Учреждение образования
«Белорусский государственный педагогический университет
имени Максима Танка»

УТВЕРЖДАЮ
Проректор по учебной работе БГПУ
_____ Зеленкевич В.М.
_____
Регистрационный № УД-24-1-130/2018 уч.

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ В КРИПТОГРАФИИ И ТЕОРИИ КОДИРОВАНИЯ

**Учебная программа учреждения высшего образования
по учебной дисциплине (по выбору студента) для специальности:
1-02 05 01 Математика и информатика**

2018 г.

Учебная программа составлена на основе Образовательного стандарта высшего образования первая ступень специальность 1-02 05 01 Математика и информатика (ОСВО 1-02 05 01 – 2013) и Учебного плана специальности 1-02 05 01 Математика и информатика (регистрационный № 152 – 2013/у от 25. 07. 2013 г.)

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:
З.Н.Примичева, доцент кафедры высшей математики учреждения образования «Белорусского государственного университета информатики и радиоэлектроники», кандидат физико-математических наук, доцент;
Ю.А.Быкадоров, доцент кафедры информатики и методики преподавания информатикт учреждения образования «Белорусский государственный педагогический университет имени Максима Танка», кандидат физико-математических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и методики преподавания математики
(протокол № 13 от 29.05.2018)

Заведующий кафедрой _____И.Н.Гуло

Советом физико–математического факультета
(протокол № 12 от 27.06.2018 г.)

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

Методист учебно-методического отдела БГПУ

_____ С.А.Стародуб

Ответственный за редакцию: Черняк А.А.
Ответственный за выпуск: Черняк А.А.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Цели и задачи учебной дисциплины

Программа дисциплины по выбору студента «Алгебраические методы в криптографии и теории кодирования» составлена для студентов физико-математического факультета в соответствии с требованиями образовательного стандарта высшего образования специальности 1-02 05 01 Математика и информатика.

Цели *дисциплины*:

- сформировать теоретическую базу и инструментарий для изучения многочленов над конечными полями, играющих ключевую роль в теории защиты информации.

– изучить основные алгебраические идеи и подходы, необходимые для понимания 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),

Задачи *дисциплины:*

– освоение основных понятий теории конечных групп и линейных пространств над конечными полями, утверждений и методов их обоснования;

– развитие способностей увязывать абстрактные идеи и методы высшей высшей алгебры с конкретными задачами современной информатики;

– формирование алгебраических умений и навыков, необходимые для успешного изучения других математических дисциплин и современных проблем защиты и безопасности информации.

2. Место учебной дисциплины в учебном процессе и ее связь с другими дисциплинами

Данная учебная программа по учебной дисциплине «Алгебраические методы в криптографии и теории кодирования», предназначена для студентов, обучающихся по специальности 1-02 05 01 Математика и информатика.

Актуальность изучения учебной дисциплины определяется той ролью, которую играет математика в жизни современного общества, ее влиянием на темпы развития научно-технического прогресса, а для студентов — будущих учителей — профессиональной направленностью.

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.

С точки зрения классической теории алгоритмов, исследование конечных множеств не представляет труда, так как можно перебрать все допустимые решения. Однако число таких решений на практике может достигать астрономических размеров и перебрать их даже с помощью сверхмощных ЭВМ невозможно. Именно на этом принципе основаны современные методы защиты информации. И важную роль здесь играет теория сложности вычислений, позволяющая либо находить эффективные алгоритмы решения дискретных задач, либо математически строго доказывать бесполезность поиска таких алгоритмов.

Программа соответствует первой ступени обучения в системе многоуровневого физико-математического педагогического образования. Содержание программы рассчитано на творческую межпредметную взаимосвязь с такими другими учебными дисциплинами, как предусмотренными учебным планом специальности («Аналитическая геометрия и преобразование плоскости», «Алгебра», «Информационные системы и сети»).

3. Требования к освоению учебной дисциплины

Содержание программы направлено на приобретение студентами знаний и умений по основным понятиям и методам прикладной алгебры, формирование и развитие способностей увязывать абстрактные идеи и методы с конкретными приложениями в информатике, смежных математических дисциплинах.

