КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Математические методы защиты информации» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры гуманитарных дисциплин и иностранных языков от 21 марта 2025 г., протокол № 7

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от «2» апреля 2025 г., протокол № 3.

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Цели определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по специальности подготовки «Компьютерная безопасность», в рамках которой преподается дисциплина.

Цель освоения дисциплины формирование системных представлений об информационной безопасности, знание федеральных законов по обеспечения информационной безопасности, обработки персональных данных, владение основными алгоритмами математики криптографии.

Задачи:

- научить студентов использовать в своей практической деятельности различные алгоритмы шифрования;
- ознакомить с компьютерными технологиями в области персональной и сетевой безопасности;
- привить студентам умения и навыки самостоятельного изучения специальной литературы по информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Математические методы защиты информации» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ПК-3.5		**Математические методы защиты информации** Администрирование в Linux	Системы противодействия компьютерным атакам Производственная практика, преддипломная практика

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся профессиональных компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ПК-3.5 Способен разрабатывать требования по защите, формированию политик безопасности компьютерных систем и сетей на основе менеджмента, аудита и оценки рисков информационной	ПК-3.5.1. Реализует формирование политик безопасности компьютерных систем	Знать: методы разработки и реализации политик безопасности компьютерных систем, принципы построения защищенных информационных инфраструктур, стандарты информационной безопасности и способы оценки рисков. Уметь: разрабатывать и внедрять политики безопасности компьютерной системы, оценивать риски угроз и обеспечивать защиту конфиденциальных данных, организовывать мероприятия по обеспечению соответствия стандартам информационной безопасности. Владеть: навыками проектирования и внедрения комплексных решений по защите компьютерных систем, методами анализа уязвимостей и мониторинга состояния безопасности инфраструктуры, инструментами управления доступом и защиты информации.
	ПК-3.5.2. Принимает решения о необходимости защиты информации, содержащейся в ИС	Знать: методы выявления объектов и субъектов информационной безопасности, критерии классификации уровней конфиденциальности информации, механизмы принятия решений относительно защиты информации в информационных системах. Уметь: анализировать угрозы и риски утечки или повреждения информации, определять необходимость защиты информации, содержащейся в информационных системах, формулировать требования к уровню защиты и механизмам контроля доступа. Владеть: навыками анализа и обоснования выбора методов и технологий защиты информации, принятием решений о применении конкретных мер защиты и контроле эффективности защитных мероприятий.
	ПК-3.5.3 Анализирует компьютерную систему с целью определения необходимого уровня защищенности и доверия на основе менеджмента, аудита и оценки рисков информационной	Знать: методики анализа и оценки рисков информационной безопасности, процедуры менеджмента информационной безопасности, инструменты и технологии аудита компьютерных систем, классификацию уровней защищённости и доверия. Уметь: проводить аудит информационной

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
	безопасности	безопасности компьютерной системы, выявлять потенциальные угрозы и уязвимости, определять необходимый уровень защищённости и доверия, формировать рекомендации по улучшению механизмов защиты. Владеть: навыками анализа компьютерных систем с точки зрения информационной безопасности, осуществления комплексной оценки рисков, принятия управленческих решений по повышению уровня защищённости и доверия на основе результатов аудита и анализа рисков.

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			7
1. Контактная работа обучающихся с преподавателем:		53	53
Аудиторные занятия, часов всего, в том числе:		52	52
• занятия лекционного типа		18	18
• занятия семинарского типа:		34	34
практические занятия		-	-
лабораторные занятия		34	34
в том числе занятия в форме практической подготовки		-	-
Консультация		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		55	55
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		20	20
- выполнение домашних заданий по практическим занятиям		20	20
- подготовка к зачету		7	7
Промежуточная аттестация: зачет		-	-
ИТОГО:	часов	108	108
общая трудоемкость	зач. ед.	3	3

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Математика криптографии.

Арифметика целых чисел; Модульная арифметика; Матрицы; Линейное сравнение; Поля Галуа; Простые числа - испытания простоты

Тема 2. Алгоритмы шифрования

Основы современных шифров; Стандарт шифрования с симметричным ключом (DES, AES); Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамаля, эллиптических кривых)

Тема 3. Безопасность информационных систем предприятия

Законодательство РФ в области защиты информации, обработки персональных данных, организации безопасности информационных систем на предприятии; Службы контроля исполнения законодательства РФ в области безопасности и алгоритмы взаимодействия с ними предприятия;

Организация безопасной информационной системы предприятия

Тема 4. Алгоритмы реализации электронно-цифровой подписи

Криптографические хэш-функции; Цифровая подпись; Установление подлинности объекта

Тема 5. Безопасность корпоративной сети

Безопасность на транспортном уровне; Безопасность на сетевом уровне

Тема 6. Безопасность в клиентско- серверных приложений

Организация защиты клиентско-серверного приложения; Безопасная аутентификация (API)

