Учреждение образования
«Белорусский государственный педагогический университет
имени Максима Танка»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ С.И. Василец
_____ 2022 г.

Регистрационный № УД-24-1-77-2022 уч.

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ В ЗАЩИТЕ ИНФОРМАЦИИ

**Учебная программа учреждения высшего образования
по учебной дисциплине для специальности**

1-02 05 01 Математика и информатика

.

Учебная программа составлена на основе Образовательного стандарта высшего образования первая ступень специальность 1-02 05 01 Математика и информатика, утвержденного 20.04.2022, протокол №85); учебного плана специальности 1-02 05 01 Математика и информатика; типовой учебной программы (___.___.202__, № ТД-_____/ тип.)

СОСТАВИТЕЛЬ:
А.А.Черняк, профессор кафедры математики и методики преподавания математики учреждения образования «Белорусский государственный педагогический университет имени Максима Танка», доктор физико-математических наук, доцент

РЕЦЕНЗЕНТЫ:
О.М.Михалкович, доцент кафедры физики и методики преподавания физики БГПУ им. М.Танка, кандидат физико-математических наук;
Ж.А.Черняк, доцент кафедры физических и математических основ информатики Белорусской государственной академии связи, кандидат физико-математических наук, доцент

СОГЛАСОВАНО:
Директор ГУО «Средняя школа № 191 г. Минска» _____
Ю.И.Пинчук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой математики и методики преподавания математики
(протокол № 4 от 11.11.2022);

Заведующий кафедрой _____ Н.В.Гриб

Научно-методическим советом учреждения образования «Белорусский государственный педагогический университет имени Максима Танка» (протокол №2 от 20.12.2022).

Оформление учебной программы и сопровождающих ее материалов действующим требованиям Министерства образования Республики Беларусь соответствует

Методист учебно-методического отдела
_____ Е.В.Тихонова

Директор библиотеки
_____ Н.П.Сятковская

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа по дисциплине «Алгебраические методы в защите информации» разработана для учреждений высшего образования Республики Беларусь в соответствии с требованиями образовательного стандарта высшего образования I ступени по специальности 1-02 05 01 «Математика и информатика».

Проникновение информационных технологий во все отрасли человеческой деятельности становится определяющим в тенденциях развития современной фундаментальной науки. В частности, прогресс в вычислительной технике не только привел к возникновению новых направлений математики, но и стимулировал фундаментальные исследования в тех классических разделах алгебры, теории чисел и алгебраической геометрии (группы и поля, модульная арифметика, эллиптические кривые над конечным полями, булева алгебра и т.д.), которые еще недавно считались абстрактными и оторванными от практики.

Поэтому дисциплина «Алгебраические методы в защите информации» – логическое завершение дисциплин «Теория множеств и логика высказываний», «Алгебра многочленов и расширения полей», «Алгебраические структуры и теория чисел», «Аналитическая геометрия», поскольку является основным мотивирующим фактором для изучения студентами педагогическим специальностей таких разделов абстрактной алгебры, как теория групп, расширения полей, конечномерные векторные и линейные пространства, алгебра многочленов над конечными полями.

Цель учебной дисциплины - развитие способностей, навыков и умений увязывать абстрактные идеи и методы высшей алгебры с конкретными задачами защиты и безопасности информации.

Задачи *дисциплины*:

- на базе теории групп, полей и алгебры многочленов изучить математические принципы построения криптографических систем (стандарт AES, криптосистемы с открытым ключом и функции с замком, криптосистема RSA, рюкзачные криптосистемы)
- на базе теории линейных пространств над конечными полями изучить методологию создания эффективных кодов (линейные коды, совершенные коды Хэмминга, циклические коды),

В результате изучения учебной дисциплины студент должен
***знать*:**

- классические криптосистемы;
- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- основные задачи теории кодирования;

- эффективные коды.

уметь:

- конструировать полиномиальные алгоритмы дешифрования блочно-подстановочных шрифтов;
- воспроизводить основные этапы алгоритма шифрования Рейндола и пользоваться этапными ключами алгоритма AES-128;
- определять основные характеристики кодов;
- генерировать оптимальные коды.

***владеть*:**

- навыками шифрования и дешифрования криптосистемы с открытым ключом;
- навыками шифрования и дешифрования криптосистемы RSA;
- основными алгоритмами распознавания и устранения ошибок при передачи информации.

Освоение учебной дисциплины «Алгебраические методы защиты информации» должно обеспечить формирование **базовой профессиональной компетенции БПК-16:** Применять теорию многочленов для решения прикладных задач в педагогической практике

В рамках образовательного процесса по учебной дисциплине «Алгебраические методы в защите информации» студент должен приобрести не только теоретические и практические знания, умения и навыки по специальности, но и развить свой ценностно-личностный, духовный потенциал, сформировать качества патриота и гражданина, готового к активному участию в экономической, производственной, социально-культурной и общественной жизни страны.

