МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 025493C4E0B34808564BE6735EBB2702
Владелец: Ситов Илья Сергеевич
Действителен: с 16.01.2023 до 10.04.2024

УТВЕРЖДАЮ

Проректор по учебной работе

_____Е.И.Луковникова

05 июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.05.05 Основы информационной безопасности интеллектуальных систем

Закреплена за кафедрой **Управления в технических системах**

Учебный план b110302_23_ИИС.plx
Направление: 11.03.02 Инфокоммуникационные технологии и системы связи

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **8 ЗЕТ**

Виды контроля в семестрах:
Контрольная работа 8, Экзамен 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	13			
Вид занятий	УП	РП	УП	РП
Лекции	52	52	52	52
Лабораторные	39	39	39	39
Практические	39	39	39	39
В том числе инт.	18	18	18	18
Итого ауд.	130	130	130	130
Контактная работа	130	130	130	130
Сам. работа	131	131	131	131
Часы на контроль	27	27	27	27
Итого	288	288	288	288

Программу составил(и):
к.т.н., доц., Ульянов А.Д. _____
Рабочая программа дисциплины

Основы информационной безопасности интеллектуальных систем

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (приказ Минобрнауки России от 19.09.2017 г. № 930)
составлена на основании учебного плана:

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи
утвержденного приказом ректора от 17.02.2023 № 72.

Рабочая программа одобрена на заседании кафедры

Управления в технических системах

Протокол от 19 апреля 2023 г. № 9

Срок действия программы: 2023-2027 уч.г.

Зав. кафедрой Григорьева Т.А.

Председатель МКФ

старший преподаватель Латушкина С.В. _____ 24 апреля 2023г. №9

Ответственный за реализацию ОПОП _____ Григорьева Т.А.

Директор библиотеки _____ Сотник Т.Ф.

№ регистрации 13
(методический отдел)

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Управления в технических системах

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2024 г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Управления в технических системах

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2025 г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Управления в технических системах

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2026 г. № __
Зав. кафедрой

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Управления в технических системах

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2027 г. № __
Зав. кафедрой

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования про граммных и аппаратных средств в сетях и системах связи, а также в области поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.05.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Сетевые технологии высокоскоростной передачи данных
2.1.3	Вычислительная техника и информационные технологии
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная (преддипломная) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3: Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	
Индикатор 1	ОПК-3.1. Применяет методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основные методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности.
3.2	**Уметь:**
3.2.1	Оценивать основные проблемы в области информационной безопасности, связанные с эксплуатацией и внедрением новой телекоммуникационной техники.
3.3	**Владеть:**
3.3.1	Навыками применения основных требований информационной безопасности при эксплуатации интеллектуальных систем

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел	**Раздел 1. Введение в информационную безопасность**						
1.1	Лек	Понятие информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	2	Лекция беседа, ОПК -3.1.
1.2	Лек	Основные составляющие информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	2	Лекция беседа, ОПК -3.1.
1.3	Лек	Важность и сложность проблемы информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	2	Лекция беседа, ОПК -3.1.
1.4	Лек	Основные определения и критерии классификации угроз	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.

1.5	Лек	Некоторые примеры угроз доступности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
1.6	Лек	Вредоносное программное обеспечение	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
1.7	Лек	Основные угрозы целостности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
1.8	Лек	Основные угрозы конфиденциальности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
1.9	Ср	Подготовка к экзамену	8	41	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
1.10	Экзамен		8	5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
	Раздел	**Раздел 2. Уровни информационной безопасности**						
2.1	Лек	Законодательный уровень информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.2	Лек	Обзор российского законодательства в области информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.3	Лек	Обзор зарубежного законодательства в области информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.4	Лек	Административный уровень информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.5	Лек	Политика безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.6	Лек	Программа безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.7	Лек	Синхронизация программы безопасности с жизненным циклом систем	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.8	Лек	Процедурный уровень информационной безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.9	Лек	Управление персоналом	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.

