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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.05.01 Компьютерная безопасность

Специализация: «Разработка защищенного программного обеспечения»

Формы обучения: очная

Объем дисциплины:

в зачетных единицах: 9 з.е.

в академических часах: 324 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Рабочая программа по дисциплине «Методы и средства криптографической 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 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

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.

Задачи: формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области; знать: правовые основы защиты компьютерной информации, математические основы криптографии, стандарты, модели и методы шифрования.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства криптографической 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
ОПК-10	Криптографические протоколы Организация и правовое обеспечение информационной безопасности	Безопасные методы извлечения информации из сетевых источников	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-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Применяет в профессиональной деятельности знания об основных алгоритмах, используемых в криптографии, а также методы оценивания сложности таких алгоритмов	Знать: основные алгоритмы, используемые в криптографии, их принципы работы и области применения, а также методы оценки их сложности и стойкости. Уметь: применять эти знания для анализа и выбора оптимальных алгоритмов в зависимости от конкретных задач и условий профессиональной деятельности. Владеть: навыками практического использования криптографических алгоритмов и методами их адаптации к различным информационным системам.
	ОПК-10.3. Демонстрирует умения разработки криптографических протоколов и исследования их стойкости к различным атакам в составе средств защиты компьютерных систем	Знать: принципы разработки криптографических протоколов, включая их структуру, основные компоненты и методы обеспечения устойчивости к атакам. Уметь: разрабатывать криптографические протоколы, анализировать их эффективность и устойчивость к различным видам атак, а также адаптировать их под конкретные задачи защиты информации. Владеть: навыками исследования стойкости криптографических протоколов, тестирования их безопасности и применения на практике в составе комплексных средств защиты компьютерных систем.

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	
		9	А
1. Контактная работа обучающихся с преподавателем:	138	69	69
Аудиторные занятия, часов всего, в том числе:	136	68	68
• занятия лекционного типа	68	34	34
• занятия семинарского типа:	68	34	34

практические занятия		-	-	
лабораторные занятия		68	34	34
в том числе занятия в форме практической подготовки		-	-	-
Консультации		1	0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		1	0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		114	39	75
- подготовка курсовой работы		-	-	-
- проработка учебного (теоретического) материала		45	15	30
- выполнение домашних заданий по практическим занятиям		45	15	30
- подготовка к экзамену		24	9	15
Промежуточная аттестация: экзамен		72	36	36
ИТОГО: общая трудоемкость	часов	324		
	зач. ед.	9		

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

5.1. Содержание дисциплины

Тема 1. Встроенные средства обеспечени безопасности распространенных операционных систем и серверов различных сетевых протоколов.

Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов. Архитектура системы безопасности операционных систем.

Тема 2. Основы криптографической защиты информации в компьютерных системах и сетях

Управление ключами. Время жизни ключей. Виды ключевой информации. Распределение ключей. Сертификация ключей. Причины ненадежности криптосистем. Человеческий фактор. Особенности реализации. Типичные ошибки пользователей. Применение нестойких криптоалгоритмов (КА). Неправильное применение КА. Ошибки в реализации КА. Криптография как математическая наука vs криптография как инженерная дисциплина

Тема 3. Продвинутые технологии криптографической защиты данных в компьютерных системах и сетях

Криптография как часть системы обеспечения безопасности информации (ОБИ). Философия проектирования систем ОБИ. Противоборствующее окружение. Параноидальная модель. Модель информационного противоборства. Информационная безопасность государства. Программные средства скрытого информационного воздействия (ПССИВ). Виды ПССИВ. Компьютерные вирусы (КВ).

Тема 4. Стохастические методы защиты информации

Основы теории генераторов псевдослучайных чисел(ГПСЧ). Требования к качественным ГПСЧ. Классификация ГПСЧ, ориентированных на использование в задачах криптографической защиты информации. Структура ГПСЧ. Типы используемых нелинейных функций. Блочные и поточные ГПСЧ.ГПСЧ на основе односторонних функций. ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями. ГПСЧ И.А. Кулакова. Основы теории конечных полей. Структура конечного поля. Мультипликативная группа конечного поля. Поля Галуа вида GF(p),где p– простое Поля Галуа вида GF(2n), где n–натуральное. Реализация операций сложения и умножения в конечных полях. Вычисление мультипликативной инверсии. ГПСЧ, функционирующие в конечных полях. Детальное описание раундов KAAES-128 и Кузнечик. Многомерные КА. Построение ранцевой криптосистемы на основе использования вычислений в конечных полях. Криптосистема Шора-Ривеста.