На изучение учебной дисциплины отводится 108 часов, из них аудиторных – 52 часов (лекции – 20 часов, практические занятия – 32 часа).

Рекомендуемая форма текущей аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Криптосистемы.

1.1. Криптосистемы с закрытым ключом: общие понятия.

Подстановочные шифры; блочные методы шифрования; аффинный шифр над кольцом Z_n; аффинное шифрование над конечными полями.

1.2. Продвинутый стандарт шифрования.

Общая идея алгоритма шифрования AES; этапы и три раунда шифрования; эффективный алгоритм дешифрования.

1.3. Полиномиальные алгоритмы.

Общая и индивидуальная задачи; входная длина задачи и временная сложность алгоритма; полиномиальные и экспоненциальные алгоритмы.

1.4. Криптосистемы с открытым ключом: общие понятия. Криптосистема RSA.

Ключи шифрования и дешифрования; функции с замком и алгоритмически трудноразрешимые задачи; Криптосистема Ривеста, Шамира и Айдельмана.

1.5. Рюкзачная криптосистема.

Задача о рюкзаке; быстрорастущие наборы чисел; функции с замком рюкзачной криптосистемы.

Раздел 2. Теория кодирования.

2.1. Корректирующие коды: основные понятия.

Главная проблема теории кодирования; совершенные коды.

2.2. Линейные коды.

Генератором кода; матрицы контроля четности; расстояние линейного кода; коды Хэмминга; исправление ошибок линейных кодов.

2.3. Циклические коды.

Кодовые многочлены; генератор кодовых многочленов и многочлен контроля.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА
(дневная форма получения образования)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов		Самостоятельная работа студентов	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		Лекции	Практические занятия				
1	2	3	4	5	6	7	8
2 семестр							
1	**Криптосистемы**	**11**	**17**	**30**		[3,4,6]	
1.1	Криптосистемы с закрытым ключом: общие понятия Подстановочные шифры; блочные методы шифрования; аффинный шифр над кольцом Z_n; аффинное шифрование над конечными полями	3	5	15	Раздаточные материалы		Практический тест. Отчет о проделанной самостоятельной работе
1.2	**Продвинутый стандарт шифрования**	2	4		Раздаточные материалы, ресурсный центр БГПУ		Проверочная самостоятельная

	Общая идея алгоритма шифрования AES; этапы и три раунда шифрования; эффективный алгоритм дешифрования.						работа
1.3	**Полиномиальные алгоритмы** Общая и индивидуальная задачи; входная длина задачи и временная сложность алгоритма; полиномиальные и экспоненциальные алгоритмы.	2	1	15	Учебное пособие [5]		Отчет о проделанной самостоятельной работе
1.4	**Криптосистемы с открытым ключом: общие понятия. Криптосистема RSA** Ключи шифрования и дешифрования; функции с замком и алгоритмически трудноразрешимые задачи; Криптосистема Ривеста, Шамира и Айдельмана.	2	3		Учебные пособия [3,4,6]		Проверочная самостоятельная работа
1.5	**Рюкзачная криптосистема** Задача о рюкзаке; быстрорастущие наборы чисел; функции с замком рюкзачной криптосистемы.	2	4		Раздаточные материалы, ресурсный центр БГПУ		Практический тест

2	**Теория кодирования**	**9**	**15**	**26**		[1,2,7,8]	
2.1	**Корректирующие коды: основные понятия** Главная проблема теории кодирования; совершенные коды.	2	3				Устный опрос
2.2	**Линейные коды** Генератором кода; матрицы контроля четности; расстояние линейного кода; коды Хэмминга; исправление ошибок линейных кодов.	4	8		Методические пособия [1,2,7,8]		Устный опрос
2.3	**Циклические коды** Кодовые многочлены; генератор кодовых многочленов и многочлен контроля.	3	4	26	Методические пособия [1,2,7,8]		Устный опрос Отчет о проделанной самостоятельной работе
	Итого:	**20**	**32**	**56**			Зачет

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Митюхин, А. И. Элементы алгебры для теории кодирования: математические основы кодирования информации корректирующими кодами [Электронный ресурс] / А. И. Митюхин // Репозиторий БГУИР. – Режим доступа: https://libeldoc.bsuir.by/handle/123456789/10389. – Дата доступа: 22.11.2022.

Дополнительная литература

1. Баричев, С. Г. Основы современной криптографии : учеб. курс / С. Г. Баричев, Р. Е Серов, В. В. Гончаров. – М. : Горячая линия-Телеком, 2002. – 175 с.

2. Берлекэмп, Э. Алгебраическая теория кодирования / Э. Берлекэмп. – М.: Мир, 1971. – 480 с.

3. Зуев, Ю. А. Современная дискретная математика в задачах и решениях: от перечислительной комбинаторики до криптографии XXI века : более 700 задач с решениями / Ю. А. Зуев. – М. : URSS, 2019. – 304 с.

4. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – М. : ТВП, 2001. – 254 с.

