Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.Т.Прохоренко

30 июня 2023 г.

Регистрационный № УД-12735/уч.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности первой ступени высшего образования:

1-98 01 01 Компьютерная безопасность (по направлениям)
Направления специальности:
1-98 01 01 - 01 Компьютерная безопасность (математические методы и программные системы)

2023 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01-2021, учебных планов: № Р 98-1-005/уч. от 23.07.2021 г., № Р 98-1-024/уч.ин. от 09.08.2021 г.

СОСТАВИТЕЛЬ:
С.В. Агиевич, доцент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТ:
Д.В. Васильев, заведующий отделом теории чисел и дискретной математики ГНУ «Институт математики НАН Беларуси», кандидат физико-математических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой математического моделирования и анализа данных факультета прикладной математики и информатики БГУ (протокол № 11 от 25 мая 2023 г.);

Научно-методическим Советом БГУ (протокол № 9 от 29 июня 2023 г.).

Заведующий кафедрой _____ В.И. Малюгин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Криптографические методы защиты информации обеспечивают конфиденциальность, контроль целостности и подлинности данных с помощью ключезависимых или бесключевых криптографических преобразований.

Учебная дисциплина «Криптографические методы» знакомит студентов с методами построения криптографических преобразований, а также методами оценки их надежности. Дисциплина дает представление об основных типах криптографических систем: блочных, поточных, криптосистемах с открытым ключом, систем электронной цифровой подписи, функций хэширования.

Изучаемые криптографические методы основываются на использовании объектов и применении методов широкого набора математических дисциплин: алгебры, теории чисел, теории вероятностей, математической статистики, теории информации, теории сложности вычислений.

Цели и задачи учебной дисциплины

Цели дисциплины «Криптографические методы»:

– изучение теоретических основ построения надежных криптографических преобразований;

– формирование навыков использования криптографических преобразований для построения систем защиты информации.

При изложении материала учебной дисциплины важно показать возможности использования конкретных криптографических методов при решении прикладных задач защиты информации.

Задачи дисциплины «Криптографические методы»:

– изучение криптосистем с секретным ключом (блочных и поточных шифров, систем имитозащиты);

– изучение функций хэширования;

– изучение базовых криптографических платформ с открытым ключом;

– изучение систем шифрования с открытым ключом и систем электронной цифровой подписи (ЭЦП);

– применение блочных и поточных криптосистем для решения практических задач в области защиты информации.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Криптографические методы» относится к модулю «Криптография» компонента учреждения высшего образования.

Связи с другими учебными дисциплинами

Основой для изучения учебной дисциплины «Криптографические методы» являются учебные дисциплины «Геометрия и алгебра», «Дискретная математика и математическая логика», «Теория вероятностей и

математическая статистика» государственного компонента, «Математический анализ», «Теория информации» компонента учреждения высшего образования. Сведения, излагаемые в учебной дисциплине «Криптографические методы» используются учебными дисциплинами «Теоретические основы информационной безопасности», «Программно-аппаратные и технические средства защиты информации» государственного компонента, а также при изучении ряда учебных дисциплин специальности.

Требования к компетенциям

Освоение учебной дисциплины «Криптографические методы» должно обеспечить формирование следующей с**пециализированной** компетенции:

СК-6 Разрабатывать и анализировать надежность блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи.

В результате освоения учебной дисциплины студент должен:

знать:

– методы построения надежных блочных и поточных криптосистем, функций хэширования, систем шифрования с открытым ключом и систем электронной цифровой подписи;

– задачи и основные методы криптоанализа;

– стандартные криптосистемы и правила их практического использования.

уметь:

– применять полученные знания для создания надежных систем защиты информации;

владеть:

– методами построения надежных криптосистем и функций хэширования;

– методами построения криптосистем с открытым ключом и систем электронной цифровой подписи;

– основными методами криптоанализа.

Структура учебной дисциплины

Дисциплина изучается в 5 и 6 семестре. Всего на освоение учебной дисциплины «Криптографические методы» отведено:

– для очной формы получения высшего образования – 314 часов, в том числе 140 аудиторных часов, из них: лекции – 70 часов, лабораторные занятия – 62 часа, УСР – 8 часов.

5 семестр: 72 аудиторных часа, в том числе лекции – 36 часов, лабораторные занятия – 32 часа, УСР – 4 часа.