Тема 7. Методы защиты информации

Основные понятия и методы шифрования. Системы шифрования с открытым ключом.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)	Индикаторы достижения

		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	компетенций
1	Тема 1. Математика криптографии.	2	6/6	8	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
2	Тема 2. Алгоритмы шифрования	2	6/6	8	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
3	Тема 3. Безопасность информационных систем предприятия	2	6/6	8	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
4	Тема 4. Алгоритмы реализации электронно-цифровой подписи	2	6/6	8	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
5	Тема 5. Безопасность корпоративной сети	2	6/6	8	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
6	Тема 6. Безопасность в клиентско- серверных приложений	4	2/2	8	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
7	Тема 7. Методы защиты информации	4	2/2	7	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК-3.5.3
	Всего	**18**	**34/34**	**55**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
1.	Тема 1. Лабораторная работа № 1. Математика криптографии. Поиск чисел НОД	Ознакомление студентов с методами нахождения наибольшего общего делителя (НОД) двух целых чисел и закрепление практических навыков вычисления НОД для решения криптографических задач. Методы вычисления НОД:метод перебора делителей: алгоритм заключается в последовательном переборе всех возможных общих делителей меньшего из двух чисел и выборе максимального среди них. Алгоритм Евклида: используется принцип деления остатков. Для пары (a,b), где $a>b$, повторяем деление большего числа на меньшее, пока остаток не станет равным нулю. Последний ненулевой остаток является искомым НОД. Расширенный алгоритм Евклида: позволяет дополнительно находить коэффициенты линейного представления НОД, т.е. целые	6

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.) Очная форма обучения
		числа x и y такие, что $ax+by=\gcd(a,b)$. Используется для решения диофантовых уравнений и построения обратимых элементов в кольцах вычетов. Подробное изложение методов вычисления НОД. Примеры расчета НОД различными методами. Выводы о преимуществах каждого метода. Программную реализацию любого выбранного вами метода на Python.	
2.	Тема 2. Лабораторная работа № 2. Поля Галуа, Многочлены, Примитивность многочлена	Изучение свойств конечных полей Галуа, операций над элементами поля, примитивных многочленов и формирование практических навыков работы с ними. Основные понятия и обозначения: Поле Галуа: конечное поле с числом элементов p^n, где p — простое число, называется полем Галуа и обозначается GF(p^n). Если n=1, поле называют простым полем, примитивный элемент: Элемент поля, порождающий мультипликативную группу поля, называется примитивным элементом, простой неприводимый многочлен. Операции в полях Галуа: сложение и умножение.	6
3.	Тема 3. Лабораторная работа № 3. Безопасность информационных систем предприятия.	Практическое изучение механизмов защиты информационной инфраструктуры предприятий, освоение методик оценки рисков и разработка мер противодействия угрозам информационной безопасности. Информационная безопасность предприятия включает защиту конфиденциальных данных, предотвращение несанкционированного доступа, контроль целостности информации и обеспечение доступности ресурсов. Оценка риска включает выявление уязвимостей системы, определение вероятных угроз и оценку последствий атак. Изучение топологии локальной сети предприятия. Идентификация ключевых компонентов ИТ-инфраструктуры. Моделирование потенциальных киберугроз (DDoS атаки, фишинговые кампании, вирусы-шифровальщики и др.). Разработка сценария действий злоумышленника. Настройка межсетевых экранов (firewall) и антивирусных решений. Использование технологии виртуальных частных сетей (VPN) для удалённого доступа сотрудников.	6
4.	Тема 4. Лабораторная работа № 4. Алгоритмы реализации электронно цифровой подписи.	Изучить принципы функционирования электронных цифровых подписей (ЭЦП), освоить базовые алгоритмы их формирования и верификации, закрепить практические навыки разработки приложений, обеспечивающих надежную цифровую подпись документов. Электронная цифровая подпись (ЭЦП) используется для подтверждения подлинности документа, целостности передаваемых данных и ответственности отправителя за содержание информации. Основой большинства современных схем ЭЦП являются асимметричные криптографические алгоритмы, использующие ключи шифрования и дешифрования. Авторизация сообщений и подтверждение происхождения информации. Целостность данных: защита от изменения или искажения содержания.	6

