МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.03
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**6**	**Итого**
Форма контроля / **Вид занятий**	**Экзамен**	
Лекции	32	32
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,35	0,35
Контактная работа	64,35	64,35
Самостоятельная работа	80	80
Контроль	35,65	35,65
Итого	180	180

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Цель освоения дисциплины – изучить основы криптографии и криптографические методы защиты информации.

Дисциплина " Криптографические методы и средства защиты информации " содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью. Объясняется математическая теория, лежащая в основе криптографии. Рассматриваются вопросы реализации алгоритмов шифрования и криптоанализа. Изучаются вопросы правовой регуляторики и применение средств СКЗИ.

Студент получает практические навыки в использовании средств криптографической защиты.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

Основы дискретной математики и логики

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Техническая защита информации

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-11 Способен противодействовать угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	ПК-11.1 Использует знания основ современных криптографических алгоритмов и протоколы для обеспечения информационной безопасности	Знать: - основы современные криптографические алгоритмы и протоколы для обеспечения информационной безопасности; - нормативно-правовые акты по КЗИ
		Уметь: - применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных системах
		Владеть: - навыками работы с программными и аппаратными средствами защиты информации в компьютерных системах; - навыками разработки РПД по КЗИ.
	ПК-11.2 Умеет применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных системах	Знать: - принципы работы ЭП, КриптоПро
		Уметь: - организовать работу с ЭП
		Владеть: - навыками применения программных средств для выполнения криптографических преобразований;

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
	ПК-11.3 Владеет навыками применения программных средств для выполнения криптографических преобразований	Знать: - организацию защищенных каналов связи; - средства КЗИ
		Уметь: - применять и настраивать средства КЗИ
		Владеть: - навыками применения программных средств

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Теоретические основы криптографии 1. Основные понятия и определения 2. Классификация методов преобразования информации 3. История криптографии 4. Требования к криптосистемам 5. Компьютерная криптография	6	2		-	
Модуль 1	Ср	Тема 1 Теоретические основы криптографии	6	6			
Модуль 1	Лек	Тема 2 Нормативно-правовое регулирование в области криптографии 1.Правовое регулирование применения СКЗИ и ЭП в информационных системах 2. Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств 3. КоАП в области криптографии	6	2			
Модуль 1	Ср	Тема 2 Нормативно-правовое регулирование в области криптографии	6	6			
Модуль 1	Лек	Тема 3 Основы криптоанализа 1. Методы криптоанализа 2.Соотнесение методов шифрования и методов криптоанализа	6	2			

		3. Атаки на шифратор 4. Атаки на человека					
Модуль 1	Ср	Тема 3 Основы криптоанализа	6	6			
Модуль 1	Лек	Тема 4 Основы криптографических методов 1 Краткий обзор проблематики и методов современной криптографии. Квантовая криптография. 2. Основные используемые результаты теории чисел. 3. Модель криптосистемы. 4. Задачи и фундаментальные проблемы криптографии. 5. Криптографический протокол как распределенный вычислительный алгоритм 6. Сетевые протоколы TLS\ SSL	6	2		-	
Модуль 1	Пр	Тема 4 Основы криптографических методов Сетевые протоколы TLS\ SSL	6	2			Отчет по практическому занятию № 1
Модуль 1	Ср	Тема 4 Основы криптографических методов	6	6			
Модуль 1	Лек	Тема 5 СКЗИ и среда функционирования 1.Общая схем использования СКЗИ 2.Надежность шифра 3. Методы криптографического преобразования 4. Шифры 5.Алгоритмы блочного шифрования 6.Алгоритмы хэширования 7. Порядок обращения с СКЗИ и криптоключами к ним.	6	2			

