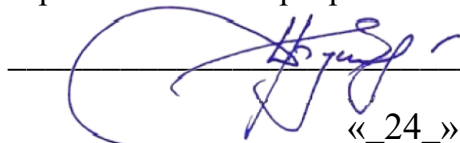


Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной  
образовательной программы

 Буинцев Д.Н.  
«\_24\_» сентября 2024 г

## РАБОЧАЯ ПРОГРАММА

Дисциплины

*Б1.О.31 Безопасность компьютерных сетей*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

*10.03.01 Информационная безопасность*

профиль

*Безопасность автоматизированных систем  
(по отрасли или в сфере профессиональной деятельности)*

Квалификация

*бакалавр*

Форма обучения

*очная*

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск  
2024

Рабочая программа дисциплины Безопасность компьютерных сетей составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(и):

Г.В. Филиппова, старший преподаватель кафедры информатики



Рабочая программа дисциплины Безопасность компьютерных сетей утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности  
заведующего кафедрой

Г.С. Осипов



## 1. Цель и задачи дисциплины

### Цель дисциплины

Целями освоения дисциплины *«Безопасность компьютерных сетей»* являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по принципам администрирования систем защиты информации компьютерных сетей достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

### Задачи дисциплины

Основными задачами изучения дисциплины являются:

- основные меры по защите информации в компьютерных сетях, а также содержание эксплуатационной документации компьютерных сетей;
- критерии оценки защищенности компьютерных сетей, средства контроля эффективности мер защиты информации;
- выработка практических навыков по решению задач защиты компьютерных сетей, исходя из задач, стоящих перед вычислительной системой.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность компьютерных сетей» относится к обязательной части Блока 1 Дисциплины (модули) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность

### Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знаниях, полученных в результате изучения таких дисциплин как «Основы информационной безопасности», «Операционные системы», «Администрирование операционных систем», Безопасность операционных систем, Сети и системы передачи информации

Изучение данной дисциплины проходит параллельно с изучением такой дисциплины, как «Программно-аппаратные средства защиты информации», «Защита информации от утечки по техническим каналам» и базируется на знаниях, полученных в результате изучения этих дисциплин.

### Постреквизиты дисциплины:

Знания и умения, полученные студентами при изучении дисциплины «Безопасность компьютерных сетей», применяются ими во время учебной и преддипломной практик и в их профессиональной деятельности.

## 3. Формируемые компетенции и индикаторы их достижения по дисциплине

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы;

	технических средств защиты информации автоматизированных систем	ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы
ОПК-4.4	ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 - Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации; ОПК-4.4.2 - Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия пользователей автоматизированных систем, а также документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы; ОПК-4.4.3 - Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств.

#### 4. Структура и содержание дисциплины

##### 4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц (72 академических часа).

Вид работы	Трудоемкость, акад. часов	
	8 семестр	всего
<b>Общая трудоемкость</b>	<b>72</b>	<b>72</b>
<b>Контактная работа:</b>	<b>50</b>	<b>50</b>
Лекции	22	22
Лабораторные работы (Лаб)	24	24
Контактная работа в период теоретического обучения (КонтТО) ( <i>Проведение текущих консультаций и индивидуальная работа со студентами</i> )	4	4
<b>Промежуточная аттестация (зачет)</b>		
<b>Самостоятельная работа:</b>	<b>22</b>	<b>22</b>

- самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий);	10	10
- подготовка к лабораторным занятиям;	12	12