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
		Ознакомление с основными принципами и свойствами ЭЦП. Изучение математической основы наиболее популярных алгоритмов цифровой подписи (RSA, DSA, ECDSA). Освоение процедуры генерации открытых и закрытых ключей для указанных алгоритмов. Рассмотрение форматов хранения и распространения сертификатов открытого ключа. Реализация процесса хеширования документа и создание цифровой подписи с использованием закрытого ключа. Запись формата подписи в файл и сохранение вместе с документом.	
5.	Тема 5. Лабораторная работа № 5. Безопасность корпоративной сети.	Освоение основ проектирования безопасной корпоративной сети, изучение методов защиты корпоративных информационных систем, обучение построению эффективной модели управления доступом и защиты каналов передачи данных. Проектирование надежной архитектуры корпоративной сети с применением соответствующих стандартов и технологий. Изучение методов защиты периметра сети, включая использование брандмауэров, IDS/IPS, VPN и прокси-серверов. Освоение методов контроля доступа и идентификации пользователей внутри корпоративной сети. Оценка угроз безопасности и выбор оптимальных мер защиты. Изучение требований безопасности при проектировании топологии корпоративной сети. Выбор оптимальной конфигурации аппаратных и программных компонентов. Настройка правил фильтрации и управления пакетами на уровне брандмауэра. Анализ возможностей использования NAT, DHCP и DNS-сервисов для повышения безопасности. Применение механизмов аутентификации и авторизации пользователей (LDAP, Kerberos, Radius). Интеграция сервисов единого входа (SSO).	6
6.	Тема 6. Лабораторная работа № 6. Безопасность в клиентско серверных приложений.	Изучение и применение методов обеспечения безопасности в клиентско-серверных системах, ознакомление с основными угрозами и способами их нейтрализации, приобретение навыков практической настройки защиты веб-приложений. Освоение базового инструментария и приемов защиты клиентских и серверных частей веб-приложений. Углубленное изучение методов защиты от инъекций SQL, XSS-атак, CSRF-атак и атак типа "перехват сессии". Изучение и реализация практик безопасного кодирования на стороне клиента и сервера. Оценка эффективности применяемых мер защиты и проведение тестов на проникновение.	2
7.	Тема 7. Лабораторная работа № 7. Решение Диофантовых уравнений, Китайская теорема об остатках	Изучение и практика решения линейных диофантовых уравнений и применения китайской теоремы об остатках для решения задач целочисленной арифметики. Научиться применять расширенный алгоритм Евклида для решения диофантовых уравнений. Овладеть техникой нахождения наименьших положительных решений систем сравнений с помощью китайской теоремы об остатках. Написать программу на выбранном языке	2

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
		программирования (например, Python или JavaScript), которая решает указанные типы задач автоматически. Подробное решение приведённых примеров вручную. Листинг написанной программы с пояснениями к каждому этапу. Результаты расчётов и анализ полученных решений. Выводы о целесообразности использования изученных методов в реальных задачах криптографии и компьютерной безопасности.	
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Математические методы защиты информации» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету с оценкой.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого

применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Код контролируемой компетенции - ПК-3.5

Зачетно-экзаменационные материалыдля промежуточной аттестации (зачет)

1. Криптоалгоритмы. Общие понятия.
2. Классификация шифров.
3. Классические шифры.
4. DES
5. AES
6. Ассиметричное шифрование. Общий подход. Односторонняя и криптографически- односторонняя функция. Общие требования.
7. RSA
8. El-gamal
9. Понятие хэш-алгоритмов. Общая структура и классификация.
10. SHA-512
11. Общие понятия электронной цифровой подписи. Функции и область применения.
12. Виды ЭЦП и схемы ЭЦП
13. Правовое обеспечение ЭЦП.
14. Удостоверяющие центры. Структура.
15. Цифровой сертификат. Жизненный цикл.
16. Общая схема протоколов ЭЦП.
17. Алгоритмы построения ЭЦП на основе RSA и El-gamal
18. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
19. Свойства информации. Угрозы информационной безопасности.
20. Атаки на информационную систему. Понятие и классификация.
21. Систем защиты от НСД.
22. Виды ЭЦП и схемы ЭЦП
23. Правовое обеспечение ЭЦП.
24. Удостоверяющие центры. Структура.
25. Цифровой сертификат. Жизненный цикл.
26. Общая схема протоколов ЭЦП.
27. Уровни защиты и классы защищенности систем защиты от НСД
28. Механизмы аутентификации пользователей
29. Терминология ФСТЭК защиты АС от НСД.
30. Государственное регулирование систем защиты от НСД. Реестры ФСТЭК и ФСБ России.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии оценочным материалам.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388- 9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 (дата обращения: 27.06.2023).;

2. Конституция Российской Федерации: Официальный текст с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года. Федеральные конституционные законы "О Государственном флаге Российской Федерации", "О Государственном гербе Российской Федерации", "О Государственном гимне Российской Федерации". - Москва : Норма : ИНФРА-М, 2024. - 160 с. - URL: https://znanium.ru/catalog/product/2134102 (дата обращения: 07.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-00156-358-7

3. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518441 (дата обращения: 27.06.2023).;

Дополнительная литература:

1. Илякова, И. Е. Коммерческая тайна: учебное пособие для вузов / И. Е. Илякова. — Москва: Издательство Юрайт, 2023. — 139 с. — (Высшее образование). — ISBN 978-5-534-14712-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520253 (дата обращения: 27.06.2023).;

2. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269 (дата обращения: 27.06.2023).

Электронные библиотечные системы (ЭБС) и электронные

образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения

обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Аудитория информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения:

персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____