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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Криптографические протоколы» 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 дисциплины «Криптографические протоколы» является формирование у студентов способность анализировать тенденции развития методов и средств криптографической защиты информации, в частности ознакомить с различными видами современных криптографических протоколов, стандартами в области криптографических протоколов.

Задачи:

- обучить студентов принципам работы основных протоколов;
- привить студентам навыки реализации криптографических протоколов;
- дать студентам представление об анализе стойкости протоколов к атакам.
- уметь построить криптопротокол обмена информацией с помощью встроенных библиотек,
- уметь построить программную реализацию существующих криптоалгоритмов средствами произвольного языка;

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические протоколы» 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».

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	ОПК-10.1. Применяет в профессиональной деятельности знания об основных алгоритмах, используемых в криптографии, а также методы оценивания сложности таких алгоритмов	Знать: современные подходы к организации сложных криптосистем; основные международные стандарты, регламентирующие применение криптографических методов защиты информации Уметь: оценивать стойкость выбранного алгоритма, учитывая возможные угрозы и компрометацию ключей; осуществлять расчеты и оценки временных затрат на выполнение операций шифрования и расшифровки. Владеть: навыками самостоятельного анализа характеристик и возможностей

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
профессиональной деятельности		современных криптографических протоколов;
	ОПК-10.2. Демонстрирует при решении задач профессиональной деятельности умение использовать основные преобразования симметричной и асимметричной криптографии и анализировать их криптостойкость к возможным компьютерным атака	Знать: основные принципы и алгоритмы симметричного и асимметричного шифрования, методы их применения, принципы построения криптосистем, а также типичные уязвимости и известные атаки на криптографические алгоритмы. Уметь: анализировать текущее состояние ИБ на предприятии с целью разработки требований к средствам криптографической защиты информации (СКЗИ) Владеть: практическим опытом использования распространенных криптографических алгоритмов и методов, такими как DES, AES, RSA, ECC; способностями оценивать эффективность выбранных криптографических методов и адаптировать их к требованиям информационной безопасности конкретной профессиональной деятельности.

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
		6
1. Контактная работа обучающихся с преподавателем:	35	35
Аудиторные занятия, часов всего, в том числе:	34	34
• занятия лекционного типа	16	16
• занятия семинарского типа:	18	18
практические занятия	18	18
лабораторные занятия	-	-
в том числе занятия в форме практической подготовки	-	-
Консультации	0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий	0,5	0,5
2. Самостоятельная работа студентов всего, в том числе	37	37
- подготовка курсовой работы	-	-
- проработка учебного (теоретического) материала	10	10
- выполнение домашних заданий по практическим занятиям	20	20
- подготовка к зачету	7	7
Промежуточная аттестация: зачет	-	-

ИТОГО:	часов	72	72
общая трудоемкость	зач. ед.	2	2

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

5.1. Содержание дисциплины

Тема 1. Поля объектов и проблема защиты информации.

Системы вычетов. НОД, функция Эйлера, основная теорема арифметики. Мультипликативная инверсия, расширенный алгоритм Евклида. М алая теорема Ферма, формула Эйлера, примитивный элемент поля. Решение сравнений первой степени. Китайская теорема об остатках. Алгоритмы проверки на простоту. Тест Миллера- Рабина. Задача факторизации числа. Эллиптические кривые.

Тема 2. Криптоалгоритмы.

Типы атак на криптосистемы. Понятие стойкости шифра по Шеннону. Совершенные шифры. Алгоритм Блюм-Блюм-Шуба. Регистр сдвига. М-последовательность, нелинейный усложнитель. Вихрь Мерсена. Тесты NIST. Тесты DIE HARD. Общие подходы к построению блочных симметричных шифров. Обратимые и необратимые операции, классификация блочных шифров. Шифры Фейстеля. Шифр DES. Шифр AES. SubBytes, AddRoundKey. Криптография в эллиптических кривых

Тема 3. Криптопротоколы

Понятие хэш-функции. Понятие коллизий. Понятие криптографически стойкой хэш функции, классификация. MD5. Sha-2 . Стрибог. Построение хэш функций на симметричных алгоритмах. Протоколы построения. Whirpool. ЭЦП. ГОСТ 34.10-2018.

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	

№ 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	
1	Тема 1. Математические основы криптологии.	6	8	12	ОПК-10, ОПК-10.1, ОПК-10.2
2	Тема 2. Криптоалгоритмы.	6	6	12	ОПК-10, ОПК-10.1, ОПК-10.2
3	Тема 3. Криптопротоколы	4	4	13	ОПК-10, ОПК-10.1, ОПК-10.2
	Всего	**16**	**18**	**37**	