#### 4.2. Распределение видов работы и их трудоемкости по разделам дисциплины

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
		контактная			Самостоятельная работа	
		Лекции	Практические занятия	Лабораторные занятия		
8 семестр						
1.	Тема 1. Основы безопасности компьютерных сетей. Основные понятия и терминология, угрозы, уязвимости, атаки	2			1	Устный опрос по теме лекции
2.	Тема 2. Основы безопасности компьютерных сетей. Нормативно-правовое обеспечение информационной безопасности КС	2			1	Устный опрос по теме лекции .
3.	Тема 3 Основы безопасности компьютерных сетей. Классификация угроз и уязвимостей, банки угроз и уязвимостей, Банк данных угроз ФСТЭК, MITRE ATT&CK	2			1	Устный опрос по теме лекции
4.	Тема 4 Основы безопасности компьютерных сетей. Сетевые атаки, модель Cyber-Kill Chain	2			1	Устный опрос по теме лекции
5.	Тема 5 Средства обеспечения безопасности компьютерных сетей. Фильтрация сетевого трафика, межсетевые экраны, NGFW	2		2	1	Устный опрос по теме лекции Выполнение практического задания
6.	Тема 6 Средства обеспечения безопасности компьютерных сетей. Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений	2		2	2	Устный опрос по теме лекции Выполнение практического задания
7.	Тема 7. Средства обеспечения безопасности компьютерных сетей. Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей	2		4	2	Устный опрос по теме лекции Выполнение практического задания
8.	Тема 8. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети	2		4	3	Устный опрос по теме лекции Выполнение практического задания

9.	Тема 9 Средства обеспечения безопасности компьютерных сетей. Предотвращение утечек информации, DLP-системы	2		4	2	Устный опрос по теме лекции Выполнение практического задания
10.	Тема 10 Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)	2		4	4	Устный опрос по теме лекции Выполнение практического задания
11.	Тема 11. Современные тенденции в обеспечении безопасности компьютерных сетей Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты. XDR-системы	2		4	4	Устный опрос по теме лекции Выполнение практического задания
	<b>итого:</b>	22		24	22	

### 4.3.Содержание разделов дисциплины

#### Раздел 1 Основы безопасности компьютерных сетей

Тема 1. Основные понятия и терминология, угрозы, уязвимости, атаки

Тема 2. Нормативно-правовое обеспечение информационной безопасности КС

Тема 3. Классификация угроз и уязвимостей, банки угроз и уязвимостей. Банк данных угроз ФСТЭК, MITRE ATT&CK

Тема 4 Сетевые атаки, модель Cyber-Kill Chain

#### Раздел 2 Средства обеспечения безопасности компьютерных сетей

Тема 5. Фильтрация сетевого трафика, межсетевые экраны, NGFW

Тема 6 Средства обеспечения безопасности компьютерных сетей. Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений

Тема 7. Средства обеспечения безопасности компьютерных сетей. Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей

Тема 8. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети

Тема 9 Средства обеспечения безопасности компьютерных сетей. Предотвращение утечек информации, DLP-системы

Тема 10 Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)

Тема 11. Современные тенденции в обеспечении безопасности компьютерных сетей Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты. XDR-системы

### Темы и планы лабораторных занятий

#### Лабораторное занятие №1 (2 ч.)

Тема. Межсетевые экраны

Вопросы для обсуждения:

1. Фильтрация сетевого трафика, межсетевые экраны, NGFW
2. возможности межсетевого экрана, встроенного в операционную систему
3. Включение межсетевого экран на рабочей станции
4. Блокирование сетевых ресурсов
5. Отключение межсетевого экрана.

### **Лабораторное занятие №2 ( 2 ч.)**

Тема. Системы обнаружения вторжений

Вопросы для обсуждения:

1. Технологии обнаружения сетевых атак,
2. Виды систем обнаружения вторжений.
3. Использование систем для предотвращения вторжений.