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 (лабораторные работы)	самос-тоятельная работа	
Раздел 1. Основы защиты информации в операционных системах и сетях.					
1	Тема 1. Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.	16	16/16	26	ОПК-10, ОПК-10.1, ОПК-10.3
2	Тема 2. Основы криптографической защиты информации в компьютерных системах и сетях	16	16/16	26	ОПК-10, ОПК-10.1, ОПК-10.3
Раздел 2. Продвинутые методы защиты информации.					
3	Тема 3. Продвинутые технологии криптографической защиты данных в компьютерных системах и сетях	16	16/16	26	ОПК-10, ОПК-10.1, ОПК-10.3
4	Тема 4. Стохастические методы защиты информации	20	20/20	36	ОПК-10, ОПК-10.1, ОПК-10.3

№ 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 (лабораторные работы)	самос-тоятельная работа	
	Всего	**68**	**68/68**	**114**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
Раздел 1. Основы защиты информации в операционных системах и сетях.			
1.	Тема 1. Локальный администратор безопасности, центр аутентификации, диспетчер учетных записей, монитор безопасности. Механизм контроля доступа. Безопасность серверов SMB, RAS, IIS. Защищенные сетевые протоколы (SSL, TSL, IPsec и др.). Система аудита.	Локальный администратор безопасности, центр аутентификации, диспетчер учетных записей, монитор безопасности. Механизм контроля доступа. Безопасность серверов SMB, RAS, IIS. Защищенные сетевые протоколы (SSL, TSL, IPsec и др.). Система аудита.	16
2.	Тема 2. ГПСЧ, функционирующие в конечных полях. Криптографические основы блокчейн технологий. Блокчейн- системы системы первого и второго поколений. Криптосистема RSA, режим шифрования со	ГПСЧ, функционирующие в конечных полях. Криптографические основы блокчейн технологий. Блокчейн- системы системы первого и второго поколений. Криптосистема RSA, режим шифрования со сцеплением блоков. Криптосистема Шамира. Криптосистема Эль-Гамаля, электронная подпись Эль Гамаля.	16

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.) Очная форма обучения
	сцеплением блоков. Криптосистема Шамира. Криптосистема Эль-Гамаля, электронная подпись Эль Гамал		
Раздел 2. Продвинутые методы защиты информации.			
3.	Тема 3. Ранцевая криптосистема на основе вычислений в конечных полях. Построение ранцевой криптосистемы на основе использования вычислений в конечных полях Криптографические хеш-функции (ХФ). Построение ХФ на основе использования блочного шифра.	Ранцевая криптосистема на основе вычислений в конечных полях. Построение ранцевой криптосистемы на основе использования вычислений в конечных полях. Криптографические хеш-функции (ХФ). Построение ХФ на основе использования блочного шифра.	16
4.	Тема 4. Стохастические методы в парольных системах разграничения доступа. Одноразовые пароли. Вероятностное шифрование. Криптопротоколы Zero Knowledge Proofs. Logic Encryption. Теория кодирования. R-блоки.	Стохастические методы в парольных системах разграничения доступа. Одноразовые пароли. Вероятностное шифрование. Криптопротоколы Zero Knowledge Proofs. Logic Encryption.	20
	Всего		**68**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Методы и средства криптографической 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 экзамену.

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 (экзамен/зачет)

1. Основы защиты информации в операционных системах и сетях

1. Протокол классической ЭП. (ИОПК-10.1, ИОПК-10.3)
2. Атака на схему ЭП, основанная на парадоксе дней рождения. (ИОПК-10.1, ИОПК-10.3)
3. Симметричный протокол аутентификации удаленных абонентов

НидхемаШредера. (ИОПК-10.1, ИОПК-10.3)

4. Асимметричный протокол аутентификации удаленных абонентов ДиффиХеллмана. (ИОПК-10.1, ИОПК-10.3)

5. Протоколы разделения секрета. (ИОПК-10.1, ИОПК-10.3)

6. Протоколы доказательства с нулевым разглашением знаний. (ИОПК-10.1, ИОПК-10.3)

7. Схема Kerberos. (ИОПК-10.1, ИОПК-10.3)

8. Причины трудоемкости решения задач защиты информации. (ИОПК-10.1, ИОПК-10.3)

9. Примеры уязвимости IT-технологий. (ИОПК-10.1, ИОПК-10.3)

10. Источники угроз кибербезопасности. (ИОПК-10.1, ИОПК-10.3)

11. Ошибки, сделанные в области кибербезопасности в ближайшем прошлом. Пути исправления ситуации. (ИОПК-10.1, ИОПК-10.3)

12. Процессный подход к решению задач защиты информации (ЗИ). (ИОПК-10.1, ИОПК-10.3)

13. Стохастические методы ЗИ. (ИОПК-10.1, ИОПК-10.3)

14. Особенности криптографии как науки. Задачи ЗИ, решаемые криптографическими методами. (ИОПК-10.1, ИОПК-10.3)

15. Основы криптологии. Криптография и криптоанализ. Основные термины. Правило Керхгофса. Требования к качественному шифру. (ИОПК-10.1, ИОПК-10.3)

16. Методы оценки стойкости шифров. Полиномиальные и экспоненциальные алгоритмы. (ИОПК- 10.1, ИОПК-10.3)