Модуль 1	Ср	Тема 5 СКЗИ и среда функционирования	6	6			
Модуль 1	Лек	Тема 6 Симметричные и Асимметричные системы шифрования 2. Симметричные системы шифрования с одним ключом. 3. Достоинства и недостатки шифров с одним ключом. 4. Создание шифров на основе блочных алгоритмом перестановки. 5. Стандарты шифрования DES, 3DES и ГОСТ. 6. Стандарт шифрования AES. 7. Асимметричные системы шифрования с открытым ключом. Достоинства и недостатки шифров с открытым ключом. 8. Способы передачи секретного ключа. Создание ключа на основе псевдослучайных последовательностей. Примеры шифров на основе алгоритма Эль-Гамаля и алгоритма RSA. 9. Однонаправленное преобразование	6	2			
Модуль 1	Пр	Тема 6 Симметричные и Асимметричные системы шифрования Протокол открытого согласования ключа. Шифрование по протоколу Эль-	6	4			Отчет по практическому занятию №2

		Гамаля					
Модуль 1	Пр	Тема 6 Симметричные и Асимметричные системы шифрования Криптосистема RSA	6	2			Отчет по практическому занятию №3
Модуль 1	Ср	Тема 6 Симметричные и Асимметричные системы шифрования	6	5			
Модуль 1	Лек	Тема 7 Криптографические протоколы 1. Основные понятия, классификация протоколов. Протоколы аутентификации (разделение доступа к информации – пароли). 2. Протоколы цифровой подписи (связь аутентификации и цифровой подписи). 3. Протоколы управления ключами, открытое распределение ключей. 4. Организации сетей засекреченной связи 5. Протоколы электронного голосования 6. Протоколы платежных систем	6	2			
Модуль 1	Пр	Тема 7 Криптографические протоколы Применение систем симметричного и ассиметричного шифрования	6	4			Отчет по практическому занятию №4
Модуль 1	Ср	Тема 7 Криптографические протоколы	6	5			
Модуль 1	Лек	Тема 8 Практическое применение сертифицированных шифровальных (криптографических) средств 1. Архитектура криптографических функций ОС MS Windows 2. Хранилища сертификатов в ОС MS Windows 3. eToken 4.КриптоПро CSP	6	2			

Модуль 1	Пр	Тема 8 Практическое применение сертифицированных шифровальных (криптографических) средств Работа с локальным хранилищем сертификатов в ОС Windows	6	4			Отчет по практическому занятию №5
Модуль 1	Ср	Тема 8 Практическое применение сертифицированных шифровальных (криптографических) средств	6	5			
Модуль 1	Лек	Тема 9 Средства идентификации и аутентификации в компьютерных системах 1. Классификация средств идентификации и аутентификации в КС 2. Аутентификация по многоразовым паролям. Протокол аутентификации Kerberos. 3. Протокол аутентификации RADIUS. Аутентификация по предъявлению цифрового сертификата. 4. Использование смарт-карт и USB-ключей с шифрованием. 5. Генерация ключевой пары вне устройства. Генерация ключевой пары с помощью устройства.	6	2		-	
Модуль 1	Пр	Тема 9 Средства идентификации и аутентификации в компьютерных системах Установка и настройка СКЗИ КриптоПро CSP Работа с контейнерами закрытого ключа и сертификатами пользователя	6	4			Отчет по практическому занятию №6
Модуль 1	Ср	Тема 9 Средства идентификации и аутентификации в компьютерных системах	6	5			
Модуль 1	Лек	Тема 10 Организационные мероприятия по использованию криптографических средств	6	2			

		1. Технические vs организационные меры 2. Организация использования СКЗИ и ЭП в организации 3. Организация и обеспечение безопасности СКЗИ и криптоключей к ним на рабочем месте пользователя 4. Лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами					
Модуль 1	Ср	Тема 10 Организационные мероприятия по использованию криптографических средств	6	5			
Модуль 1	Лек	Тема 11 Удостоверяющие центры. Электронная подпись. 1 Аккредитованные УД 2 Технологии ЭП 3 Обеспечение достоверности 4 Обеспечение конфиденциальности 5. Инфраструктура открытых ключей 6.Основные компоненты PKI. Сертификат открытого ключа 7. Виды ключевых носителей	6	2			
Модуль 1	Ср	Тема 11 Удостоверяющие центры. Электронная подпись.		5			
Модуль 1	Лек	Тема 12 ПАК «Удостоверяющий центр «КриптоПроУЦ» 1 Состав и назначение программных компонентов ПАК «КриптоПро УЦ» 2 Описание и назначение программных компонентов ПАК «КриптоПро УЦ»	6	2			
Модуль 1	Пр	Тема 12 ПАК «Удостоверяющий центр «КриптоПроУЦ»	6	4			Отчет по практическому занятию №7