Практические занятия должны быть направлены на приобретение студентами навыков использования полученных теоретических знаний при решении прикладных задач. Методика их организации и проведения должна способствовать развитию способностей каждого студента и приобретению ими навыков самостоятельной работы. При проведении занятий необходимо использовать современные информационные технологии. Особое внимание требуется уделить учебно-методическому обеспечению самостоятельной работы студентов.

Методика проведения всех видов учебных занятий должна подчиняться основной задаче – подготовке учителей математики и информатики с достаточно широким математическим кругозором. Излагать материал следует доступно, при соблюдении разумной математической строгости, без перегрузки второстепенными деталями. При обилии новых абстрактных понятий и непривычного для недавнего школьника формализма в обосновании утверждений и теорем, целесообразно выносить из лекционного курса громоздкие доказательства и, разбивая их на отдельные этапы-задачи,

рассматривать на практических занятиях, заранее снабдив студентов соответствующим методическим материалом.

Практические занятия следует строить так, чтобы на каждом из них повторялся соответствующий теоретический материал и были закреплены основные навыки и умения владения усвоенным математическим аппаратом на уровне, необходимом для решения практических задач криптографии и теории кодирования.

4. Профессиональные компетенции студента

Требования к уровню усвоения содержания дисциплины «Алгебраические методы в криптографии и теории кодирования» определены образовательным стандартом высшего образования по специальности 1-02 05 01 Математика и информатика, в котором с учетом компетентностного подхода определены общенаучные умения, система предметных знаний и комплекс методологических знаний.

Изучение учебной дисциплины «Алгебраические методы в криптографии и теории кодирования» должно обеспечить формирование у студентов академических, социально-личностных и профессиональных компетенций.

Требования к академическим компетенциям

Студент должен:

- АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.
- АК-2. Владеть методами научно-педагогического исследования.
- АК-3. Владеть исследовательскими навыками.
- АК-4. Уметь работать самостоятельно.
- АК-5. Быть способным порождать новые идеи (обладать креативностью).
- АК-6. Владеть междисциплинарным подходом при решении проблем.
- АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.
- АК-10. Уметь осуществлять учебно-исследовательскую деятельность.
- АК-11. Уметь регулировать образовательные отношения и взаимодействия в педагогическом процессе.

Требования к социально-личностным компетенциям

Студент должен:

- СЛК-3. Обладать способностью к межличностным коммуникациям.
- СЛК-4. Владеть навыками здоровье сбережения.
- СЛК-7. Быть способным к осуществлению самообразования и самосовершенствования профессиональной деятельности.

Требования к профессиональным компетенциям

Студент должен быть способен:

Обучающая деятельность

- ПК-3. Использовать оптимальные методы, формы, средства обучения.

- ПК-4. Осуществлять оптимальный отбор и эффективно реализовывать технологии воспитания.

- ПК-5. Организовывать и проводить учебные занятия различных видов.

- ПК-6. Организовывать самостоятельную работу обучающихся.

Воспитательная деятельность

- ПК-7. Эффективно реализовывать воспитательную деятельность.

Развивающая деятельность

- ПК-13. Эффективно реализовывать развивающую деятельность в качестве учителя-предметника и классного руководителя.

- ПК-14. Развивать навыки самостоятельной работы обучающихся с учебной, справочной, научной литературой и др. источниками информации.

- ПК-17. Предупреждать и преодолевать школьную неуспеваемость.

Ценностно-ориентационная деятельность

- ПК-21. Оценивать учебные достижения учащихся, а также уровни их воспитанности и развития.

- ПК-22. Осуществлять самообразование и самосовершенствование профессиональной деятельности.

В результате изучения учебной дисциплины «Алгебраические методы в криптографии и теории кодирования» студент должен

***знать*:**

- свойства конечных полей по модулю простого многочлена;
- классические криптосистемы;
- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- свойства линейных пространств над конечными полями;
- основные задачи теории кодирования;
- эффективные коды.