6 семестр: 68 часов, в том числе лекции – 34 часа, лабораторные занятия – 30 часов, УСР – 4 часа.

Трудоемкость учебной дисциплины составляет 9 зачетных единиц (5 семестр – 6 зачётных единиц, 6 семестр – 3 зачётные единицы).

Форма промежуточной аттестации – экзамен (5 и 6 семестры).

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел I. Криптография с секретным ключом

Тема 1.1. Введение в криптографию. История криптографии. Абоненты, коммуникации и угрозы. Криптосистема.

Тема 1.2. Классические криптосистемы. Шифр сдвига. Аффинный шифр. Шифр простой замены. Шифр Хилла. Шифр перестановки. Шифр Виженера.

Тема 1.3. Задачи криптоанализа. Атаки. Частотные атаки. Криптоанализ шифра Виженера.

Тема 1.4. Элементы теории Шеннона. Модель противника. Совершенные криптосистемы. Энтропия, условная энтропия, удельная энтропия. Расстояние единственности.

Тема 1.5. Элементы теории конечных полей. Подполя и расширения полей. Характеристика поля. Существование конечного поля. Единственность конечного поля. Соотношения между подполями. Функция «след». Мультипликативная группа конечного поля.

Тема 1.6. Блочные криптосистемы. Блочно-итерационные криптосистемы. SP-криптосистемы. AES. Использование инволютивных подстановок. Криптосистемы Фейстеля.

Тема 1.7. Атаки на блочные криптосистемы. Атака «грубой силой». Баланс «время-память». Таблицы разностей. Разностная атака. Конструкция Нюберг. Линейные аппроксимации. Линейная атака.

Тема 1.8. Режимы шифрования. Режим простой замены. Режим счетчика. Режим сцепления обработки. Режим гаммирования с обратной связью. Имитозащита.

Тема 1.9. Поточные криптосистемы. Поточные криптосистемы. Конечные автоматы. Регистры сдвига с линейной обратной связью.

Тема 1.10. Свойства линейных рекуррентных последовательностей. Порядок многочлена. Примитивные многочлены. Период л.р.п. Минимальный многочлен. Постулаты Голомба.

Тема 1.11. Усложнение линейных рекуррентных последовательностей. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Криптосистема A5/1. Сжимающий и самосжимающий генератор. Линейная сложность. Корреляционный криптоанализ. Корреляционно-иммунные функции.

Раздел II. Криптография с открытым ключом

Тема 2.1. Протокол Диффи-Хеллмана. Идея криптографии с открытым ключом. Головоломки Меркля. Протокол Диффи-Хеллмана. Реализация протокола Диффи-Хеллмана.

Тема 2.2. Элементы теории сложности вычислений. Вычислительные задачи. Машина Тьюринга. Разрешимые и неразрешимые задачи. Ресурсы. Вероятностные машины. Алгоритмы Монте-Карло и Лас-Вегас. Классы сложности. Язык *PRIMES*.

Тема 2.3. Односторонние функции. Односторонние функции. Функции с лазейкой. Шифрование с открытым ключом. Системы ЭЦП.

Тема 2.4. Инфраструктура открытых ключей. Сертификаты открытых ключей. Инфраструктура открытых ключей. Инфраструктура РБ.

Тема 2.5. Криптосистема RSA. Криптосистема RSA. RSA и факторизация. Арифметика больших чисел. Алгоритм Евклида. Расширенный алгоритм Евклида. Возведение в степень. Китайская система сравнений. Оптимизация RSA.

Тема 2.6. Генерация простых чисел. Генерация простых. Распределение простых. Тест Ферма. Тест Рабина–Миллера. Построение простых.

Тема 2.7. Функции хэширования. Определения и использование. Задачи криптоанализа. Блочно-итерационные функции хэширования. Конструкция Дамгарда. Функция хэширования СТБ 34.101.31.

Тема 2.8. Атака «дней рождения». Базовая атака. Среднее время ожидания коллизии. Модифицированная атака. Алгоритм Брента.

Тема 2.9. Электронные цифровые подписи. ЭЦП Эль-Гамаля. Модификации ЭЦП Эль-Гамаля. Метод Монтгомери. ЭЦП Шнорра. ЭЦП СТБ 1176.2.