		Порядок развёртывания и настройки ПАК «Криптопро УЦ 2.0» с дополнительными службами штампов времени и актуальных статусов сертификатов					
Модуль 1	Ср	Тема 12 ПАК «Удостоверяющий центр «КриптоПроУЦ»	6	5			
Модуль 1	Лек	Тема 13 Использование дополнительных служб в инфраструктуре открытых ключей 1.Преимущества протокола OCSP 2. КриптоПроOCSP Server 3. КриптоПро Revocation Provider	6	2			
Тема 13 Использование дополнительных служб в инфраструктуре открытых ключей	Ср	Тема 13 Использование дополнительных служб в инфраструктуре открытых ключей	6	5			
Модуль 1	Лек	Тема 14_1 Передача информации по защищенным каналам с использованием крипто алгоритмов. ПО и ПАК для организации защищенных каналов. 1. Средства криптографической защиты информации 2 Дискретная, мандатная политика управления доступом в компьютерных системах 3. Требования ФАПСИ к передаче информации по защишенным каналам связи 4. Организация защищенных каналов связи 5. Обзор ПАК для защищенных каналов	6	2			
Модуль 1	Лек	Тема 14_2 Передача информации по защищенным	6	2			

		каналам с использованием крипто алгоритмов. ПО и ПАК для организации защищенных каналов. 6. Установка и настройка продуктов семейства VipNet 7. Особенности применения VipNet Coordinator 8 Требования к физической защите помещений, где используются СКЗИ					
Модуль 1	Пр	Тема 14 Передача информации по защищенным каналам с использованием крипто алгоритмов. ПО и ПАКи для организации защищенных каналов Установка и настройка VipNet Client	6	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 14 Передача информации по защищенным каналам с использованием крипто алгоритмов. ПО и ПАКи для организации защищенных каналов	6	5			
Модуль 1	Лек	Тема 15 Разработка ОРД 1 Формальные модели и примеры политик безопасности для ИС использующих криптографию 2. Примеры разработки пакета документов по СКЗИ 3. Система управления ЭП	6	2			
Модуль 1	Пр	Тема 15 Разработка ОРД Практическое применение СКЗИ КриптоПро CSP и сертификатов для защиты сообщений электронной почты	6	4			Отчет по практическому занятию №9
Модуль 1	Ср	Тема 15 Разработка ОРД	6	5			
	Контроль		6	35,65			
	ПА	Сдача экзамена	6	0,35		-	Банк тестовых заданий /Вопросы к

							экзамену
			Итого:	**180**			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-11	Протоколы практических заданий №1-9
		Вопросы к экзамену №№1-60
		Темы рефератов
		Банк тестовых заданий №1-350

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1 Реферат: Разработка алгоритма и программы разложения целых чисел для шифра RSA

7.2.2 Использование криптографии для защиты информации

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Сетевые протоколы TLS\SSL
2	Протокол открытого согласования ключа. Шифрование по протоколу Эль-Гамаля
3	Криптосистема RSA
4	Применение систем симметричного и ассиметричного шифрования
5	Работа с локальным хранилищем сертификатов в ОС Windows
6	Установка и настройка СКЗИ КриптоПро CSP Работа с контейнерами закрытого ключа и сертификатами пользователя
7	Порядок развёртывания и настройки ПАК «Криптопро УЦ 2.0» с дополнительными службами штампов времени и актуальных статусов сертификатов
8	Установка и настройка VipNet Client
9	Практическое применение СКЗИ КриптоПро CSP и сертификатов для защиты сообщений электронной почты

