БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.Г. Прохоренко
«08» июля 2022 г.

Регистрационный № УД – 11265/уч.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-31 03 09 Компьютерная математика и системный анализ

2022 г.

Учебная программа составлена на основе ОСВО 1-31 03 09-2021, утвержден постановлением № 98 от 25.04.2022, учебных планов: № G31-1-019/уч. от 25.05.2021, №G31-1-004/уч. ин. от 31.05.2021., № G31-1-222/уч. от 22.03.2022 г., №G31-1-226 уч. ин. от 27.05.2022 г.

СОСТАВИТЕЛИ:

Д.Н. Чергинец, доцент кафедры дифференциальных уравнений и системного анализа Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТЫ:

В.В. Цегельник, профессор кафедры высшей математики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор физико-математических наук, профессор.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа Белорусского государственного университета
(протокол № 16 от 25.05.2022);

Научно-методическим советом БГУ
(протокол № 6 от 29.06.2022).

Зав. кафедрой дифференциальных уравнений
и системного анализа  Л.Л. Голубева

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины – обучение студентов основным математическим понятиям и алгоритмам, которые используются в криптографии.

Задачи учебной дисциплины:

1. формировать у студентов глубокое понимание математических объектов, используемых в криптографии;
2. развивать способности реализации алгоритмов на языках программирования Wolfram Language и Python;
3. познакомить студентов с основными понятиями теории сложности вычислений;
4. обучить студентов основным объектам криптографии: криптосистемам, функциям хеширования, электронным цифровым подписям.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина является дисциплиной компонента учреждения высшего образования и входит в состав **модуля** «Компьютерное моделирование».

При изучении дисциплины «Математические основы защиты информации» используются знания, умения и навыки, полученные при изучении дисциплин «Компьютерная математика», «Алгебра и теория чисел», «Математический анализ». Приобретенные при изучении данной дисциплины компетенции пригодятся студенту при изучении дисциплины «Теория помехоустойчивого кодирования».

Требования к компетенциям

Освоение учебной дисциплины «Математические основы защиты информации» должно обеспечить формирование следующей **специализированной компетенции:**

СК-8. Осуществлять математическое и компьютерное моделирование для прикладных исследований.

В результате освоения учебной дисциплины студент должен:

знать:

- основные симметричные и асимметричные криптосистемы;
- стандарты электронной цифровой подписи;
- типовые криптографические протоколы;

уметь:

- корректно применять основные криптосистемы;
- формировать электронную цифровую подпись под электронным документом;

владеть:

- методами шифрования и передачи информации;
- методами обеспечения целостности и аутентификации информации.

Структура учебной дисциплины

Дисциплина изучается в 3 и 4 семестре. Всего на изучение учебной дисциплины «Математические основы защиты информации» отведено: 120 часов, в том числе 70 аудиторных часов, из них: лекции – 34 часа, лабораторные занятия – 28 часов, управляемая самостоятельная работа – 8 часов.

Форма получения высшего образования очная (дневная).

На третий семестр отводится 36 аудиторных часов, из которых: лекции – 18 часов, лабораторные занятия – 14 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины – нет зачетных единиц.

Форма текущей аттестации – без текущей аттестации.

На четвертый семестр отводится 34 аудиторных часа, из которых: лекции – 16 часов, лабораторные занятия – 14 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма текущей аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Введение в теорию сложности вычислений и основные алгоритмы теории чисел.

Полиномиальный и экспоненциальный алгоритмы. Алгоритм Евклида, расширенный алгоритм Евклида, возведение в степень в кольце классов вычетов. Вычисление обратных элементов в мультипликативной группе кольца классов вычетов.

Тема 2. Алгебраические уравнения в кольце вычетов.

Уравнение первой степени. Китайская теорема об остатках. Алгоритм Гаусса. Алгоритм Гарнера. Квадратичный вычет. Квадратичный невычет. Символ Лежандра. Символ Якоби. Вычисление символа Якоби при помощи квадратичного закона взаимности Гаусса. Алгоритм Тонелли-Шенкса. Квадратное уравнения в случае составного модуля. Алгоритм Лас-Вегаса.

Тема 3. Функции хеширования.

Функции хеширования. Коллизии. Хранение паролей. Хранение и поиск данных. Хеш-таблицы. Контроль целостности данных. Имитовставка. Функция формирования ключа. Криптографические функции хеширования. Стандарт SHA-3.

Тема 4. Генерация простых чисел.