17. Классификация шифров. (ИОПК-10.1, ИОПК-10.3)

18. Модель криптосистемы (КС) с секретным ключом. Основные проблемы. (ИОПК-10.1, ИОПК- 10.3)

19. Совершенно секретный шифр. (ИОПК-10.1, ИОПК-10.3

20. Схема гаммирования, ее свойства. (ИОПК-10.1, ИОПК-10.3)

21. Блочные и поточные шифры. (ИОПК-10.1, ИОПК-10.3)

22. S-блоки. SP-сеть. Сеть Фейстеля. Рассеивание и перемешивание информации. Основы дифференциального криптоанализа. (ИОПК-10.1, ИОПК-10.3)

23. Идея криптоалгоритма (КА) AES-128. Архитектура Квадрат. (ИОПК-10.1, ИОПК-10.3)

24. Идея КА Кузнечик. XSL-шифры. (ИОПК-10.1, ИОПК-10.3)

25. Режимы использования блочных шифров. (ИОПК-10.1, ИОПК-10.3)

26. Криптографические методы контроля целостности информации. (ИОПК-10.1, ИОПК-10.3)

27. Поточные шифры A5 и PIKE. (ИОПК-10.1, ИОПК-10.3)

28. Поточный шифр RC4. (ИОПК-10.1, ИОПК-10.3)

29. Хеш-функции, требования к качественной хеш-функции. (ИОПК-10.1, ИОПК-10.3)

30. Модель КС с открытым ключом. (ИОПК-10.1, ИОПК-10.3)

31. Односторонняя функция. Односторонняя функция с секретом. (ИОПК-10.1, ИОПК-10.3)

32. Криптосистема RSA. Пример. (ИОПК-10.1, ИОПК-10.3)

33. Ранцевая КС. Пример. (ИОПК-10.1, ИОПК-10.3)

34. Протокол выработки общего секретного ключа Диффи-Хеллмана. Пример. (ИОПК-10.1, ИОПК- 10.3)

35. Идея электронной подписи (ЭП). Пример. (ИОПК-10.1, ИОПК-10.3)

2. Продвинутые методы защиты информации

36. Электронные, цифровые и виртуальные деньги. (ИОПК-10.1, ИОПК-10.3)

37. Электронные платежные системы (ЭПС) как объект ЗИ. (ИОПК-10.1, ИОПК-10.3)

38. ЭПС на основе цифровых денег. Формат цифровой купюры. Задачи ЗИ, требующие решения. (ИОПК-10.1, ИОПК-10.3)

39. Слепая ЭП RSA. (ИОПК-10.1, ИОПК-10.3)

40. Централизованная ЭПС на основе цифровых денег. Основные транзакции. (ИОПК-10.1, ИОПК- 10.3)

41. Биткоин. Блокчейн. Публичный блокчейн. Как построить блокчейн у себя на ноутбуке или смартфоне. (ИОПК-10.1, ИОПК-10.3)

42. Алгоритм работы системы Биткоин. Формат транзакций. (ИОПК-10.1, ИОПК-10.3)

43. Механизмы консенсуса блокчейн-систем. (ИОПК-10.1, ИОПК-10.3)

44. Причины ненадежности криптосистем. (ИОПК-10.1, ИОПК-10.3)

45. Управление ключами. Человеческий фактор. Особенности конкретной реализации КА. (ИОПК- 10.1, ИОПК-10.3)

46. Парольные системы разграничения доступа. (ИОПК-10.1, ИОПК-10.3)

47. Методы ЗИ от активного противника. (ИОПК-10.1, ИОПК-10.3)

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. Торстейнсон, П. Криптография и безопасность в технологии .NET : руководство / П. Торстейнсон, Г. А. Ганеш ; перевод с англ. В. Д. Хорева под редакцией С. М. Молявко. - 5-е изд. (эл.). - Москва : Лаборатория знаний, 2024. - 482 с. - URL: https://e.lanbook.com/book/418025 (дата обращения:

17.01.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-93208-734- 3. - Текст : электронный.

2. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Юрайт, 2022. - 473 с. - URL: https://urait.ru/bcode/489242 (дата обращения: 26.01.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-12474 3. - Текст : электронный.

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2022. - 349 с. - URL: : https://urait.ru/bcode/489919 (дата обращения: 30.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-02883-6. - Текст : электронный.

Дополнительная литература:

1. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург : Лань, 2022. - 400 с. - URL: https://e.lanbook.com/book/210746 (дата обращения: 18.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-1116-0. - Текст : электронный.

2. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стереотипное. - Москва : Горячая линия-Телеком, 2017. - 230 с. - https://e.lanbook.com/book/111097. - Текст : электронный.

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. Лаборатория программно-аппаратных средств защиты информации

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

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - - 15, сетевое оборудование; стенды; коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей.

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 №____