

Документ подписан простой электронной подписью
Информация о владельце: МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФИО: Луковникова Елена Ивановна
Должность: Проректор по учебной работе
Дата подписания: 10.06.2022 10:36:43
Уникальный программный ключ:
890f5aae3463de1924cbcf76ac5d7ab89e9fe3d2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ



Проректор по учебной работе

Е.И.Луковникова

20 22 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07.ДВ.02.01 Комплексное обеспечение безопасности объекта информатизации

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план **b010302_22_ИПОиЗИ.plx**

Направление: **01.03.02 Прикладная математика и информатика**

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля в семестрах:

Зачет 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	УИ	ПИ		
Неделя	17			
Вид занятий	УИ	ПИ	УИ	ПИ
Лекции	17	17	17	17
Лабораторные	51	51	51	51
В том числе инт.	20	20	20	20
В том числе в форме практ.подготовки	51	51	51	51
Итого ауд.	68	68	68	68
Контактная работа	68	68	68	68
Сам. работа	40	40	40	40
Итого	108	108	108	108

Программу составил(и):

к.т.н., доц., Фигура К.Н.

Рабочая программа дисциплины

Комплексное обеспечение безопасности объекта информатизации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление: 01.03.02 Прикладная математика и информатика
утвержденного приказом ректора от 08.02.2022 протокол № 45.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 12 апреля 2022 г. № 09

Срок действия программы: 2022-2026 уч.г.

Зав. кафедрой Горохов Д.Б.

Председатель МКФ

старший преподаватель Латушкина С.В.

Ответственный за реализацию ОПОП

Директор библиотеки

№ регистрации

(методический отдел)

№ 1118 апреля 2022 г.

(подпись)

Д.Б. Горохов
(ФИО)

(подпись)

Сотникова Т.С.
(ФИО)

45

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

старший преподаватель Латушкина С.В. _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2023-2024 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2023 г. № ____
Зав. кафедрой Горохов Д.Б.

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

старший преподаватель Латушкина С.В. _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2024-2025 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2024 г. № ____
Зав. кафедрой Горохов Д.Б.

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

старший преподаватель Латушкина С.В. _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2025-2026 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2025 г. № ____
Зав. кафедрой Горохов Д.Б.

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

старший преподаватель Латушкина С.В. _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2026-2027 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2026 г. № ____
Зав. кафедрой Горохов Д.Б.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Получить устойчивые навыки по обеспечению комплексной защиты объекта информатизации
-----	---

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.07.ДВ.02.01
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Криптографические методы защиты информации
2.1.2	Основы информационной безопасности *
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	Защита в операционных системах
2.2.3	Основы проектирования программных комплексов

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
Индикатор 1	УК-1.1. Выполняет поиск необходимой информации, её критический анализ и синтез информации, полученной из разных источников
Индикатор 2	УК-1.2. Использует системный подход для решения поставленных задач
ПК-3: Способен анализировать требования к программному обеспечению с целью определения технических возможностей их реализации	
Индикатор 1	ПК-3.1. Применяет знания языков, утилит, средств пакетного выполнения процедур при проведении исследований научного и прикладного характеров
Индикатор 2	ПК-3.2. При согласовании требований к программному обеспечению с заинтересованными сторонами, производит анализ требований и проводит обоснование рекомендуемых решений

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	основные принципы критического анализа и синтеза информации; методы критического анализа и оценки современных научных достижений; основные принципы и методы системного подхода; возможности современных средств разработки программных продуктов; требования к программному обеспечению; требования к программному обеспечению, применяемому для защиты информации.
3.2	Уметь:
3.2.1	осуществлять поиск информации в разных источниках; получать новые знания на основе критического анализа и синтеза информации; получать новые знания на основе критического анализа и синтеза информации; применять методы системного подхода для решения поставленных задач; использовать языки, утилиты, средства пакетного выполнения процедур при проведении исследований научного и прикладного характера в области информационной безопасности; собирать и анализировать информацию о программном обеспечении, применяемом для защиты информации при обосновании рекомендуемого решения.
3.3	Владеть:
3.3.1	навыками исследования проблем предметной деятельности с применением критического анализа и синтеза; навыками выявления научных проблем предметной области и использования адекватных методов для их решения; навыками проведения исследований научного и прикладного характера в области информационной безопасности; навыками выстраивания коммуникаций с заинтересованными сторонами в процессе реализации проекта, проведения презентаций, публичных выступлений.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел	Раздел 1. Защита информации ограниченного доступа криптографическими средствами						