В результате изучения учебной дисциплины «Алгебраические методы в криптографии и теории кодирования» студент должен ***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.

В результате изучения учебной дисциплины «Алгебраические методы в криптографии и теории кодирования» студент должен ***владеть*:**

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

5. Структура учебной дисциплины

Дисциплина по выбору студента «Алгебраические методы в криптографии и теории кодирования» изучается в 6 семестре при дневной форме получения образования и в 7 семестре при заочной форме получения образования. Согласно типовым учебным планам на изучение учебной дисциплины всего отводится:

дневная форма получения образования – 82 часа, из них аудиторных 52 часа (лекций – 28 часов, практических занятий – 24 часа), на самостоятельную работу студентов 30 часов, форма итогового контроля – зачёт;

заочная форма получения образования – 82 часа, из них аудиторных 14 часа (лекций – 8 часов, практических занятий – 6 часа), на самостоятельную работу студентов 68 часов, форма итогового контроля – зачёт.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1. Математический аппарат

Существование и единственность конечных полей. Структура конечных полей, минимальные расширения. Линейные пространства над конечными полями. Временная оценка сложности алгоритмов. Полиномиальные алгоритмы. Сложность алгоритмов в конечных полях. Основы теории NP-полных и NP-трудных задач.

2. Алгебраическая криптография

Подстановочные шрифты, частотный анализ. Блочное и периодическое шифрование, аффинный шифр. Стандарт AES. Алгоритм Рейндола и его три основных этапа. Понятие цифровой подписи. Криптосистемы Нидхама. Рюкзачная криптосистема. Криптосистема Ривеста, Шамира и Айдельмана

3. Теория кодирования

Основные параметры кодов и их оценка. Совершенные коды. Матрица контроля четности. Коды Хэмминга. Линейные коды специального вида (циклические коды).

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(дневная форма получения образования)

Номер раздела, темы, занятия	Название раздела, темы, занятия, перечень изучаемых вопросов	Количество аудиторных часов				Самостоятельная работа	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические (семинарские) занятия	УСР (лекции)	УСР (практика)				
1	2	3	4	5	6	7	8	9	10
6 семестр									
1	**Математический аппарат**	**8**				**6**			
1.1	**Конечные поля**	**4**							
1.1.1	Существование и единственность конечных полей	2						[9-11]	
1.1.2	Структура конечных полей, минимальные расширения	1						[9-11]	устный опрос на лекциях и практических занятиях
1.1.3	Линейные пространства над конечными полями	1						[9-11]	письменная работа по аудиторным (домашним) практическим упражнениям

1.2	**Теория сложности вычислений**	**4**				**6**			
1.2.1	Временная оценка сложности алгоритмов. Полиномиальные алгоритмы	2						[12]	
1.2.2	Сложность алгоритмов в конечных полях	1				6	Раздаточные материалы	[12]	
1.2.3	Основы теории NP-полных и NP-трудных задач	1					Раздаточные материалы	[12]	Коллоквиум
2	**Алгебраическая криптография**	**10**	**12**			**12**			
2.1	**Классические криптосистемы**	**2**	**2**						
2.1.1	Подстановочные шрифты, частотный анализ							[1-7]	устный опрос на лекциях и практических занятиях
2.1.2	Блочное и периодическое шифрование, аффинный шифр		2				Раздаточные материалы	[1-7]	
2.2	**Симметричные криптосистемы**	**4**	**6**						
2.2.1	Стандарт AES	2	2					[1-7]	Индивид. контрольные задания
2.2.2	Алгоритм Рейндола и его три основных этапа	2	4					[1-7]	письменная работа по аудиторным (домашним) практическим упражнениям
2.3	**Криптосистемы с открытым ключом**	**4**	**4**			**12**			
2.3.1	Понятие цифровой подписи. Криптосистемы Нидхама	2				6		[1-7]	Самостоятельная работа
2.3.2	Рюкзачная криптосистема		2			6		[1-7]	