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 6

№ п/п	Вопросы к экзамену
1.	Какие нормативные акты определяют порядок применения средств криптозащиты
2.	Требования, определяемые приказом ФСБ № 378
3.	Что определяют криптография и криптология
4.	Сущность крипто анализа
5.	Чем отличаются симметричные ключи шифрования от асимметричных
6.	Сформулировать понятие блочного и поточного шифрования
7.	Сформулировать основные требования к хэш-функциям по стойкости
8.	Алгоритмы электронной подписи
9.	Виды электронной подписи
10.	Открытый и закрытый ключи
11.	Сертификат ЭП
12.	Как работает электронная подпись
13.	Дискретная политика управления доступом в компьютерных системах
14.	Мандатная политика управления доступом в компьютерных системах
15.	Три основные задачи криптографии. Типы криптосистем
16.	Проблема аутентификации открытых ключей
17.	Удостоверяющие центры. Цифровые сертификаты.
18.	Система RSA и схема ЭЦП Рабина
19.	Требования к шифрам. Принцип Керхкоффа
20.	Классические шифры
21.	Хэш-функции: общие требования
22.	Контроль целостности и информации
23.	Алгоритмы защитного контрольного суммирования
24.	Протокол аутентификации RADIUS.
25.	Использование смарт-карт и USB-ключей с шифрованием
26.	Генерация ключевой пары
27.	Требования ФАПСИ к передаче информации по защищённым каналам связи
28.	Организация защищенных каналов связи
29.	Требования к физической защите помещений, где используются СКЗИ
30.	КриптоПро, назначение и область применения
31.	Организация системы управления ЭП
32.	Назначение и порядок использования VipNet Client
33.	Порядок установки и настройки сертификатов
34.	Регуляторика в криптографии
35.	Криптографические протоколы TSL/SSL
36.	Протоколы электронного голосования
37.	Протоколы электронных платежей
38.	Потоковые шифры
39.	Блочная система шифрования
40.	Определение шифра. Методы замены, перестановок, гаммирования

41.	Требования к ЭП
42.	Как происходит проверка сертификата открытого ключа
43.	Недостатки алгоритма DSA
44.	Сущность стеганографии
45.	Сущность квантовой криптографии
46.	Что понимается под криптографическим протоколом?
47.	Какой протокол одновременно решает задачи распределения ключей и аутентификации?
48.	Как может быть создан скрытый канал передачи данных в цифровых подписях? Можно ли для этих целей использовать электронную подпись RSA?
49.	Каковы методы противодействия созданию скрытого канала в электронных подписях?
50.	Какие практические задачи предполагают использование средств криптографической защиты информации?
51.	Каковы основные сетевые протоколы, использующие криптографические методы защиты информации?
52.	
53.	Каковы особенности использования криптографических методов защиты информации в системах электронного документооборота, банковских и финансовых информационных системах?
54.	Какие задачи решает код HMAC?
55.	Какую задачу решает вероятностное шифрование?
56.	Что понимается под семантической стойкостью? Какие криптосистемы обладают свойством семантической стойкости?
57.	Каков принцип работы смешанных (гибридных) схем шифрования? Чем обусловлено применение таких схем?
58.	Каковы основные причины ненадежности практических реализаций криптосистем?
59.	Каковы особенности программных и аппаратных средств криптографической защиты информации?
60.	Какие инструменты операционных систем Windows позволяют использовать криптографические функции для создания защищенных приложений?

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки
Экзамен (по накопительному рейтингу)	«отлично»	80-100 баллов
	«хорошо»	60-79 баллов
	«удовлетворительно»	40-59 баллов
	«неудовлетворительно»	0-39 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Ермакова А.Ю.	Криптографические методы защиты информации	Учебное пособие	2022	https://reader.lanbook.com/book/176563
2	Кушнир А.П.	Криптографические системы	Учебное пособие	2021	https://reader.lanbook.com/book/182424
3	Ушакова Н.Н.	Криптография	Практикум	2021	https://reader.lanbook.com/book/182517#23

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	С.Н. Никифоров	Шифрование данных	Учебное пособие	2022	https://reader.lanbook.com/book/206285#1

8.3. Перечень профессиональных баз данных и информационных справочных систем

- Securitylab.ru Адрес ресурса: https://www.securitylab.ru
- Информационная безопасность. Защита информации Адрес ресурса: http://all-ib.ru/
- Ассоциация по вопросам защиты информации BISA Адрес ресурса: http://bis-expert.ru

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф