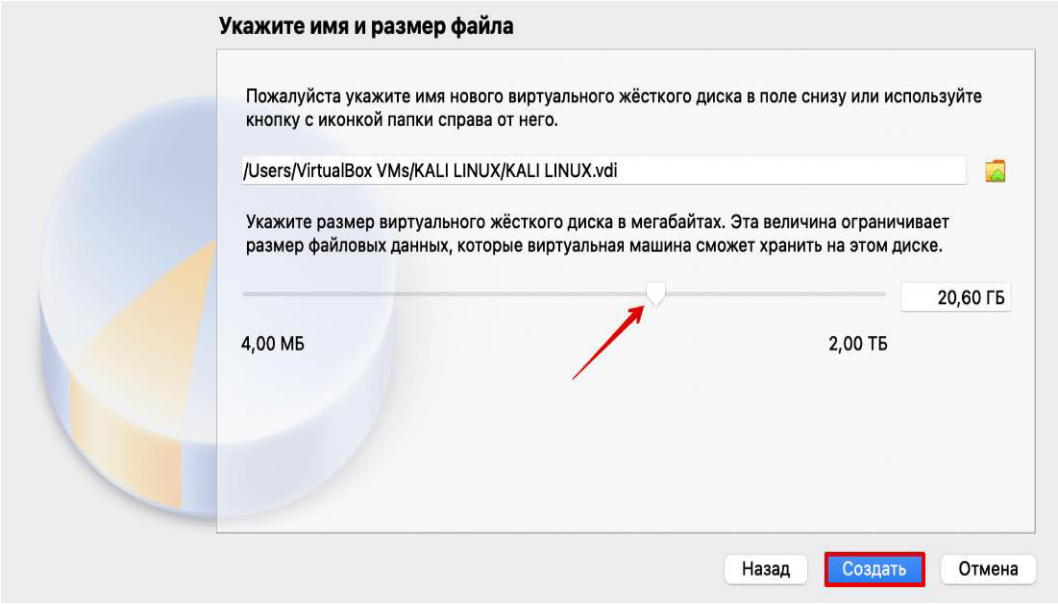
Укажите тип файла VDI (VirtualBox Disk Image) и нажмите Продолжить:



Выберите формат хранения Динамический виртуальный жёсткий диск. Нажмите Продолжить:



Выберите объём диска виртуальной машины. Для установки Kali Linux будет достаточно 20 ГБ. Передвиньте ползунок вправо и нажмите Создать:

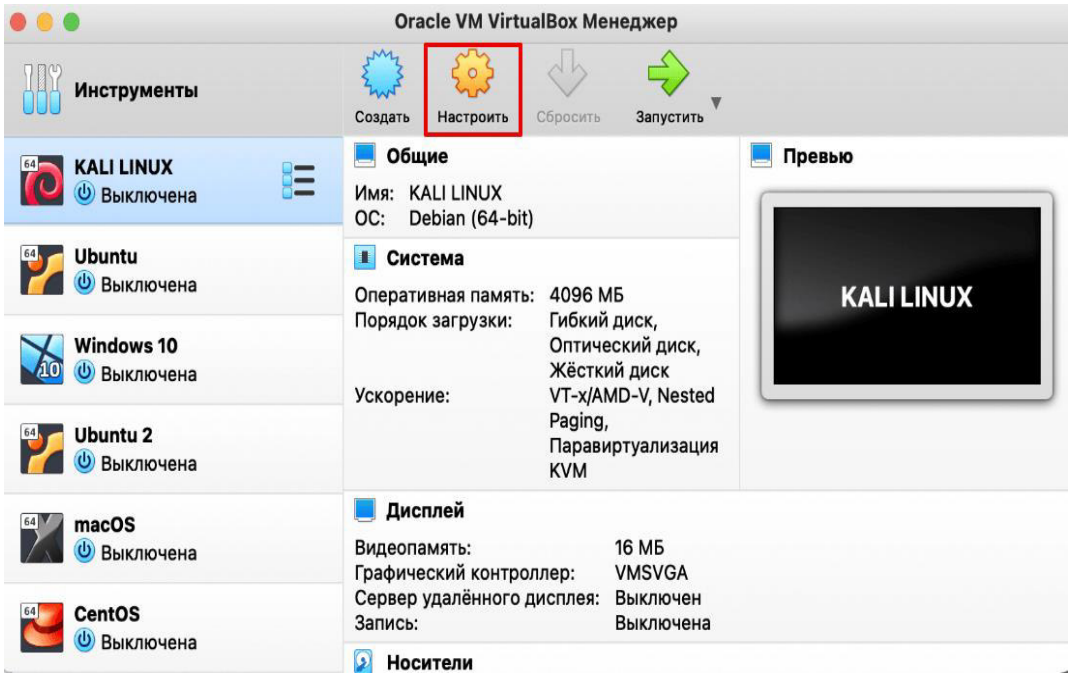


Готово, вы создали виртуальную машину.