5. Коробейников, А. Г. Математические основы криптологии : учеб. пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб : С.-Петерб. нац. исслед. ун-т информ. технологий, механики и оптики, 2002. – 106 с.

6. Молдовян, А. А. Криптография / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. – СПб. : Лань, 2001. – 224 с.

7. Применко, Э. А. Алгебраические основы криптографии / Э. А. Применко. – М. : URSS, 2022. – 288 с.

РЕКОМЕНДУЕМЫЕ ФОРМЫ И МЕТОДЫ ОБУЧЕНИЯ

Основными методами обучения, отвечающими целям учебной дисциплины, являются: методы проблемного обучения (проблемное изложение, частично-поисковый и исследовательский методы). В процессе реализации учебной программы особое место должна занимать организация учебно-исследовательской работы студентов. Эта работа должна органично включаться в образовательный процесс в сочетании со всеми видами учебных занятий.

Рекомендуется проведение практических занятий на базе систем компьютерной математики, что призвано повысить эффективность учебного процесса, а также проиллюстрировать студентам преимущества использования современных информационных технологий в учебном процессе.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Каждая тема программы позволяет организовывать творческую самостоятельную работу студентов, которая будет содействовать становлению преподавателя-исследователя, владеющего значительным творческим потенциалом. Рекомендуем следующие темы для организации самостоятельной работы студентов:

- аффинный шифр Хилла;
- определение полиномиально эквивалентных алгоритмов; NP-трудные задачи;
- понятия о классах P и NP распознавательных задач; структура класса NP;
- BCH коды (циклические коды с генератором из кольца многочленов над конечным полем по модулю $x^n - 1$);
- коды Рида-Соломона;
- декодирование в BCH кодах.

Контроль за самостоятельной работой студентов предполагается проводить на еженедельных консультациях и коллоквиумах.

ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА

№ /п	Название темы раздела	Кол-во часов на СРС	Задание	Форма выполнения
1	Аффинный шифр Хилла	10	[5,6,9]	Решение индивидуальных контрольных примеров
2.	Определение полиномиально эквивалентных алгоритмов; NP-трудные задачи	10	[8,9]	Самостоятельный разбор основных понятий
3.	Понятия о классах P и NP распознавательных задач; структура класса NP	10	[10]	Рассмотрение конкретных распознавательных задач из классов P и NP
4.	BCH коды (циклические коды с генератором из кольца многочленов над конечным полем по модулю $x^n - 1$)	10	[1,2,7,8]	Самостоятельный разбор основных теорем
5.	Коды Рида-Соломона	10	[1,2,7,8]	Решение индивидуальных контрольных примеров
6.	Декодирование в BCH кодах	6	[1,2,7,8]	Решение индивидуальных контрольных примеров

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ

Рекомендуется проведение одного коллоквиума по второму разделу программы для подготовки к устной части экзамена.

С целью текущего контроля предусматривается проведение двух контрольных работ – по одной по каждому из двух последних разделов.

Для контроля и самоконтроля знаний и умений студентов по отдельным темам или разделам представляется целесообразным использование тестовых технологий.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Подстановочные шифры; блочные методы шифрования.
2. Аффинный шифр над кольцом Z_n.
3. Аффинное шифрование над конечными полями.
4. Общая идея алгоритма шифрования AES; этапы и три раунда шифрования.
5. Эффективный алгоритм дешифрования.
6. Временная сложность алгоритма.
7. Полиномиальные и экспоненциальные алгоритмы.
8. Ключи шифрования и дешифрования; функции с замком и алгоритмически трудноразрешимые задачи.
9. Криптосистема Ривеста, Шамира и Айдельмана.
10. Задача о рюкзаке; быстрорастущие наборы чисел.
11. Функции с замком рюкзачной криптосистемы.
12. Корректирующие коды: основные понятия.
13. Главная проблема теории кодирования.
14. Совершенные коды.
15. Генератором кода; матрицы контроля четности.
16. Расстояние линейного кода.
17. Коды Хэмминга.
18. Исправление ошибок линейных кодов.
19. Кодовые многочлены.
20. Генератор кодовых многочленов и многочлен контроля.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

по учебной дисциплине «Алгебраические методы в защите информации»

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
1	2	3	4
Теория множеств и логика высказываний	Кафедра математики и методики преподавния математики	С содержанием данной учебной дисциплины согласуются, замечаний и предложений нет	Протокол № 4 от 11.11.2022
Алгебра многочленов и расширения полей	Кафедра математики и методики преподавния математики	С содержанием данной учебной дисциплины согласуются, замечаний и предложений нет	Протокол № 4 от 11.11.2022
Алгебраические структуры и теория чисел	Кафедра математики и методики преподавния математики	С содержанием данной учебной дисциплины согласуются, замечаний и предложений нет	Протокол № 4 от 11.11.2022
Аналитическая геометрия	Кафедра математики и методики преподавния математики	С содержанием данной учебной дисциплины согласуются, замечаний и предложений нет	Протокол № 4 от 11.11.2022