1.1	Лек	Криптосистемы с открытым ключом, электронная подпись	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.2	Лаб	Криптосистемы с открытым ключом, электронная подпись	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.3	Лек	Хеш-функции. Обеспечение контроля целостности сообщений	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.4	Лаб	Хеш-функции. Обеспечение контроля целостности сообщений	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.5	Лаб	Инфраструктура открытых ключей	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.6	Лаб	Защита информации с использованием средств криптографической защиты	7	4	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.7	Ср	Подготовка к выполнению ЛР	7	10	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
1.8	Зачёт	Подготовка к зачёту	7	10	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
	Раздел	Раздел 2. Программные и программно-аппаратные средства защиты информации						
2.1	Лек	Защищенная автоматизированная система	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
2.2	Лаб	Защищенная автоматизированная система	7	4	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2

2.3	Лек	Защита сетевого сегмента информационной системы корпоративного уровня	7	7	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
2.4	Лаб	Защита сетевого сегмента информационной системы корпоративного уровня	7	20	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	10	case-study (анализ конкретных ситуаций, ситуационный анализ), УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
	Раздел	Раздел 3. Техническая защита информации						
3.1	Лек	Технические каналы утечки информации	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
3.2	Лек	Методы добывания и защиты информации	7	2	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
3.3	Лаб	Технические средства и методы защиты информации	7	17	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	6	case-study (анализ конкретных ситуаций, ситуационный анализ), УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
3.4	Ср	Подготовка к выполнению ЛР	7	10	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2
3.5	Зачёт	Подготовка к зачёту	7	10	УК-1 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	УК-1.1, УК-1.2, ПК-3.1, ПК-3.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием интерактивных методов обучения (круглый стол (дискуссия))

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностей (электронные библиотеки))

Образовательные технологии с использованием интерактивных методов обучения (case-study (анализ конкретных ситуаций))

Образовательные технологии с использованием интерактивных методов обучения (case-study (ситуационный анализ))

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**6.1. Контрольные вопросы и задания****ЛЕКЦИЯ-ДИСКУССИЯ**

Лекция-дискуссия №1(2 час.)

Тема: Защищенная автоматизированная система

Лекция-дискуссия №2(2 час.)

Тема: Методы добывания и защиты информации

CASE-STUDY (АНАЛИЗ КОНКРЕТНЫХ СИТУАЦИЙ, СИТУАЦИОННЫЙ АНАЛИЗ)

case-study (анализ конкретных ситуаций, ситуационный анализ) №1 (10 час.)

Тема: Защита сетевого сегмента информационной системы корпоративного уровня

case-study (анализ конкретных ситуаций, ситуационный анализ) №2 (6 час.)

Тема: Технические средства и методы защиты информации

ЛАБОРАТОРНЫЕ РАБОТЫ

Лабораторная работа №1 (2 час.)

Тема: Криптосистемы с открытым ключом, электронная подпись

Вопросы:

- 1)Основные виды электронной подписи;
- 2)Средства электронной подписи;
- 3)Сертификат ключа проверки электронной подписи;
- 4)Криптосистема RSA;
- 5)Криптосистема Эль-Гамала.

Лабораторная работа №2 (2 час.)

Тема:Хеш-функции. Обеспечение контроля целостности сообщений

Вопросы:

- 1)Хэш-функции SHA-1, SHA-2, SHA-3 и ГОСТ Р 34.11;
- 2)Контроль целостности сообщений;

Лабораторная работа №3 (2 час.)

Тема:Инфраструктура открытых ключей

Вопросы:

- 1)Основные понятия, термины и определения в области PKI;
- 2)Управление сертификатами и ключами;
- 3)Архитектура, основные компоненты PKI, их функции и взаимодействие;
- 4)Основные стандарты в области PKI: Стандарты серии X (X.509), стандарты криптографии с открытым ключом PKCS.