Тема 2.10. Факторизация и дискретное логарифмирование. Задача факторизации. Алгоритм $p-1$. ρ-метод факторизации. Выбор модуля RSA. Задача логарифмирования. Метод больших-малых шагов. ρ-метод логарифмирования. Метод Поллига-Хеллмана. λ-метод.

Тема 2.11. Субэкспоненциальные алгоритмы факторизации и логарифмирования. Метод Диксона. Квадратичное решето. Индекс-метод.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

№п/п	Название раздела, темы	Количество часов				Количество часов УСР	Форма контроля знаний
		Аудиторные					
		Лекции	Практические занятия	Лабораторные занятия	Иное		
1	**Криптография с секретным ключом**	36		32		4	
1.1	Введение в криптографию	2		2			Опрос
1.2	Классические криптосистемы	4		4			Защита реферата
1.3	Задачи криптоанализа	2		2			Опрос
1.4	Элементы теории Шеннона	4		2			Контрольная работа
1.5	Элементы теории конечных полей	4		4			Коллок-виум
1.6	Блочные криптосистемы	4		4			Решение задач. Отчет по заданию с устной защитой
1.7	Атаки на блочные криптосистемы	4		2		2	Опрос
1.8	Режимы шифрования	2		4			Отчет по заданию с устной защитой
1.9	Поточные криптосистемы	2		2			Опрос
1.10	Свойства линейных рекуррентных последовательностей	4		4			Решение задач. Отчет по заданию с устной защитой
1.11	Усложнение линейных рекуррентных последовательностей	4		2		2	Контрольная работа
2	**Криптография с открытым ключом**	34		30		4	
2.1	Протокол Диффи–Хеллмана	2		4			Решение задач
2.2	Элементы теории сложности вычислений	4		2			Коллок-виум
2.3	Односторонние функции	2		2			Опрос

2.4	Инфраструктура открытых ключей	2		2		2	Опрос
2.5	Криптосистема RSA	6		4			Контрольная работа
2.6	Генерация простых чисел	2		4			Решение задач
2.7	Функции хэширования	4		4			Защита реферата
2.8	Атака «дней рождения»	2		2			Опрос
2.9	Электронные цифровые подписи	4		4			Решение задач. Отчет по заданию с устной защитой
2.10	Факторизация и дискретное логарифмирование	4		2			Контрольная работа
2.11	Субэкспоненциальные алгоритмы факторизации и логарифмирования	2				2	Опрос
ИТОГО		**70**		**62**		**8**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Введение в теоретико-числовые методы криптографии: учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2024. — 396 с. — ISBN 978-5-507-47610-7. - URL: https://e.lanbook.com/book/397286.

2. Криптология: учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.]; БГУ. – 2-е изд., пересмотр. – Минск: БГУ, 2023. – 511 с. – URL: https://elib.bsu.by/handle/123456789/309839.

Перечень дополнительной литературы

1. Основы криптографии / Алферов А. П. [и др.]. – Москва : Гелиос АРБ, 2001. – 480 с.

2. Столлингс В. Криптография и защита сетей: принципы и практика (2 изд.) / В. Столлингс – М: Вильямс, 2001. – 669 с.

3. Харин, Ю. С. Компьютерный практикум по математическим методам защиты информации / Ю. С. Харин, С. В Агиевич – Минск, БГУ, 2001. – 190 с.

4. Menezes, A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone – CRC Press, 1996. – 816 p.

5. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source code in C / B. Schneier – John Wiley & Sons, 1996. – 675 p.

6. Stinson, D. Cryptography. Theory and Practice / D. Stinson – N.Y. CRC, 1995 – 434 p.

Информационно-методическое обеспечение дисциплины доступно студентам в виде онлайн-курса, размещенного в интернете по адресу https://apmi.bsu.by/resources/cm.

Примерный перечень тем для коллоквиумов

1) Элементы теории конечных полей.
2) Элементы теории сложности вычислений.

