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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 «Основы информационной безопасности» 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 естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

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.

К основным целям освоения дисциплины «Основы информационной безопасности» следует отнести:

-раскрытие сущности и значения информационной безопасности и методов защиты информации в практических задачах и их место в системе национальной безопасности;

-формирование у студентов научного мировоззрения, понимания важности научно обоснованных методов для решения профессиональных задач в области безопасности информационных технологий.

Основные задачи освоения дисциплины:

- анализ и построение эффективных вычислительных алгоритмов для решения овладение студентами понятийным аппаратом в области информационной безопасности и защиты информации; установление и раскрытие структуры угроз защищаемой информации;
- изучение базовых содержательных положений в области информационной безопасности и защиты информации; раскрытие современной доктрины информационной безопасности;
- раскрытие различных форм представления информации в проблемах обеспечения информационной безопасности;
- ознакомление с современными подходами к решению общей задачи – созданию комплексной(-ых) системы(-ем) защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» 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
ОПК-1	-	Основы информационной безопасности	Основы управления информационной безопасности Учебная практика, ознакомительная практика 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
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Демонстрирует умение оценивать роль информации и информационных технологий при решении задачи профессиональной деятельности	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности Владеет видами защищаемой информации, классификациями, навыками оценивания угроз информационной безопасности
	ОПК-1.2. Демонстрирует умение оценивать роль информационной безопасности при решении задачи профессиональной деятельности	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь классифицировать защищаемую

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности Владеет видами защищаемой информации, классификациями, навыками оценивания угроз информационной безопасности

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
			3
1. Контактная работа обучающихся с преподавателем:		5**3**	53
Аудиторные занятия, часов всего, в том числе:		52	52
• занятия лекционного типа		34	34
• занятия семинарского типа:		18	18
практические занятия		-	-
лабораторные занятия		18	18
в том числе занятия в форме практической подготовки		-	-
Иная контактная работа:		1	1
Контроль самостоятельной работы (КСР)		-	-
Промежуточная аттестация (ИКР)			
2. Самостоятельная работа студентов всего, в том числе		5**5**	55
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		40	40
- выполнение домашних заданий по практическим занятиям		-	-
- подготовка к зачету		15	15
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. Защита информации как объективная закономерность

эволюции постиндустриального общества.

Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности, основная и дополнительная литература. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Глобализация информационных отношений. Информационные технологии. Информационные ресурсы услуги. Объективная необходимость и общественная потребность в защите информации. Сущность защиты информации. Правовое регулирование вопросов защиты информации.

.

Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

Право на информацию в системе гражданских прав личности. Возможные ограничения. Массовая информация и информация ограниченного доступа. Неприкосновенность частной жизни, персональные данные. Виды тайн. Коммерческая тайна. Государственная тайна. Документированная информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности РФ. Информационные войны, информационное оружие. Доктрина информационной безопасности РФ.

Тема 3. Угрозы информационной безопасности в компьютерных системах.

Компьютерная система (КС) как объект защиты информации. Понятие угрозы информационной безопасности в КС. Классификация и общий анализ угроз информационной безопасности в КС. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Сбои и отказы. Общие сведения о кодах для обнаружения и исправления случайных ошибок. Система охраны объектов КС. Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Механизмы заражения компьютерными вирусами.

Тема 4. Общая характеристика средств и методов защиты информации

Эволюция концепции информационной безопасности в компьютерных системах. Реализация угроз информационной безопасности путём несанкционированного доступа. Модель поведения потенциального нарушителя Обобщённые модели систем защиты информации. Основные принципы обеспечения информационной безопасности в КС. Понятие комплексной системы защиты информации (КСЗИ).

Тема 5. Организационно- правовое обеспечение защиты

информации.

Общая характеристика организационного обеспечения защиты информации. Основные задачи службы безопасности предприятия. Организационные мероприятия, обеспечивающие защиту информации. Необходимость правового регулирования в области защиты информации. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности; международные и отечественные нормативные и руководящие документы.

Тема 6. Защита компьютерных систем от несанкционированного вмешательства.

Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования и исследования. Защита от несанкционированного изменения структуры КС в процессе эксплуатации. Контроль целостности программ и данных в процессе эксплуатации. Регистрация и контроль действий пользователей.

Тема 7. Криптографические методы защиты информации.

Основные понятия и этапы развития криптографии. Классификация криптографических средств. Основные методы шифрования. Шифрование методами замены и перестановки. Аналитические и аддитивные методы шифрования. Системы шифрования с открытым ключом.

Тема 8. Комплексная защита информации в компьютерных системах.

Концепция создания КСЗИ в КС. Технология разработки КСЗИ. Функционирование комплексных систем защиты информации. Аудит в защищенных КС. Организационная структура КСЗИ.