Метод пробных делений. Малая теорема Ферма. Псевдопростые числа. Числа Кармайкла. Свидетели простоты. Вероятностный тест на простоту Миллера-Рабина. Теорема Диемитко. Детерминированный полиномиальный алгоритм проверки простоты чисел. Детерминированный и вероятностный алгоритмы. Алгоритм Монте-Карло.

Тема 5. Факторизация чисел. Экспоненциальные алгоритмы.

Метод пробных делений. Парадокс дней рождения. Ро-метод Полларда. (p-1)-алгоритм Полларда. Классы P и NP.

Тема 6. Криптосистемы с открытым ключом.

Парадокс симметричных криптосистем. Криптосистемы с открытым ключом. Односторонние функции. Односторонние функции с лазейкой. Криптосистема RSA. Эквивалентность задачи разложения модуля на множители и вычисления функции Эйлера. Эквивалентность задачи разложения модуля на множители и вычисления секретной экспоненты.

Тема 7. Применение криптосистемы RSA.

Стандарт PKCS. Применение китайской теоремы об остатках при дешифровании. Дополнение сообщений. Алгоритм дополнения PKCS. Функция генерации маски. Алгоритм дополнения OAEP. Перевод текста в числа и обратно.

Тема 8. Факторизация чисел. Субэкспоненциальные алгоритмы.

Факторизация Ферма и факторные базы. Метод Диксона. Факторизация методом квадратичного решета. Субэкспоненциальный алгоритм.

Тема 9. Цепные дроби.

Цепная дробь. Конечная цепная дробь. k-ая подходящая дробь. Рекуррентная формула вычисления подходящей дроби. Сходимость последовательности подходящих дробей. Цепная дробь как обобщение алгоритма Евклида. Взаимно однозначное соответствие между действительными числами и цепными дробями. Атака Винера.

Тема 10. Дискретное логарифмирование.

Определение дискретного логарифма. Образующий элемент. Алгоритм больших и малых шагов. Алгоритм Полига-Хеллмана.

Тема 11. Дискретное логарифмирование. Субэкспоненциальные алгоритмы.

Алгоритм Адлемана нахождения дискретного логарифма.

Тема 12. Электронная цифровая подпись.

Электронная цифровая подпись. Электронная цифровая подпись Эль-Гамаля. Электронная цифровая подпись Шнорра.

Тема 13. Эллиптические кривые.

Определение эллиптической кривой. Дискриминант. Пересечение эллиптической кривой и прямой. Группа точек эллиптической кривой. Цикличность группы точек эллиптической кривой. Порядок группы точек эллиптической кривой. Алгоритм вычисления произведения натурального числа и точки эллиптической кривой. Дискретное логарифмирование на эллиптической кривой. Алгоритм больших и малых шагов. Алгоритм Полига-Хеллмана. Криптография с использованием эллиптических кривых.

Тема 14. Решетки.

Определение решетки. Базис решетки. Определитель решетки. Ортогонализация Грама-Шмидта. LLL-приведенный базис и его свойства. LLL-алгоритм.

Тема 15. Нахождение малых корней полиномов в кольце вычетов.

Норма многочлена. Теорема об эквивалентности малых корней полиномов в кольце вычетов и в кольце целых чисел. Алгоритм вычисления малых корней в кольце вычетов.

Тема 16. Атаки на криптосистему RSA при помощи решеток.

Атака Хастада. Результант многочленов. Атака Франклина-Райтера.

Тема 17. Криптографические протоколы.

Схемы обязательств. Обмен ключами Диффи-Хеллмана. Доказательства с нулевым разглашением. Разделение секрета.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования с применением электронных средств обучения (ДО)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
	Математические основы защиты информации	**34**			**28**		**8**	
1.	Введение в теорию сложности вычислений и основные алгоритмы теории чисел	2			2			Электронный отчет с устной защитой, устный опрос
2.	Алгебраические уравнения в кольце вычетов	2			2		2	Электронный отчет с устной защитой, устный опрос
3.	Функции хеширования	2			2			Электронный отчет с устной защитой, устный опрос
4.	Генерация простых чисел	2			2			Электронный отчет с устной защитой, устный опрос
5.	Факторизация чисел. Экспоненциальные алгоритмы	2			2			Электронный отчет с устной защитой, устный опрос
6.	Криптосистемы с открытым ключом	2			2			Электронный отчет с устной защитой, устный опрос
7.	Применение криптосистемы RSA	2					2	Электронный отчет с устной защитой, устный опрос
8.	Факторизация чисел. Субэкспоненциальные алгоритмы	2			2			Электронный отчет с устной защитой, устный опрос