2.10	Лек	Физическая защита	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.11	Лек	Поддержание работоспособности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.12	Лек	Реагирование на нарушения режима безопасности	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.13	Лек	Планирование восстановительных работ	8	2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.14	Ср	Подготовка к экзамену	8	50	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
2.15	Экзамен		8	5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
	Раздел	**Раздел 3. Основные программно-технические меры информационной безопасности сетей и систем**						
3.1	Лек	Основные понятия программно-технического уровня информационной безопасности	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.2	Лек	Особенности современных информационных систем, существенные с точки зрения безопасности	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.3	Лек	Идентификация и аутентификация	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.4	Лек	Архитектурная безопасность	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.5	Лек	Управление доступом. Протоколирование и аудит	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.6	Лек	Активный аудит. Шифрование	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.7	Лек	Контроль целостности. Экранирование	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.8	Лек	Анализ защищенности. Обеспечение высокой доступности	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.9	Лек	Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.

3.10	Лек	Программное обеспечение промежуточного слоя. Обеспечение обслуживаемости	8	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.11	Лаб	Программирование арифметических алгоритмов	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	6	Работа в малых группах, ОПК-3.1.
3.12	Лаб	Программирование алгебраических алгоритмов	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.13	Лаб	Защита от закладок при разработке программ	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.14	Лаб	Программирование алгоритмов криптосистем с открытым ключом	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.15	Лаб	Профилактика заражения вирусами компьютерных систем	8	7	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.16	Пр	Криптографические методы защиты	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	6	Работа в малых группах, ОПК-3.1.
3.17	Пр	Шифрование методом IDEA	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.18	Пр	Шифрование методом RC6	8	8	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.19	Пр	Шифрование методом Джиффорда	8	5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.20	Пр	Шифрование методом аналитических преобразований	8	5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.

3.21	Пр	Сокрытие информации методом стеганографии	8	5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.22	Контр.раб.	Информационная безопасность сетей и систем	8	7	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	0	ОПК-3.1.
3.23	Ср	Подготовка к экзамену	8	40	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.
3.24	Экзамен		8	10	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	ОПК-3.1.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием активных методов обучения (лекция – беседа)

Технология коллективного взаимодействия (работа в малых группах) (самостоятельное изучение обучающимися нового материала посредством сотрудничества в малых группах, дает возможность всем участникам участвовать в работе, практиковать навыки сотрудничества, межличностного общения)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Вопросы для текущего контроля:

1. В чем главный принцип стенографии?
2. В каких «контейнерах» может быть спрятано зашифрованное сообщение?
3. Привести примеры стеганографии древних времён.
4. Дать определение аналитическим преобразованиям.
5. В каких случаях могут быть использованы аналитические преобразования?
6. К какой информации этот вид шифрования может быть применим?
7. Принцип действия метода шифрования Джиффорда?
8. Для каких целей использовался данный метода шифрования?
9. В каком году он был взломан?.
10. Что является входной информацией для шифра RC6?
11. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
12. На сколько блоков делиться входная информация?
13. Что является входной информацией для шифра IDEA?
14. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
15. На сколько блоков делиться входная информация?
16. Что такое шифрование?
17. Чем отличается открытый ключ от закрытого?
18. Дать определение стеганографии.

6.2. Темы письменных работ

Тема контрольной работы : Информационная безопасность сетей и систем.

Цель: Развить навыки студентов по использованию приобретённых знаний в ответах на конкретные вопросы.

Структура: Каждое индивидуальное задание предполагает ответ студента на десять вопросов по 5 темам:

- Основные понятия информационной безопасности.
- Правовое обеспечение защиты информации
- Организационное обеспечение защиты информации
- Инженерно-техническое обеспечение защиты информации
- Программно-аппаратные методы защиты информации

Основная тематика: Информационная безопасность сетей и систем.

Рекомендуемый объем: Пояснительная записка объемом 15 - 20 страниц должна содержать титульный лист, задание, ответ на заданные вопросы, список используемой литературы.

6.3. Фонд оценочных средств

Вопросы к экзамену:

Раздел 1. Введение в информационную безопасность

1.1. Понятие и основные составляющие информационной безопасности.
1.2. Важность и сложность проблемы информационной безопасности.
1.3. Основные определения и критерии классификации угроз.
1.4. Наиболее распространенные угрозы доступности.
1.5. Вредоносное программное обеспечение.
1.6. Угрозы целостности.
1.7. Угрозы конфиденциальности.