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 компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки	самос-тоятельная работа	
1	Тема 1. Защита информации как объективная закономерность эволюции постиндустриального общества.	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки	самос-тоятельная работа	
2	Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2
3	Тема 3. Угрозы информационной безопасности в компьютерных системах.	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2
4	Тема 4. Общая характеристика средств и методов защиты информации	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2
5	Тема 5. Организационно-правовое обеспечение защиты информации.	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2
6	Тема 6. Защита компьютерных систем от несанкционированного вмешательства.	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2
7	Тема 7. Криптографические методы защиты информации.	4	2/2	6	ОПК-1, ОПК-1.1, ОПК-1.2
8	Тема 8. Комплексная защита информации в компьютерных системах.	6	4/4	9,8	ОПК-1, ОПК-1.1, ОПК-1.2
	Всего	**34**	**18/18**	**51,8**	

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. Защита информации как объективная закономерность эволюции постиндустриального общества.	Лабораторная работа №1.1. Роль информации в современном мире. Лабораторная работа №1.2. Основные понятия в информационной безопасности.	2

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
2.	Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.	Лабораторная работа №2.1. Виды информации. Лабораторная работа №2.2. Доктрина информационной безопасности РФ	2
3.	Тема 3. Угрозы информационной безопасности в компьютерных системах.	Лабораторная работа №3.1. Классификация и общий анализ угроз информационной безопасности в КС. Лабораторная работа №3.2. Система охраны объектов КС.	2
4.	Тема 4. Общая характеристика средств и методов защиты информации	Лабораторная работа №4.1. Средства защиты информации в КС. Лабораторная работа №4.2. Методы защиты информации в КС.	2
5.	Тема 5. Организационно-правовое обеспечение защиты информации.	Лабораторная работа №5.1. Основные задачи службы безопасности предприятия. Лабораторная работа №5.2. Стандартизация в области обеспечения информационной безопасности.	2
6.	Тема 6. Защита компьютерных систем от несанкционированного вмешательства.	Лабораторная работа №6.1. Модели управления доступом к информации в КС. Лабораторная работа №6.2. Регистрация и контроль действий пользователей.	2
7.	Тема 7. Криптографические методы защиты информации.	Лабораторная работа №7.1. Классификация криптографических средств. Лабораторная работа №7.2. Аналитические и аддитивные методы шифрования.	2
8.	Тема 8. Комплексная защита информации в компьютерных системах.	Лабораторная работа №8.1. Технология разработки КСЗИ. Лабораторная работа №8.2. Организационная структура КСЗИ.	2
	Всего		**18**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Базы данных» 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.

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

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
3. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
4. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
5. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
6. Общая характеристика случайных угроз информационной безопасности в КС.
7. Общая характеристика преднамеренных угроз информационной

безопасности в КС.

8. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.

9. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.

10. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.

11. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.

12. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, и правообладателя информационных ресурсов.

13. Отечественное законодательство в области информации и защиты информации.

14. Ответственность за правонарушения при работе с компьютерными системами.

15. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.

16. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.

17. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.

18. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование. Технология RAID.

19. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.

20. Система охраны объектов КС.

21. Общая характеристика технических каналов утечки информации в КС.

22. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.

23. Средства противодействия подслушивания и дистанционному наблюдению.

24. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.

25. Идентификация и аутентификация субъектов доступа к ресурсам КС.

Парольные методы и оценка их эффективности. Биометрические методы.

26. Средства и методы разграничения доступа к ресурсам КС.

27. Защита программных средств КС от несанкционированного копирования и исследования.

28. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.

29. Общие понятия, история развития и классификация криптографических средств.

30. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.

31. Шифрование методом замены. Простая, полиалфавитная и многозначная замена.

32. Аналитические методы шифрования.

33. Шифрование методом гаммирования.

34. Отечественные и зарубежные стандарты шифрования.

35. Общая характеристика и классификация компьютерных вирусов.

36. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.

37. Средства, используемые для обнаружения компьютерных вирусов.

38. Профилактика заражения компьютерными вирусами.

39. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы полифаги. Эвристические анализаторы.

40. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.

41. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.

42. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.

43. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.

44. Основные технологические этапы разработки КСЗИ.

45. Средства моделирования, применяемые для оптимизации КСЗИ.

46. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.

47. Задачи, решаемые подсистемой аудита в составе защищенных КС.

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 с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Нестеров, С. А. Основы информационной безопасности : учебник / С. А. Нестеров. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 324 с. - URL: https://e.lanbook.com/book/370967 - Режим доступа: для авториз. пользователей. - ISBN 978-5- 507-49077-6. - Текст : электронный..

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. - Москва: Юрайт, 2023. - 325 с. - URL: https://urait.ru/bcode/511239. - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-03600-8. - Текст : электронный..

Дополнительная литература:

1. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2025. — 337 с. — (Высшее образование). — DOI 10.12737/1932260. - ISBN 978-5-16-018225-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2199796

2. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. – Москва: РГУП, 2025. - 220 с. – ISBN 978-5-00209-188-1. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2228306

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

1. Лицензионное программное обеспечение, в том числе отечественного производства:

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

2. 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).

– ЯндексБраузер, Google Crome (браузеры).

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

– NVDA (социально-информационный проект для людей с ограниченными возможностями по зрению, использующих бесплатную программу экранного доступа)

3. Профессиональные базы данных не используются.

4. 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 системе и электронной информационно-образовательной среде.

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.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, обеспечивающей доступ к сети Интернет и электронной информационно-образовательной среде.

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 №____