Лабораторная работа №4 (4 час.)

Тема:Защита информации с использованием средств криптографической защиты

Вопросы:

- 1)Защита автоматизированных систем предприятия с применением средств криптографической защиты;
- 2)Состав СКЗИ;
- 3)Структура СКЗИ;
- 4)Работа с ключевой информацией.

Лабораторная работа №5 (4 час.)

Тема:Защищенная автоматизированная система

Вопросы:

- 1)Автоматизация процесса обработки информации. Понятие автоматизированной системы;
- 2)Особенности автоматизированных систем в защищенном исполнении;
- 4)Основные виды АС в защищенном исполнении;
- 5)Методы создания безопасных систем;
- 6)Методология проектирования гарантированно защищенных КС;
- 7)Дискреционные модели;
- 8)Мандатные модели.

Лабораторная работа №6 (20 час.)

Тема:Защита сетевого сегмента информационной системы корпоративного уровня

Вопросы:

- 1) Работа с учётными записями пользователей и группами;
- 2) Настройка параметров мандатного управления доступом и мандатного контроля целостности;
- 3) Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности;
- 4) Администрирование ОССН в рамках реализации мандатного контроля целостности;
- 5) Настройка механизмов организации замкнутой программной среды;
- 6) Настройка сетевого взаимодействия;

Лабораторная работа №7 (17 час.)

Тема:Технические средства и методы защиты информации

Вопросы:

- 1) Типовые структура и виды технических каналов утечки информации;

- 2) Основные показатели технических каналов утечки информации;
- 3) Комплексное использование технических каналов утечки информации;
- 4) Акустические и оптические каналы утечки информации;
- 5) Радиоэлектронные каналы утечки информации;
- 6) Вещественные каналы утечки информации;
- 7) Концепция инженерно-технической защиты информации;
- 8) Цели, задачи, ресурсы системы защиты информации;
- 9) Угрозы безопасности информации и меры по их предотвращению;
- 10) Принципы инженерно-технической защиты информации;
- 11) Принципы построения системы инженерно-технической защиты информации.

6.2. Темы письменных работ

Учебным планом не предусмотрены

6.3. Фонд оценочных средств

Вопросы к зачёту:

Раздел 1. Защита информации ограниченного доступа криптографическими средствами

- 1) Основные виды электронной подписи;
- 2) Средства электронной подписи;
- 3) Сертификат ключа проверки электронной подписи;
- 4) Криптосистема RSA;
- 5) Криптосистема Эль-Гамала.
- 6) Хэш-функции SHA-1, SHA-2, SHA-3 и ГОСТ Р 34.11;
- 7) Контроль целостности сообщений;
- 8) Основные понятия, термины и определения в области PKI;
- 9) Управление сертификатами и ключами;
- 10) Архитектура, основные компоненты PKI, их функции и взаимодействие;
- 11) Основные стандарты в области PKI: Стандарты серии X (X.509), стандарты криптографии с открытым ключом PKCS;
- 12) Защита автоматизированных систем предприятия с применением средств криптографической защиты;
- 13) Состав СКЗИ;
- 14) Структура СКЗИ;
- 15) Работа с ключевой информацией;
- 16) Автоматизация процесса обработки информации. Понятие автоматизированной системы;
- 17) Особенности автоматизированных систем в защищенном исполнении;
- 18) Основные виды АС в защищенном исполнении;
- 19) Методы создания безопасных систем;
- 20) Методология проектирования гарантированно защищенных КС;
- 21) Дискреционные модели;
- 22) Мандатные модели;
- 22) Типовые структура и виды технических каналов утечки информации;
- 23) Основные показатели технических каналов утечки информации;
- 24) Комплексное использование технических каналов утечки информации;
- 25) Акустические и оптические каналы утечки информации;
- 26) Радиоэлектронные каналы утечки информации;
- 27) Вещественные каналы утечки информации;
- 28) Концепция инженерно-технической защиты информации;
- 29) Цели, задачи, ресурсы системы защиты информации;
- 30) Угрозы безопасности информации и меры по их предотвращению;
- 31) Принципы инженерно-технической защиты информации;
- 32) Принципы построения системы инженерно-технической защиты информации.