2.3.3	Криптосистема криптосистема Ривеста, Шамира и Айдельмана.	2	2				Раздаточные материалы		Индивид. контрольные задания
3	**Теория кодирования**	**10**	**12**			**12**			
3.1	**Корректирующие коды**								
3.1.1	Основные параметры кодов и их оценка							[2,8]	Самостоятельная работа
3.1.2	Совершенные коды							[2,8]	устный опрос на лекциях и практических занятиях
3.2	**Линейные коды**					**12**			
3.2.1	Матрица контроля четности							[2,8]	Индивид. контрольные задания
3.2.2	Коды Хэмминга					6		[2,8]	письменная работа по аудиторным (домашним) практическим упражнениям
3.3.3	Линейные коды специального вида (циклические коды)					6		[2,8]	
	Всего	**28**	**24**			**30**			Зачет

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(заочная форма получения образования)

Номер раздела, темы, занятия	Название раздела, темы, занятия, перечень изучаемых вопросов	Количество аудиторных часов				Самостоятельная работа	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические (семинарские) занятия	УСР (лекции)	УСР (практика)				
1	2	3	4	5	6	7	8	9	10
7 семестр									
1	**Математический аппарат**	**2**				**12**			
1.1	**Конечные поля**	**1**							
1.1.1	Существование и единственность конечных полей	1						[9-11]	
1.1.2	Структура конечных полей, минимальные расширения	0						[9-11]	
1.1.3	Линейные пространства над конечными полями	0						[9-11]	устный опрос на лекциях и практических занятиях

1.2	**Теория сложности вычислений**	**1**				**12**			
1.2.1	Временная оценка сложности алгоритмов. Полиномиальные алгоритмы	1						[12]	Самостоятельная работа
1.2.2	Сложность алгоритмов в конечных полях	0				12	Раздаточные материалы	[12]	
1.2.3	Основы теории NP-полных и NP-трудных задач	0					Раздаточные материалы	[12]	Коллоквиум
2	**Алгебраическая криптография**	**4**	**6**			**28**			
2.1	**Классические криптосистемы**		**2**						
2.1.1	Подстановочные шрифты, частотный анализ							[1-7]	устный опрос на лекциях и практических занятиях
2.1.2	Блочное и периодическое шифрование, аффинный шифр		2				Раздаточные материалы	[1-7]	
2.2	**Симметричные криптосистемы**	**2**	**2**						
2.2.1	Стандарт AES							[1-7]	
2.2.2	Алгоритм Рейндола и его три основных этапа	2	2					[1-7]	письменная работа по аудиторным (домашним) практическим упражнениям
2.3	**Криптосистемы с открытым ключом**	**2**	**2**			**28**			
2.3.1	Понятие цифровой подписи. Криптосистемы Нидхама					14		[1-7]	письменная работа по аудиторным (домашним)

									практическим упражнениям
2.3.2	Рюкзачная криптосистема					14		[1-7]	
2.3.3	Криптосистема криптосистема Ривеста, Шамира и Айдельмана.	2	2				Раздаточные материалы		Индивид. контрольные задания
3	**Теория кодирования**	**2**				**28**			
3.1	**Корректирующие коды**	**2**							
3.1.1	Основные параметры кодов и их оценка	2						[2,8]	устный опрос на лекциях и практических занятиях
3.1.2	Совершенные коды							[2,8]	
3.2	**Линейные коды**					**28**			
3.2.1	Матрица контроля четности							[2,8]	Индивид. контрольные задания
3.2.2	Коды Хэмминга					14		[2,8]	Самостоятельная работа
3.3.3	Линейные коды специального вида (циклические коды)					14		[2,8]	
	Всего	**8**	**6**			**68**			Зачет

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная литература:

1. Коблиц Н. Курс теории чисел и криптографии.– Москва: ТВП, 2001. – 254 с.
2. Nagpaul S., Jain S. Topics in applied abstract algebra. – Brooks/Cole series in advanced mathematics, USA, 2005, 324 с.
3. Баричев С.Г. , Серов Р.Е. Основы современной криптографии. – М.: Телеком, 2002. – 152 с.
4. Аграновский А.В., Балакин А.В, Хади Р.А. "Классические шифры и методы их криптоанализа", М: Машиностроение, Информационные технологии, № 10,
5. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. – 41 с.
6. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб: Издательство "Лань", 2001. – 224 с.
7. Чмора А.Л. Современная прикладная криптография. 2-е изд. – М.: Гелиос, АРВ, 2002. – 256 с. ил.
8. Берлекэмп Э. Алгебраическая теория кодирования - М.: Мир , 1971 – 480 с.
9. Курош А.Г. Курс высшей алгебры / А.Г. Курош. – Санкт-Петербург: Лань, 2003.
10. Бухштаб А.А. Теория чисел / А.А. Бухштаб – Москва: Просвещение, 1966.
11. Черняк А.А. Алгебра в задачах и решениях. Часть 2: Алгебраические структуры, целочисленная арифметика, многочлены / А.А. Черняк. – Минск: БГПУ, 2008. – 110 с.
12. Черняк А.А., Черняк Ж.А., Метельский Ю.М. Математическое программирование: алгоритмический подход – Мн: Вышэйшая школа, 2007– 352 с.

Дополнительная литература:

13. Левин М. Криптография. Руководство пользователя. - М.: Познавательная книга плюс, 2001. – 320 с.
14. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
15. Шеннон К.Э. Теория связи в секретных системах. В кн. Шеннона К.Э. “Работы по теории информации и кибернетике”. – М.: ИЛ, 1963. – с. 333 – 402.
16. Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, ”ЧеРо”, 1998. – 272 с.
17. Гатчин Ю. А., Коробейников А. Г. Основы криптографических алгоритмов. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. – 29 с.

18. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА

В процессе изучения дисциплины по выбору студента «Алгебраические методы в криптографии и теории кодирования» большое внимание уделяется организации самостоятельной работы студентов, как при изучении теоретических вопросов, так и при выполнении практических заданий.

Самостоятельная работа студентов реализуется как в процессе аудиторных занятий (на лекциях, практических занятиях), так и на консультациях, при выполнении индивидуальных заданий и т.д.

Формы самостоятельной работы студентов:

– выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и методической компетенции;

– выполнение обучающих и контрольных тестов;

Основными **задачами** самостоятельной работы студентов являются:

– углубление знаний и умений студентов, полученных в ходе плановых учебных занятий;

– формирование когнитивных компетенций;

– подготовка студентов к занятиям, к промежуточному и итоговому контролю;

– формирование навыков самостоятельной научно-исследовательской деятельности.

Самостоятельная работа студентов проводится в предусмотренном учебным планом объеме.

№ п/п	Название темы, раздела	Кол-во часов на СРС	Задание	Форма выполнения
1.2	**Теория сложности вычислений**	6	[12] Полиномиальные алгоритмы целочисленной арифметики	Устный отчет
2.3	**Криптосистемы с открытым ключом**	12	[1-7] Шифрование и дешифрование рюкзачных криптосистем. Особенности криптосистемы Нидхама.	Письменный отчет с решениями не менее 5 задач
3.2	**Линейные коды**	12	[2,8] Нахождение матриц контроля четности для кодов Хэмминга. Определение бинарных и тернарных циклических кодов заданной длины	Письменный отчет с решениями не менее 5 задач

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ

Для оценки достижений и уровня знаний студента при изучении дисциплины целесообразно применить инструментарий, который включает

– самостоятельное решение задачи у доски;

– блиц-опрос при обсуждении плана решения задачи и отдельных пунктов плана.

Диагностика компетенций может проводиться в разных формах.

В устной форме:

– устный опрос на лекциях и практических занятиях;

– коллоквиумы.

В письменной форме:

– самостоятельные работы;

–письменные работы по аудиторным (домашним) практическим упражнениям.

В устно-письменной форме:

– индивидуальные контрольные задания;

– зачет.