Раздел 2. Уровни информационной безопасности

2.1. Что такое законодательный уровень информационной безопасности и почему он важен.
2.2. Обзор российского законодательства в области информационной безопасности.
2.3. Обзор зарубежного законодательства в области информационной безопасности.
2.4. Политика безопасности.
2.5. Программа безопасности.
2.6. Синхронизация программы безопасности с жизненным циклом инфокоммуникационных систем.
2.7. Управление рисками.
2.8. Основные классы мер процедурного уровня.
2.9. Управление персоналом.
2.10. Физическая защита.
2.11. Поддержание работоспособности.
2.12. Реагирование на нарушения режима безопасности.
2.13. Планирование восстановительных работ.

Раздел 3. Основные программно-технические меры информационной безопасности сетей и систем

3.1. Основные понятия программно-технического уровня информационной безопасности.
3.2. Особенности современных информационных систем, существенные с точки зрения безопасности.
3.3. Архитектурная безопасность.
3.4. Основные понятия об идентификации и аутентификации.
3.5. Парольная аутентификация.
3.6. Идентификация/ аутентификация с помощью биометрических данных.
3.7. Управление доступом.
3.8. Ролевое управление доступом.
3.9. Основные понятия протоколирования и аудита.
3.10. Активный аудит.
3.11. Симметричное и ассиметричное шифрование.
3.12. Контроль целостности: хэш-функции и электронно-цифровая подпись.
3.13. Экранирование: основные понятия и архитектурные аспекты.
3.14. Классификация межсетевых экранов.
3.15. Анализ защищенности.
3.16. Основные понятия доступности.
3.17. Основы мер обеспечения высокой доступности.
3.18. Отказоустойчивость и зона риска.
3.19. Обеспечение обслуживаемости.

6.4. Перечень видов оценочных средств

Отчеты по лабораторным работам, контрольная работа, экзаменационные вопросы

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Иванов М.Ю.	Информационные технологии: методы криптографии: учебное пособие	Братск: БрГУ, 2010	1	http://ecat.brstu.ru/catalog/Учебные%20и%20учебно-методические%20пособия/Информатика%20-%20Вычислительная%20техника%20-%20Программирование/Иванов%20М.Ю.%20Информационные%20технологии.Методы%20криптографии.2010.pdf

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.2	Нестеров С. А.	Основы информационной безопасности: учебное пособие	Санкт-Петербург: Издательство Политехническо го университета, 2014	1	http://biblioclub.ru/index.php?page=book&id=363040
Л1.3	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие	Томск: Эль Контент, 2011	1	http://biblioclub.ru/index.php?page=book&id=208694

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие	Москва: Горячая линия-Телеком, 2012	5	
Л2.2	Малюк А.А., Пазизин С.В., Погожин Н.С.	Введение в защиту информации в автоматизированных системах: учебное пособие	Москва: Горячая линия-Телеком, 2011	5	
Л2.3	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственны й архитектурно-строительный университет, 2014	1	http://biblioclub.ru/index.php?page=book&id=438331

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л3.1	Иванов М.Ю.	Защита информации и информационная безопасность в 2 ч. Ч.1-2 .Ч.1: методические указания к выполнению практических занятий	Братск : БрГУ, 2013	22	
Л3.2	Иванов М.Ю.	Защита информации и информационная безопасность в 2 ч. Ч.1-2.Ч.2: методические указания к выполнению практических занятий	Братск : БрГУ, 2013	23	

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Издательство "Лань" электронно-библиотечная система	http://e.lanbook.com

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	Microsoft Windows (Win Pro 10)

7.3.2 Перечень информационных справочных систем

7.3.2.1	Университетская информационная система РОССИЯ (УИС РОССИЯ)
7.3.2.2	Национальная электронная библиотека НЭБ
7.3.2.3	Научная электронная библиотека eLIBRARY.RU
7.3.2.4	Информационная система "Единое окно доступа к образовательным ресурсам"
7.3.2.5	Электронная библиотека БрГУ
7.3.2.6	Электронный каталог библиотеки БрГУ
7.3.2.7	«Университетская библиотека online»
7.3.2.8	Издательство "Лань" электронно-библиотечная система