### **Лабораторное занятие №3-4 (4 ч)**

Тема. Виртуальные защищенные сети

Вопросы для обсуждения:

1. Технологии построения защищенных каналов связи,
2. средства построения виртуальных защищенных сетей

### **Лабораторное занятие №5-6 (4 ч)**

Тема. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети

Вопросы для обсуждения:

1. Инструменты для исследования сети
2. снифферы
3. сканеры безопасности
4. инструменты мониторинга состояния сети

### **Лабораторное занятие №7-8 (4 ч)**

Тема. DLP-системы. Системы защиты конечных точек (EPP-решения)

Вопросы для обсуждения:

1. Предотвращение утечек информации,
2. DLP-системы

### **Лабораторное занятие №9-10 (4 ч)**

Тема. Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)

Вопросы для обсуждения:

1. средства обеспечения безопасности компьютерных сетей.
2. защита конечных устройств КС,
3. технологии Endpoint Security,
4. системы защиты конечных точек (Endpoint Protection Platform)

### **Лабораторное занятие №11-12 (4 ч)**

Тема. Современные тенденции в обеспечении безопасности компьютерных сетей. Этапы проведения тестирования на проникновение, инструменты. XDR-системы Инструменты тестирования на проникновение

Вопросы для обсуждения:

1. основы тестирования на проникновение,
2. этапы проведения тестирования на проникновение,
3. инструменты.
4. XDR-системы
5. Инструменты тестирования на проникновение

## **5. Темы дисциплины (модуля) для самостоятельного изучения**

Не предусмотрены

## **6. Образовательные технологии**

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
----------	----------------------	----------------------	----------------------------

1.	Тема 1. Основы безопасности компьютерных сетей. Основные понятия и терминология, угрозы, уязвимости, атаки	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
2.	Тема 2. Основы безопасности компьютерных сетей. Нормативно-правовое обеспечение информационной безопасности КС	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
3.	Тема 3 Основы безопасности компьютерных сетей. Классификация угроз и уязвимостей, банки угроз и уязвимостей, Банк данных угроз ФСТЭК, MITRE ATT&CK	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
4.	Тема 4 Основы безопасности компьютерных сетей. Сетевые атаки, модель Cyber-Kill Chain	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
5.	Тема 5 Средства обеспечения безопасности компьютерных сетей. Фильтрация сетевого трафика, межсетевые экраны, NGFW	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
6.	Тема 6 Средства обеспечения безопасности компьютерных сетей. Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
7.	Тема 7. Средства обеспечения безопасности компьютерных сетей. Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
8.	Тема 8. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
9.	Тема 9 Средства обеспечения безопасности компьютерных сетей. Предотвращение утечек информации, DLP-системы	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
10.	Тема 10 Средства обеспечения безопасности компьютерных сетей.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором



	Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)	Лабораторное занятие 1 Лабораторное занятие 2	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
11.	Тема 11. Современные тенденции в обеспечении безопасности компьютерных сетей Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты. XDR-системы	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.

## 7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Форма контроля для очной формы обучения – *зачет*,

Примеры заданий для текущего контроля и промежуточных заданий по различным темам:

### Примерный перечень тестовых заданий

- В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?
  - использовать систему обнаружения вторжений
  - переименовать учетную запись администратора
  - включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации
  - использовать мультифакторную аутентификацию
- Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?
  - система обнаружения вторжений
  - персональный межсетевой экран
  - трансляция сетевых адресов
  - антивирусное программное обеспечение
- Какое из средств защиты используется для мониторинга сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности?
  - межсетевой экран
  - система анализа защищенности
  - система предотвращения вторжений
  - средство антивирусной защиты
- Как называется процесс защиты ресурсов сети от несанкционированного использования?

- а) охрана оборудования сети
  - б) защита ядра безопасности
  - в) контроль доступа
  - г) защита периметра безопасности
5. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?
- а) создать диапазон IP адресов
  - б) создать параметр DHCP
  - в) создать исключение для IP адреса г) создать область DHCP
6. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?
- а) сетевой доступ
  - б) папка
  - в) каталог
  - г) домен
7. Какой протокол используется для доступа к службе каталогов Active Directory?
- а) ShareDiscovery б) ADSL
  - б) LDAP
  - в) ICMP
8. Как называется компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам?
- а) хаб
  - б) рабочая станция
  - в) сервер
  - г) хост
9. В каком методе передачи данные пересылаются в двух направлениях одновременно?
- а) симплексный
  - б) синхронный
  - в) дуплексный
  - г) полудуплексный
10. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?
- а) синхронном
  - б) асинхронном
  - в) туннельном
  - г) транспортном

### **Примерные вопросы к зачету**

1. Перехват информации в сети. Инструменты. Способы противодействия перехвату.

2. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам.
3. Сканеры безопасности. Способы выявления уязвимостей в информационных системах.
4. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.
5. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.
6. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.
7. Демилитаризованная зоны. Назначение. Способы выделения.
8. Классификация межсетевых экранов согласно нормативных документов ФСТЭК России. Применение межсетевых экранов различных классов.
9. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки. Понятие сети. Требования, предъявляемые к сети.

## 8. Система оценивания планируемых результатов обучения

**Оценка «зачтено»** выставляется,

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

**Оценка «не зачтено»** выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,5	1	8	16
Подготовка к занятию, выполнение домашнего задания	0,5	1	8	16
выполнение практических заданий по темам	3	5	27	45
Промежуточная аттестация (зачет)	10	23	10	23
<b>Итого за семестр</b>			<b>53</b>	<b>100</b>

## 9. Учебно-методическое и информационное обеспечение дисциплины

### 9.1. Основная литература

а) основная литература:

1. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва :

- Издательство Юрайт, 2022. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1.[Электронный ресурс]: — Режим доступа: <https://urait.ru/bcode/489201>.
2. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/131717>.
  3. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / Ложников П.С., Михайлов Е.М.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 263 с. — ISBN 978-5-4497-0666-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97553.html>

## **9.2.Дополнительная литература**

1. В. Г. Олифер, Н. А. Олифер. Сетевые операционные системы. — учебник для вузов 2-е изд, СПб.: Питер, 2012. —672 с: ил.
2. Таненбаум Эндрю С. Современные операционные системы. 3-е изд. 2012 год, 1120с
3. Маршрутизация в компьютерных сетях : учебно-методическое пособие / составители Г. В. Абрамов [и др.]. — Воронеж : ВГУ, 2017. — 27 с.[Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/154773>.

## **9.3.Программное обеспечение**

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. Дистрибутивы Ubuntu GNU/Linux, Debian GNU/Linux
13. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;
14. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
15. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

## **9.4.Профессиональные базы данных и информационные справочные системы современных информационных технологий**

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел

- Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки (<https://github.com/>)
  3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
  4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии ([http://window.edu.ru/catalog/?p\\_rubr=2.2.75.6](http://window.edu.ru/catalog/?p_rubr=2.2.75.6))
  5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
  6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
  7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
  8. Интернет-университет информационных технологий ([www.intuit.ru](http://www.intuit.ru))
  9. Онлайн среда разработки приложений ([ideone.com](http://ideone.com))
  10. Журнал «КомпьютерПресс» ([www.compress.ru](http://www.compress.ru))
  11. Издательство «Открытые системы» ([www.osp.ru](http://www.osp.ru))
  12. Издание о высоких технологиях ([www.cnews.ru](http://www.cnews.ru))
  13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
  14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
  15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
  16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
  17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

## **10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

### ***Для слепых и слабовидящих:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

### ***Для глухих и слабослышащих:***

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

### ***Для лиц с нарушениями опорно-двигательного аппарата:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным

- программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

***Для слепых и слабовидящих:***

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

***Для глухих и слабослышащих:***

- в печатной форме;
- в форме электронного документа.

***Для обучающихся с нарушениями опорно-двигательного аппарата:***

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

***для слепых и слабовидящих:***

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

***для глухих и слабослышащих:***

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

***для обучающихся с нарушениями опорно-двигательного аппарата:***

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

## **11. Материально-техническое обеспечение дисциплины (модуля)**

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

***К рабочей программе прилагаются:***

**Приложение 1** – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

**Приложение 2** – Методические указания для обучающихся по освоению дисциплины (модуля).