9.	Цепные дроби	2						Устный опрос
10.	Дискретное логарифмирование	2			2		2	Электронный отчет с устной защитой, устный опрос
11.	Дискретное логарифмирование. Субэкспоненциальные алгоритмы.	2			2			Электронный отчет с устной защитой, устный опрос
12.	Электронная цифровая подпись	2			2			Электронный отчет с устной защитой, устный опрос
13.	Эллиптические кривые	4			2		2	Электронный отчет с устной защитой, устный опрос
14.	Решетки	2			2			Электронный отчет с устной защитой, устный опрос
15.	Нахождение малых корней полиномов в кольце вычетов	1			2			Электронный отчет с устной защитой, устный опрос
16.	Атаки на криптосистему RSA при помощи решеток	1			2			Электронный отчет с устной защитой, устный опрос
17.	Криптографические протоколы	2						Устный опрос

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Авдошин, С.М. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. М. Авдошин, А. А. Набебин; [науч. ред. В. А. Захаров]. - Москва: ДМК Пресс, 2017.
2. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167921
3. Криптология: учебник для студ учреждений высш. образования по математическим и техн. спец. / [авт.: Ю. С. Харин и др.]; БГУ. - Минск: БГУ, 2013.
4. Харин, Ю.С. Математические основы теории информации: учеб. пособие для студ. учреждений высш. образования по спец. "Компьютерная безопасность", "Прикладная криптография" / Ю. С. Харин, И. А. Бодягин, Е. В. Вечерко; БГУ. - Минск: БГУ, 2018. http://elib.bsu.by/handle/123456789/201511.

Перечень дополнительной литературы

1. Алферов, А.П. Основы криптографии. Учебное пособие, 2-е изд., испр. и доп. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.
2. Андресс, Д. Защита данных. От авторизации до аудита / Джейсон Андресс; [пер. с англ. С. Черников]. - Санкт-Петербург; Москва; Минск: Питер, 2021.
3. Болотов, А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 328 с.
4. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.
5. Введение в криптографию / Под ред. В.В. Ященко. – М.: МЦНМО-ЧеРоб, 1998, 271 с.
6. Дориченко, С.А. 25 этюдов о шифрах / С.А. Дориченко, В.В. Ященко. – М.: ТЕИС, 1994. – 69 с.
7. Кнут, Д. Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е издание. / Д. Кнут. – М.-СПб.-Киев: Вильямс, 2003.
8. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: Научное изд-во ТВП, 2001. – 254 с.
9. Математические и компьютерные основы криптологии: Учеб. пособие для студ. матем. и инженерно-техн. спец. вузов / Ю. С. Харин, В. И.

Берник, Г. В. Матвеев, С. В. Агиевич. - Минск: Новое знание, 2003. - 381с.
10. Маховенко Е.Б. Теоретико-числовые методы в криптографии / Е.Б. Маховенко. – М.: Гелиос АРВ, 2006. – 320с.
11. Нестеренко, Ю.В. Теория чисел: учебник для студ. высш. учеб. заведений / Ю.В. Нестеренко. – М.: Издательский центр «Академия», 2008. – 272 с.
12. Омассон, Ж. О криптографии всерьез: практическое введение в современное шифрование / Жан-Филипп Омассон; [пер. с англ. А. А. Слинкина]. - Москва: ДМК Пресс, 2022.
13. Острик, В.В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые / В.В. Острик, М.А. Цфасман. – М.: МЦНМОб 2001. – 48 с.
14. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.
15. Саломаа, А. Криптография с открытым ключом / – М.: Мир, 1996. – 320 с.
16. Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 525 с.
17. Тилборг, Х.К.А. Основы криптологии / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.
18. Фергюсон, Н. Практическая криптография = Practical Cryptography / Нильс Фергюсон, Брюс Шнайер; [пер. с англ. Н. Н. Селиной ; под ред. А. В. Журавлева]. - Москва; Санкт-Петербург; Киев: Диалектика, 2005. - 422с.
19. Харин, Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Минск: БГУ, 1999. – 319 с.
20. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации: Учеб. пособие для студ. матем. и инженерно-технических спец. вузов / Ю.С.Харин, С.В.Агиевич. - Мн. : БГУ, 2001. - 190с.
21. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. 2-е издание / Брюс Шнайер. — М.: Триумф, 2002. — 816 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Контроль работы студента проходит в форме опроса на лекциях, во время устной защиты отчета по лабораторным работам. Оценка за ответы на лекциях и лабораторных занятиях включает в себя полноту ответа, наличие аргументов, примеров из практики, глубину понимания терминов, используемых студентом при ответе на вопросы. Во время защиты отчета по лабораторным работам ценится знание студентом теоретических сведений, полученных на лекции, эффективность работы реализованных алгоритмов.