6.4. Перечень видов оценочных средств

Лабораторные работы, вопросы к зачёту

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

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП.1.1	Ярочкин В.И.	Информационная безопасность: Учебник для вузов	Москва: Академический Проект, 2003	25	
ЛП.1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва Берлин: Директ-Медиа, 2020	1	http://biblioclub.ru/index.php?page=book&id=571485

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1. 3	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Москва Берлин: Директ-Медиа, 2019	1	http://biblioclub.ru/index.php?page=book&id=499170
Л1. 4	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=493175
Л1. 5	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	1	http://biblioclub.ru/index.php?page=book&id=438331

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2. 1	Торокин А.А.	Инженерно-техническая защита информации: учебное пособие	Москва: Гелиос АРВ, 2005	10	
Л2. 2	Титов А. А.	Технические средства защиты информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	1	http://biblioclub.ru/index.php?page=book&id=208661
Л2. 3	Титов А. А.	Инженерно-техническая защита информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	1	http://biblioclub.ru/index.php?page=book&id=208567

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л3. 1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л3. 2	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=562246

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	Adobe Acrobat Reader DC
7.3.1.4	Chrome

7.3.2 Перечень информационных справочных систем

7.3.2.1	Электронная библиотека БрГУ
7.3.2.2	Электронный каталог библиотеки БрГУ
7.3.2.3	«Университетская библиотека online»
7.3.2.4	Издательство "Лань" электронно-библиотечная система

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

3125	Учебная аудитория (дисплейный класс)	<p>Основное оборудование:</p> <ul style="list-style-type: none"> -комплект серверного оборудования для построения технической архитектуры комплекса терминальных решений в составе терминального сервера, терминальных рабочих мест и периферии в составе: - терминальный сервер Dell PowerEdge RX740XD; - тонких клиентов SmartClient Mini PC (Intel CPU J1900 1.99GHzx4, 4GB) - 14шт. - монитор Forgame Liquid Crystal Display MK27FC 27" 1800R 1920x1080 144 Hz -14 шт. - вебкамера Logitech C920 PRO), МФУ Canon i-Sensys MF 421dw; <p>Дополнительно:</p> <ul style="list-style-type: none"> - маркерная доска - 1 шт.; - доска интерактивная сенсорная Smart Board SB480 - 1 шт. <p>Учебная мебель:</p> <ul style="list-style-type: none"> - комплект мебели (посадочных мест/АРМ) - 28/14 шт. - комплект мебели (посадочных мест/ АРМ) для программиста - 1/ 1 шт. ПК: AMD64*2 Processor 5000+2.60GHz монитор LG FLATRON L19533 - комплект мебели (посадочных мест/АРМ) для преподавателя - 1/1 шт. ПК: AMD 3 9GHz DVD 19K монитор WACOM DTU-2231
1001	читальный зал №3	<p>Учебная мебель. Оборудование 15- CPU 5000/RAM 2Gb/HDD (Монитор TFT 19 LG 1953S-SF);принтер HP LaserJet P3005</p>

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

Лекции. Написание конспекта лекций: краткое, последовательное изложение основных положений, формулировок, выводов, обобщений; техническое оформление записей (подчеркивание, выделение ключевых слов и терминов). Активная работа на лекции.

Лабораторные работы. Выполнение заданий с использованием методических рекомендаций по выполнению лабораторных работ, оформление отчетов, защита лабораторных работ.

Самостоятельная работа обучающихся. Подготовка к лабораторным работам: проработка материалов по теме лабораторной работы с использованием рекомендуемой литературы, конспекта лекций, ресурсов информационно-телекоммуникационной сети Интернет; выполнение заданий, оформление отчетов по лабораторным работам; подготовка к защите лабораторных работ.

Подготовка к зачёту: систематическая работа с конспектом лекций: чтение записей; проверка терминов с помощью энциклопедий, словарей и справочников; обозначение вопросов, материал, которых вызывает трудности; попытка найти ответ в рекомендуемых источниках; подготовка вопросов преподавателю, если не удастся самостоятельно разобраться в материале.