Этап 2. Настройка виртуальной машины для Kali Linux

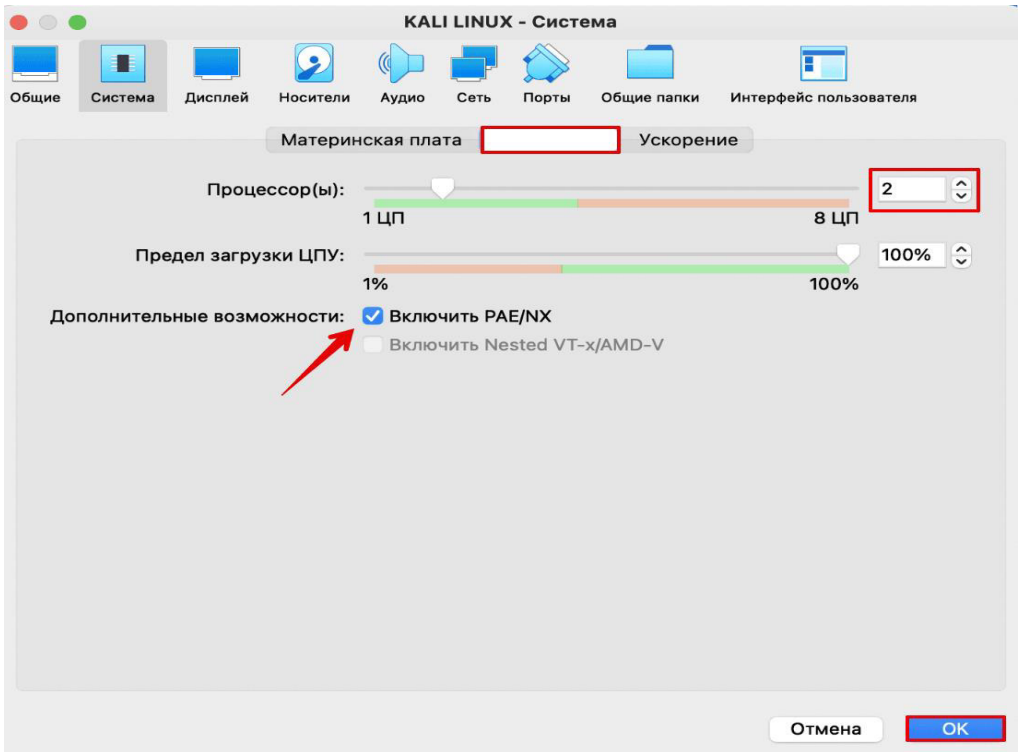
Kali Linux очень требовательна к количеству процессоров, а также использует PAE-ядро. Если вы сразу начнёте установку ОС в обычном режиме, то увидите ошибку. Поэтому перед установкой операционной системы нужно включить функцию PAE и увеличить количество ядер. Для этого:

Нажмите Настроить:



Перейдите во вкладку Система — Процессор. По умолчанию для виртуальной машины выделяется одно ядро процессора. В строке «Процессор(ы)» поставьте значение 2.