Формой текущей аттестации по дисциплине «Математические основы защиты информации» учебным планом предусмотрен экзамен в четвертом семестре.

Экзамен по дисциплине проходит в устной форме.

При формировании итоговой отметки используется рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в итоговую отметку:

Формирование отметки за текущую успеваемость:

– электронный отчет с устной защитой – 60 %;

– опросы на лекциях и лабораторных занятиях – 40 %.

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей успеваемости и экзаменационной отметки с учетом их весовых коэффициентов. Вес отметки по текущей успеваемости составляет 40 %, экзаменационной отметки – 60 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 2. Алгебраические уравнения в кольце вычетов. (2ч.)

Китайская теорема об остатках. Алгоритм Гаусса. Алгоритм Гарнера.

Реализовать в Mathematica или Python алгоритмы Гаусса и Гарнера. Сравнить практически скорость работы данных алгоритмов. Для каждого алгоритма найти количество арифметических операций, необходимых для выполнения всех шагов алгоритма. Являются ли данные алгоритмы полиномиальными?

Целью данного задания является выработка у студента навыков оценки сложности алгоритма.

Форма контроля – электронный отчет с устной защитой.

Тема 7. Применение криптосистемы RSA. (2ч.)

Стандарт PKCS. Применение китайской теоремы об остатках при дешифровании. Дополнение сообщений. Алгоритм дополнения PKCS. Функция генерации маски. Алгоритм дополнения OAEP.

Реализовать класс PublicKey с методами шифрования, использующими PKCS и OAEP. Объект класса PublicKey генерируется по открытой экспоненте e и модулю n.

Реализовать класс PrivateKey с методами дешифрования, использующими PKCS и OAEP, с методом генерации открытого ключа в виде класса PublicKey. Дешифрование должно проходить при помощи Китайской теоремы об остатках.

Форма контроля – электронный отчет с устной защитой.

Тема 10. Дискретное логарифмирование. (2ч.)

Определение дискретного логарифма. Образующий элемент. Алгоритм Полига-Хеллмана.

Реализовать алгоритм Полига-Хеллмана. Посчитать количество арифметических операций для данного алгоритма. Является ли он полиномиальным? От каких свойств модуля зависит скорость работы алгоритма? При разработке криптосистем, стойкость которых основана на проблеме вычисления дискретного логарифма, каким свойством должен обладать модуль?

Форма контроля – электронный отчет с устной защитой.

Тема 13. Эллиптические кривые. (2ч.)

Алгоритм больших и малых шагов и алгоритм Полига-Хеллмана для нахождения дискретного логарифма в группе точек на эллиптической кривой.

Реализовать алгоритм Полига-Хеллмана и алгоритм больших и малых шагов для эллиптической кривой. Посчитать количество арифметических операций для данных алгоритмов. Являются ли они полиномиальными? От каких свойств эллиптической кривой зависит скорость работы алгоритмов? При разработке криптосистем, стойкость которых основана на проблеме вычисления дискретного логарифма в группе точек над эллиптической кривой, какими свойствами должна обладать эллиптическая кривая?

Форма контроля – электронный отчет с устной защитой.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется ***эвристический подход***, который предполагает демонстрацию многообразия решений большинства профессиональных задач и жизненных проблем.

При организации образовательного процесса используется ***практико-ориентированный подход,*** который предполагает освоение содержания через решения практических задач.

При организации образовательного процесса ***используются методы и приемы развития критического мышления,*** которые представляют собой систему, формирующую навыки работы с информацией в процессе чтения и письма; понимании информации как отправного, а не конечного пункта критического мышления.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине рекомендовано разместить на образовательном портале или сайте кафедры учебно-методические материалы: методические указания к лабораторным занятиям, вопросы для подготовки к экзамену, перечень рекомендуемой литературы, информационных ресурсов.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы УВО по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)[1]
Теория помехоустойчивого кодирования	Кафедра дифференциальных уравнений и системного анализа	нет	Вносить изменения не требуется (протокол № 16 от 25.05.2022)

[1] При наличии предложений об изменениях в содержании учебной программы УВО.

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
_____ (протокол № ____ от _____ 200___ г.)
(название кафедры)

Заведующая кафедрой
кандидат физ.-мат. наук, доцент _____ Л.Л. Голубева
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета
доктор физ.-мат. наук, доцент _____ С.М. Босяков
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)