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение аудитории	Вид занятия
1230	Лаборатория УТС	Основное оборудование: -Netton Acer Revo RL 70 (6 шт.); - монитор Acer V 193 DOB (6 шт.); -системный блок P 4 Cel 2. 26/256 MD/80 (4 штуки); - монитор LCD Acer AL 1716F (4 шт);	Экзамен

		-лабораторный комплекс «Локальные сети ЭВМ. Уровень L3»; -телевизор LG 47; -трибуна докладчика SHOW; -шкаф Практик металлический; -шкаф монтажный настольный Estap. Дополнительно: - маркерная доска – 1 шт. Учебная мебель: -комплект мебели (посадочных мест/АРМ) - 16/ 10 шт. -комплект мебели (посадочных мест) для преподавателя – 1 шт.	
2201	читальный зал №1	Комплект мебели (посадочных мест) Стеллажи Комплект мебели (посадочных мест) для библиотекаря Выставочные шкафы ПК i5-2500/H67/4Gb (монитор TFT19 Samsung) (10шт.); принтер HP Laser Jet P2055D (1шт.)	Ср
1230	Лаборатория УТС	Основное оборудование: -Netton Acer Revo RL 70 (6 шт.); - монитор Acer V 193 DOB (6 шт.); -системный блок P 4 Cel 2. 26/256 MD/80 (4 штуки); - монитор LCD Acer AL 1716F (4 шт); -лабораторный комплекс «Локальные сети ЭВМ. Уровень L3»; -телевизор LG 47; -трибуна докладчика SHOW; -шкаф Практик металлический; -шкаф монтажный настольный Estap. Дополнительно: - маркерная доска – 1 шт. Учебная мебель: -комплект мебели (посадочных мест/АРМ) - 16/ 10 шт. -комплект мебели (посадочных мест) для преподавателя – 1 шт.	Пр
1230	Лаборатория УТС	Основное оборудование: -Netton Acer Revo RL 70 (6 шт.); - монитор Acer V 193 DOB (6 шт.); -системный блок P 4 Cel 2. 26/256 MD/80 (4 штуки); - монитор LCD Acer AL 1716F (4 шт); -лабораторный комплекс «Локальные сети ЭВМ. Уровень L3»; -телевизор LG 47; -трибуна докладчика SHOW; -шкаф Практик металлический; -шкаф монтажный настольный Estap. Дополнительно: - маркерная доска – 1 шт. Учебная мебель: -комплект мебели (посадочных мест/АРМ) - 16/ 10 шт. -комплект мебели (посадочных мест) для преподавателя – 1 шт.	Лек
А1210	Учебная аудитория (мультимедийный класс)	Основное оборудование: -Интерактивная доска SMART Board X885ix со встроенным проектором UX60 (Персональный компьютер i5-2500/H67/4Gb /500 Gb. Монитор TFT19 Samsung E 1920NR; акустическая система Jb-118) Дополнительно: - маркерная доска – 1 шт. Учебная мебель: -комплект мебели (посадочных мест) – 25 шт. -комплект мебели (посадочных мест/АРМ) для преподавателя – 1/1 шт.	Лаб

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Материал лекции учитывается при подготовке к лабораторным работам.
Для освоения обучающимися дисциплины и достижения запланированных результатов обучения. Учебным планом предусмотрены лекции, лабораторные работы, практические занятия, самостоятельная работа студента, выполнение контрольной работы, подготовка и сдача экзамена. В условиях рейтинговой системы контроля результаты текущего оценивания студента используются как показатель его текущего рейтинга.
Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы. Данный вид контроля стимулирует у обучающегося стремление к систематической самостоятельной работе по изучения дисциплины.
Обучающийся, пользуясь рабочей программой, основной и дополнительной литературой, сам организует процесс изучения дисциплины.
Самостоятельная работа способствует сознательному усвоению, углублению и расширению теоретических знаний; форматирует необходимые профессиональные умения и навыки и совершенствует имеющиеся; происходит более глубокое осмысление методов научного и творческого познания конкретной дисциплины.
Основными формами такой работы являются:

- конспектирование лекций и прочитанного источника;
- проработка материалов прослушанной лекции;
- самостоятельное изучение программных вопросов, указанных преподавателем на лекциях и выполнение домашних заданий;
- обзор и обобщение литературы по интересующему вопросу;
- выполнение контрольной работы;
- подготовка к лабораторным работам, практическим занятиям, экзамену.