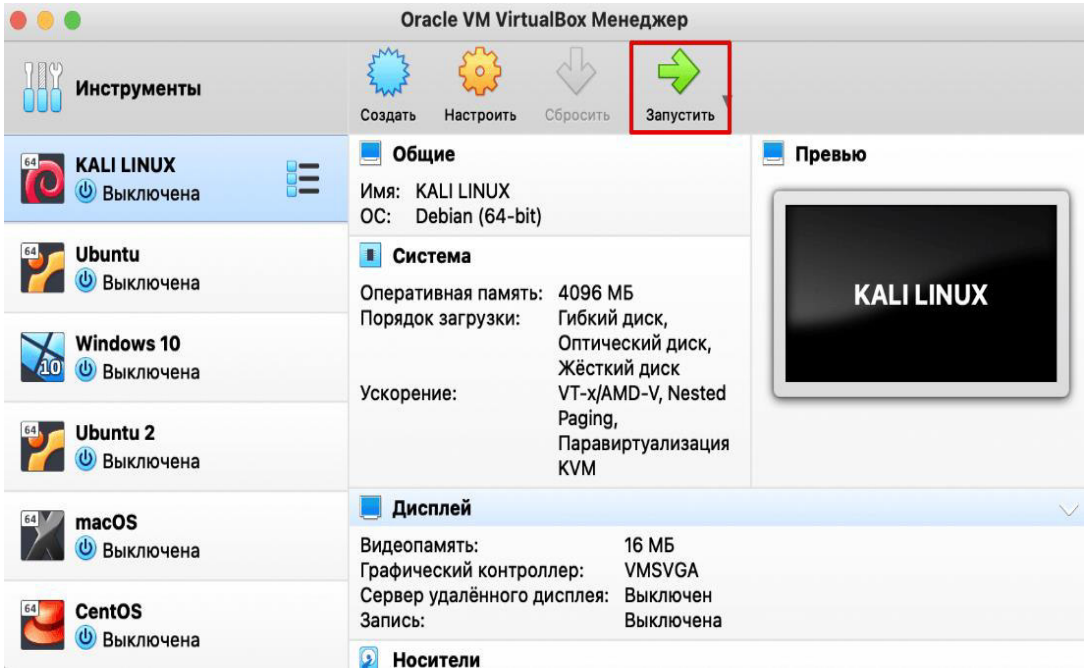
Отметьте галочку напротив «Включить PAE/NX». Нажмите OK:



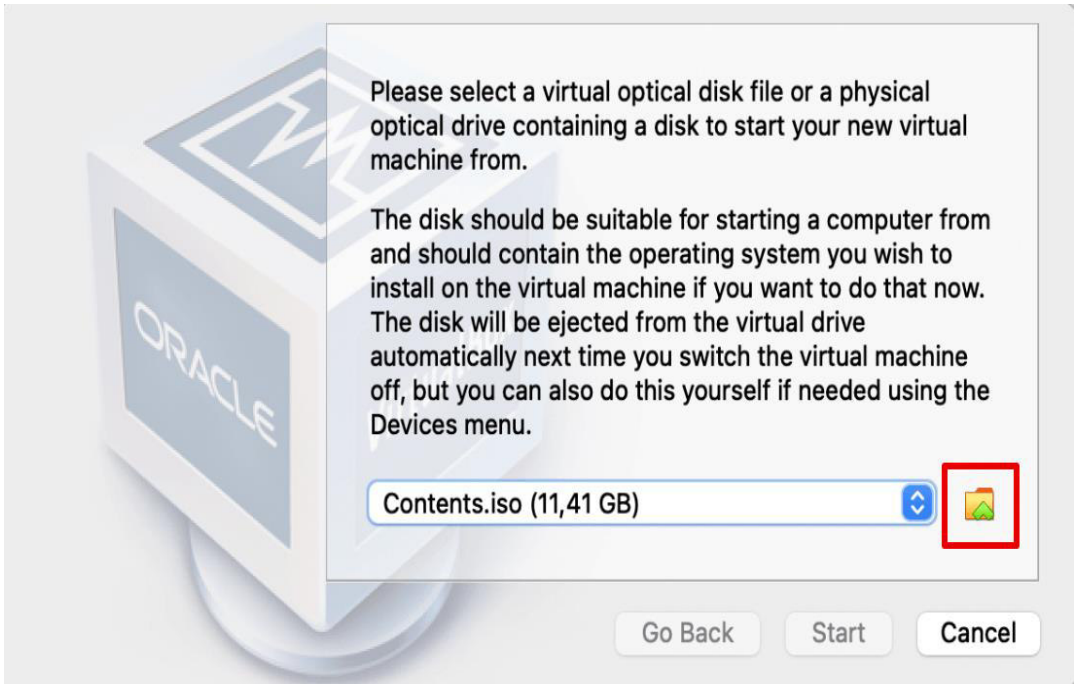
Теперь переходите к установке операционной системы.