6. Практические занятия

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
1.	Тема 1. Элементы теории чисел. Решение сравнений. Кольцо многочленов. Поля Галуа. NP-полные задачи теории чисел. Группы точек эллиптических кривых.	Элементы теории чисел делимость и простые числа , определение делимости, свойства, простые числа, решето Эратосфена, основная теорема арифметики, наибольший общий делитель (НОД) и наименьшее общее кратное (НОК), алгоритм Евклида (расширенный алгоритм Евклида), свойства НОД и НОК. Функция Эйлера. Определение и свойства функции Эйлера. Вычисление функции Эйлера. Основные понятия сравнений. Определение сравнения по модулю. Свойства сравнений. Линейные сравнений. Решение линейных сравнений. Теорема о существовании решений. Основные определения и операции. Основные понятия полей	8
2.	Тема 2. Симметричные шифры Ассиметричные шифры Применение шифров	Симметричные шифры (Шифры с секретным ключом**)**: общие принципы, определение и основные характеристики симметричных шифров, преимущества и недостатки симметричных шифров, классические симметричные шифры, Шифр Цезаря, шифр перестановки, шифр подстановки. Асимметричные шифры (Шифры с открытым ключом): общие принципы, определение и основные характеристики асимметричных шифров, открытый и закрытый ключи, принцип работы, преимущества и недостатки асимметричных шифров. Алгоритмы асимметричного шифрования. Применение шифров: безопасность веб-коммуникаций, SSL/TLS: протоколы шифрования для безопасной передачи данных в Интернете, HTTPS: безопасная версия HTTP. Защита электронной почты, PGP (Pretty Good Privacy) и S/MIME: шифрование и подпись	6

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
		электронной почты. Сравнение симметричных и асимметричных шифров.	
3.	Тема 3. ХЭШ/ЭЦП Распределение ключей Электронная подпись на основе шифрсистем с открытыми ключами. Электронные подписи на основе симметричных криптосистем.	Основные свойства хэш-функций. Определение и характеристики: односторонность, стойкость к коллизиям (первого и второго рода), лавинный эффект. Криптографические и некриптографические хэш-функции. Алгоритмы хэширования. Применение хэш-функций. 2. Электронная цифровая подпись (ЭЦП)	4
	Всего		**34**

7. Лабораторные работы

Лабораторные работы не предусмотрены

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Криптографические протоколы» 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 материалыдля промежуточной аттестации (экзамен/зачет)

1. Кольцо, поле.
2. Системы вычетов.
3. НОД, функция Эйлера, основная теорема арифметики.
4. Малая теорема Ферма, формула Эйлера, примитивный элемент поля.
5. Диофантовы уравнения. Решение простейших диофантовых уравнений 1 степени.
6. Решение сравнений первой степени.
7. Китайская теорема об остатках, решение системы сравнений.
8. Алгоритмы проверки на простоту. Вероятностные алгоритмы.
9. Тест Миллера-Рабина. Общий подход к проверке числа на простоту.
10. Задача факторизации числа, метод Ферма, методы Полларда.
11. Точки эллиптических кривых. Операции, группа точек.
12. Типы атак на криптосистемы.
13. Понятие стойкости шифра по Шеннону. Совершенные шифры. Классификация шифров.
14. Криптоалгоритмы и криптопротоколы.Классические шифры.
15. Представление данных и операции над ними в современных криптосистемах.
16. Алгоритм Блюм-Блюм-Шуба.
17. Регистр сдвига.
18. М-последовательность, нелинейный усложнитель.
19. Вихрь Мерсена.
20. Тесты NIST.
21. Тесты DIE HARD.
22. Общие подходы к построению блочных симметричных шифров.
23. Шифры Фейстеля.
24. Шифр DES. Параметры и общая структура.
25. Шифр DES. Расширение ключей.
26. Шифр DES. Уязвимости. TRIPLE DES.

27. Шифр AES. Параметры и общая структура.
28. Шифр AES. Структура раунда. SubBytes, AddRoundKey.
29. Криптография в эллиптических кривых.
30. Понятие хэш-функции. Понятие коллизий.
31. Понятие криптографически стойкой хэш функции, классификация Хэшей.
32. MD5.
33. Sha-2.
34. Стрибог
35. ЭЦП. Терминология. Общие принципы и протоколы применения.
36. ГОСТ 34.10-2018.

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 / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. - 4-еизд. - Москва : Лаборатория знаний, 2020. - 428 с. - URL: https://e.lanbook.com/book/151552 (дата обращения: 13.04.2022). - Режим доступа: для авториз. пользователей. - ISBN 978- 5-00101-700-4. - Текст : электронный.

2. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 456 с. - URL: https://e.lanbook.com/book/362942 (дата обращения: 19.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-48774-5. - Текст : электронный.

3. 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.

4. 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. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. - Санкт-Петербург : Лань, 2022. - 544 с. - URL: https://e.lanbook.com/book/193323 (дата обращения: 15.12.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-8589-5. - Текст : электронный.

2. Лапонина, О.Р. Криптографические основы безопасности : учебное пособие / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. - URL: https://biblioclub.ru/index.php?page=book&id=429092 (дата обращения: 04.03.2021).- Режим доступа: для авториз. пользователей. - ISBN 5-9556-00020-5. - 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, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа,

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, практических занятий, 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.

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 №____