Рекомендуемая тематика контрольных работ

1) Контрольная работа №1. *Классические криптосистемы. Задачи криптоанализа. Совершенные криптосистемы. Расстояние единственности.*
2) Контрольная работа №2. *Блочные криптосистемы. Использование инволютивных подстановок. Криптосистемы Фейстеля. Поточные криптосистемы. Линейные рекуррентные последовательности.*
3) Контрольная работа №3. *Протокол Диффи–Хеллмана. RSA. Простые числа.*

4) Контрольная работа №4. *Функции хэширования. ЭЦП ЭльГамаля. ЭЦП Шнорра. Метод Монтгомери.*

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

На лекционных занятиях по дисциплине «Криптографические методы» рекомендуется особое внимание обращать на установлении связей между теоретическим темами дисциплины и использованием, изучаемых методов и алгоритмов для решения практических задач защиты информации.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

– устная форма: устные опросы по текущим темам;

– письменная форма: контрольная работа, коллоквиум по нескольким теоретическим темам дисциплины;

– устно-письменная форма: отчёты по домашним практическим упражнениям и лабораторным работам с их устной защитой.

Формой промежуточной аттестации по дисциплине «Криптографические методы» учебным планом предусмотрены экзамены в пятом и шестом семестрах.

При формировании итоговой отметки используется рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения.

Отметка текущей аттестации рассчитывается как среднеарифметическая величина отметок по всем формам текущего контроля знаний по учебной дисциплине, т.е. отметки за письменную контрольную работу, отметки за коллоквиум, отметок за отчёты по домашним практическим упражнениям и лабораторным работам.

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей аттестации (рейтинговой системы оценки знаний) и отметки на экзамене с учётом их весовых коэффициентов. Вес отметки по текущей аттестации составляет 40 %, отметки на экзамене – 60 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Управляемая самостоятельная работа (УСР) студентов – это самостоятельная работа, выполняемая по заданию и при методическом руководстве преподавателя, а также контролируемая преподавателем на определенном этапе обучения. Целью УСР является целенаправленное обучение студентов основным навыкам и умению индивидуальной самостоятельной работы.

На освоение учебного материала в рамках УСР для дисциплины «Криптографические методы» отводится 8 аудиторных часов по четырем

следующим темам в соответствии с учебно-методической картой дисциплины.

Тема 1.7. Атаки на блочные криптосистемы (2 ч)

*Перечень вопросов для углубленного самостоятельного изучения***:**

- линейные аппроксимации нелинейных преобразований;
- линейный криптоанализ.

Рекомендуемая литература: [2].

Форма контроля – устный опрос.

Тема 1.11. Усложнение линейных рекуррентных последовательностей (2 ч)

*Перечень вопросов для углубленного самостоятельного изучения***:**

- линейная сложность;
- корреляционный криптоанализ;
- корреляционно-иммунные функции.

Рекомендуемая литература: [2].

Тема 2.4. Инфраструктура открытых ключей (2 ч)

Перечень вопросов для углубленного самостоятельного изучения:

- протоколы управление сертификатами открытых ключей;
- криптографическая инфраструктура РБ.

Рекомендуемая литература: [2].

Форма контроля – устный опрос.

Тема 2.11. Субэкспоненциальные алгоритмы факторизации и логарифмирования (2 ч)

Перечень вопросов для углубленного самостоятельного изучения:

- методы решета;
- рекорды факторизации и логарифмирования.

Рекомендуемая литература: [1, 2].

Форма контроля – устный опрос.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется практико-ориентированный подход.

Практико-ориентированный подход предполагает:

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы обучающихся

Студенты самостоятельно выполняют следующую работу:

– осуществляют углубленное изучение тем 1.7, 1.11, 2.4 и 2.11 с использованием рекомендуемой литературы;

– выполняют лабораторные задания с использованием различных языков программирования;

– готовят отчёт с результатами проведённых исследований в соответствии с установленными требования;

– работают над устранением указанных при проверке отчётов недостатков.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) курсов лекций, учебно-методических материалов по основным темам дисциплины. Материалы размещены по адресу https://apmi.bsu.by/resources/cm.