Этап 3. Установка операционной системы Kali Linux

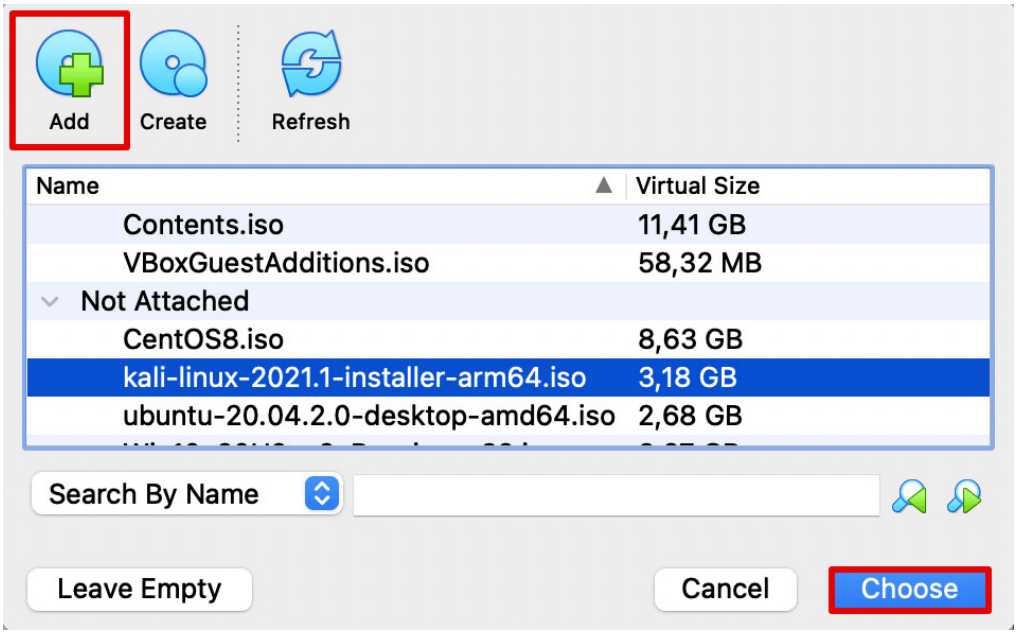
1. Запустите виртуальную машину:



2. Загрузите скачанный образ. Для этого справа нажмите на иконку папки:

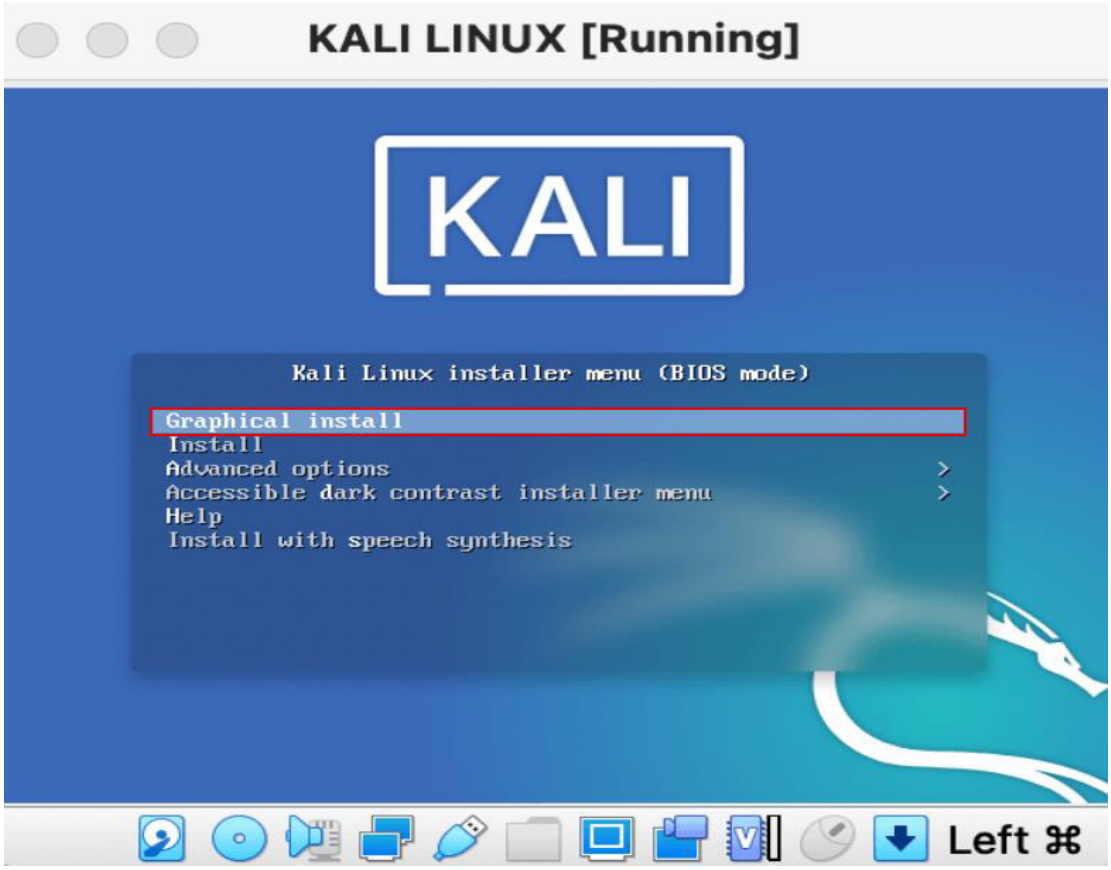


3. Выберите нужный образ из списка или загрузите новый, нажав на Add.
4. Нажмите Choose:



1. Затем нажмите Start:

Чтобы выбрать установку с графическим интерфейсом, нажмите Enter. Это самый простой способ установки ОС без работы в командной строке:



Для завершения установки следуйте подсказкам системы. На последнем этапе виртуальная машина будет перезагружена.

Готово, установка завершена.

7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Таблица 7

Планируемые результаты освоения компетенции	**Критерии оценивания результатов обучения**				**Наименование оценочного средства**
	менее 41 баллов (неуд)	**41-60 баллов (удовлетворитель)**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;					
Знать: современные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: выбирать информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	

Владеть: навыками применения современных информационно-коммуникационных технологий, программных средств системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности					
Знать: основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	

Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере профессиональной деятельности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю					
Знать: основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	

Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю .	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов					
Знать: локальные нормативные акты, стандарты информационной безопасности и меры по обеспечению безопасности объекта защиты	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	Билеты к зачету, текущий контроль
Уметь: формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
Владеть: методами повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- для слепых: задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

3. Галатенко В.А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142285.html (дата обращения: 10.06.2025). — Режим доступа: для авторизир. пользователей.

4. Бондаренко И.С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137525/details (дата обращения: 10.06.2025). — Режим доступа: для авторизир. пользователей.

5. Бирюков А.А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 3-е изд. — Москва : ДМК Пресс, 2023. — 440 с. — ISBN 978-5-93700-219-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/159410/details (дата обращения: 10.06.2025). — Режим доступа: для авторизир. пользователей.

10. Материально-техническое обеспечение дисциплины

10.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- стационарные компьютеры;
- мультимедийный проектор;
- настенный экран.

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 3-07.

Аудитория 3-07, интерактивная доска SB 480-H2-062616, проектор Smart v25, аппаратная Nettop.

Методические указания по освоению дисциплины
«Основы информационной безопасности»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Обучение по дисциплине «Основы информационной безопасности» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, доклады с презентациями, индивидуальная консультация с преподавателем).

Учебный материал структурирован и изучение дисциплины производится в тематической последовательности. Каждому лабораторному занятию и самостоятельному изучению материала предшествует лекция по данной теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе проблемных ситуаций и поисков путей их решения.

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10- 15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10-15 минут).
3. В течение недели выбрать время для работы с литературой в электронной библиотечной системе (по 1 часу).
4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1-2 задачи.

2. Методические указания по работе обучающихся во время проведения лекций

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, прибегать к противопоставлениям и сравнениям, делать

обобщения, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к лабораторным занятиям

На лабораторных занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий.

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

1. Ознакомиться с планом занятия, который отражает содержание предложенной темы.
2. Проработать конспект лекций.
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к лабораторным занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

1. Ответить на вопросы плана лабораторного занятия.
2. Выполнить домашнее задание.
3. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять практические задания, которые даются в фонде оценочных средств дисциплины.

4. Методические указания обучающимся по организации самостоятельной работы

Цель организации самостоятельной работы по дисциплине «Основы информационной безопасности» – это углубление и расширение знаний в области научной исследовательской деятельности; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к лабораторному занятию включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. Лабораторное занятие – это, прежде всего, дискуссия, обсуждение конкретной ситуации, то есть предполагает умение внимательно слушать членов малой группы и модератора, а также стараться высказать свое мнение, высказывать собственные идеи и предложения, уточнять и задавать вопросы коллегам по обсуждению.

При подготовке к контрольной работе (рубежной аттестации) обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях;

– в контакте с преподавателем вне рамок расписания – на консультациях по

учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15 баллов)

1. Доклад с презентацией
2. Подготовка к лабораторным занятиям

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), лабораторных, к изданиям электронных библиотечных систем.

Разработчик:
Старший преподаватель кафедры
«Информатика и вычислительная техника» /М.З.Исаева /

СОГЛАСОВАНО:

Заведующий кафедрой
«Информатика и вычислительная техника» /Э. Д. Алисултанова/

Директор ДУМР /М.А. Магомаева/