Примерный перечень вопросов к экзаменам

1. История криптологии.
2. Коммуникации и угрозы.
3. Криптосистема.
4. Классические криптосистемы: алфавит.
5. Шифр сдвига.
6. Аффинный шифр (обращение по модулю, функция Эйлера).
7. Шифр простой замены.
8. Шифр Хилла.
9. Шифр перестановки.
10. Шифр Виженера.
11. Задачи криптоанализа: атаки.
12. Частотные атаки.
13. Криптоанализ шифра Виженера.
14. Элементы теории Шеннона: модель противника.
15. Совершенная криптосистема.
16. Энтропия.
17. Расстояние единственности.
18. Конечные поля.
19. Многочлены.
20. Поля из p^n элементов.
21. Подгруппы.
22. Подполя и расширения полей.
23. Характеристика поля.
24. Лемма о степени суммы и разности.

25. Мультипликативная группа.
26. Функция «след».
27. Блочно-итерационные криптосистемы.
28. Представления двоичных слов.
29. SP-криптосистемы.
30. τ-инволютивные подстановки.
31. Криптосистемы Фейстеля.
32. AES.
33. Инверсные *S*-блоки.
34. Стратегия «широкого следа».
35. Атака «грубой силой».
36. Простые соотношения.
37. Баланс «время – память».
38. Разностная атака.
39. Режим простой замены.
40. Режимы шифрования.
41. Имитозащита.
42. Поточные криптосистемы.
43. Конечные автоматы.
44. РСЛОС.
45. РСЛОС и функция «след».
46. Период л.р.п..
47. Порядок многочлена.
48. Постулаты Голомба.
49. Минимальный многочлен.
50. Генераторы на базе РСЛОС.
51. Линейная сложность.
52. Протокол Диффи – Хеллмана.
53. Атака «противник посередине».
54. Реализация протокола Диффи – Хеллмана.
55. Вычислительные задачи.
56. Машина Тьюринга.
57. Разрешимые и неразрешимые задачи.
58. Вычислительные ресурсы.
59. Вероятностные машины.
60. Алгоритмы Лас-Вегас и Монте-Карло.
61. Сложностные классы.
62. Язык PRIMES.
63. Односторонние функции.
64. Функции с лазейкой.
65. Шифрование с открытым ключом.
66. Системы ЭЦП.
67. Сертификаты открытых ключей.
68. Инфраструктура открытых ключей.

69. Инфраструктура РБ.
70. Криптосистема RSA.
71. RSA и факторизация.
72. Реализация RSA: арифметика больших чисел.
73. Алгоритм Евклида.
74. Расширенный алгоритм Евклида.
75. Возведение в степень.
76. Китайская система сравнений.
77. Оптимизация RSA.
78. Генерация простых.
79. Распределение простых.
80. Тест Ферма.
81. Тест Рабина – Миллера.
82. Построение простых.
83. Функции хэширования: определение и использование.
84. Функции хэширования: задачи криптоанализа.
85. Блочно-итерационные функции хэширования.
86. Конструкция Дамгарда.
87. Атака «дней рождения».
88. Модифицированная атака «дней рождения».
89. Алгоритм Брента.
90. ЭЦП ЭльГамаля.
91. Стойкость ЭЦП ЭльГамаля.
92. Модификации ЭЦП ЭльГамаля.
93. Метод Монтгомери.
94. ЭЦП Шнорра.
95. СТБ 1176.2-99.
96. Задача факторизации.
97. Алгоритм $p - 1$.
98. Факторизация: ρ-метод.
99. Выбор модуля RSA.
100. Дискретное логарифмирование: метод больших-малых шагов.
101. Дискретное логарифмирование: ρ-метод.
102. Метод Поллига – Хеллмана.
103. Дискретное логарифмирование: λ-метод.
104. Метод Диксона.
105. Квадратичное решето.
106. Индекс-метод.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Теоретичес-кие основы информацион-ной безопасности	Технологий программиро-вания	нет	Оставить содержание учебной дисциплины без изменения (протокол № 11 от 25 мая 2023 г.)
Программно-аппаратные и технические средства защиты информации	Технологий программиро-вания	нет	Оставить содержание учебной дисциплины без изменения (протокол № 11 от 25 мая 2023 г.)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры математического моделирования и анализа данных (протокол № __ от 20___ г.).

Заведующий кафедрой
доктор эконом. наук, доцент _____ В.И.Малюгин
(ученая степень, звание) (подпись) (И.О. Фамилия)

УТВЕРЖДАЮ
Декан факультета
канд. физ.-мат. наук, доцент _____ Ю.Л.Орлович
(ученая степень, звание) (подпись) (И.О. Фамилия)