КОНТРОЛЬНЫЙ
ЭКЗЕМПЛЯР

Учреждение образования «Белорусский государственный педагогический университет имени Максима Танка»

УТВЕРЖДАЮ
Проректор по учебной и информационно-аналитической работе
_____ 2016 В.М.Зеленкевич

Регистрационный № УД 24-1-н16-2016/уч.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования по факультативной дисциплине для специальности 1– 02 05 02 Физика и информатика

2016 г.

Учебная программа составлена на основе Образовательного стандарта высшего образования первая ступень специальности 1–02 05 02 Физика и информатика (ОСВО 1–02 05 02–2013) и учебного плана специальности 1–02 05 02 Физика и информатика (регистрационные номера: №139–2013/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:
С.И.Чубаров, заведующий кафедрой информационных технологий в образовании БГПУ, кандидат технических наук, доцент
З.Н.Примичева, доцент кафедры высшей математики БГУИР, кандидат физико–математических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и методики преподавания математики
(протокол №11 от 23.06.2016 г.)

И.о. заведующего кафедрой _____ С.И.Василец

Советом физико–математического факультета
(протокол №12 от 29.06.2016 г.)

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

Методист учебно-методического
управления БГПУ

_____ С.А.Стародуб

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

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Главная отличительная черта современной научной криптографии – появление криптосистем со строгим математическим обоснованием. Прогресс в этой области стимулировал фундаментальные исследования в тех классических разделах математики (конечные поля и группы, модулярная арифметика, факторизация простых чисел), которые еще недавно считались абстрактными и оторванными от практики. К настоящему времени сформировались разделы математики, являющиеся научной основой криптологии: алгебра, теория чисел, теория алгоритмов.

Цель данного курса - изучить основные алгебраические идеи и подходы, необходимых для понимания криптографических систем и методов таких, как стандарт AES, криптосистемы с открытым ключом и функции с замком, криптосистема RSA, рюкзачные криптосистемы, передача конфиденциальной информации по электронной почте, установление подлинности передаваемых сообщений, хранение информации (баз данных, документов) на носителях в зашифрованном виде. Отметим, что RSA – первая криптосистема, стойкость которой была основана на сложности задачи факторизации простых чисел; ее создание повлекло открытие ЭЦП (электронной цифровой подписи) и электронных денег. Прорыв в криптографии начался с изобретения ассиметричных криптосистем, которые не требовали передачи секретных ключей между сторонами.

Центральное место в данной программе занимают алгоритмический анализ сложности вычислений, поскольку недостаточно дать только теоретическое решение той или иной проблемы на конечном множестве. Куда более важно получить ее конструктивное решение, предъявив для этого эффективный алгоритм. 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. Так, в 2000 г. был принят новый государственный стандарт шифрования США – стандарт AES, с пространством ключей шифрования мощности 3.4×10^8. Современному компьютеру потребовались бы триллионы лет для нахождения нужного ключа методом исчерпывающего поиска.

Представленные в данной программе разделы призваны заложить фундамент для освоения теоретических основ вычислительной техники и информатики, сформировать навыки анализа математических алгоритмов, представить математику как единое целое, дав осознание ее связи со смежными дисциплинами.

Программа соответствует первой ступени обучения в системе многоуровневого физико-математического педагогического образования. Содержание программы рассчитано на творческую взаимосвязь с другими дисциплинами, предусмотренными учебным планом специальности, с учетом

возможностей обучения студентов на высших ступенях педагогического образования.

Изучение дисциплины «Математические основы защиты информации» ставит следующие цели и задачи:

– развития алгоритмического мышления;

– расширение и углубление математического кругозора;

– развитие навыков увязывания абстрактных алгебраических идей с практическими задачами криптографии;

– формирование математической базы, необходимой для успешного изучения теоретических основ информатики.

Преподавание и успешное изучение дисциплины «Математические основы компьютерной безопасности» осуществляется на базе приобретенных студентом знаний и умений по разделам следующих дисциплин: алгебра и геометрия, информатика.

Требования к академическим компетенциям

Студент должен:

– АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

– АК-2. Владеть системным и сравнительным анализом.

Требования к профессиональным компетенциям

Студент должен быть способен:

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

В результате изучения учебной дисциплины «Математические основы защиты информации» студент должен *знать*:

Свойства конечных полей по модулю простого многочлена;

- классические криптосистемы;
- симметричные криптосистемы;
- криптосистемы с открытым ключом.

В результате изучения учебной дисциплины «Математические основы защиты информации» студент должен *уметь*:

- конструировать полиномиальные алгоритмы дешифрования блочно подстановочных шрифтов;
- воспроизводить основные этапы алгоритма шифрования Рейндола и пользоваться этапными ключами алгоритма AES-128;

В результате изучения учебной дисциплины «Математические основы защиты информации» студент должен *владеть*:

- навыками шифрования и дешифрования криптосистемы с открытым ключом;
- навыками шифрования и дешифрования криптосистемы RSA.

На изучение дисциплины «Математические основы защиты информации» типовым учебным планом предусмотрено 20 часов, из них аудиторных занятий – 20 часов, в том числе лекций – 10 часов, практических – 10 часа. Факультатив проводится на 3 курсе, 5 семестр.

Содержание факультативной дисциплины

1. Классические криптосистемы

Подстановочные шрифты, частотный анализ. Блочное и периодическое шифрование, аффинный шифр.

2. Симметричные криптосистемы

Стандарт AES. Алгоритм Рейндола и его три основных этапа.

3. Криптосистемы с открытым ключом

Понятие цифровой подписи. Криптосистемы Нидхама. Рюкзачная криптосистема. Криптосистема криптосистема Ривеста, Шамира и Айдельмана.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА
факультативной дисциплины «Математические основы защиты информации»

Номер раздела, темы, занятия	Название раздела, темы, занятия, перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические (семинарские) занятия	управляемая самостоятельная работа студента				
1	2	3	4	5	6	7	8	9
1	**Классические криптосистемы**	**2**						
1.1	Подстановочные шрифты, частотный анализ	2					[2-7]	
1.2	Блочное и периодическое шифрование, аффинный шифр		2			Раздаточные материалы	[2-7]	
2	**Симметричные криптосистемы**	**4**	**4**				[1-7]	
2.1	Стандарт AES	2					[1,3]	
2.2	Алгоритм Рейндола и его три основных этапа	2	4				[1,3]	Индивид. контрольные задания
3	**Криптосистемы с открытым ключом**	**4**	**4**					
3.1	Понятие цифровой подписи. Криптосистемы Нидхама	2					[1, 3-5]	
3.2	Рюкзачная криптосистема		2				[1]	
3.3	Криптосистема криптосистема Ривеста, Шамира и Айдельмана	2	2			Раздаточные материалы	[1-7]	
3.4	**Всего**	**10**	**10**					

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная

1. Nagpaul S., Jain S. Topics in applied abstract algebra. – Brooks/Cole series in advanced mathematics, USA, 2005, 324 с.

2. Коблиц Н. Курс теории чисел и криптографии.– Москва: ТВП, 2001. – 254 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.

Дополнительная

1. Левин М. Криптография. Руководство пользователя. - М.: Познавательная книга плюс, 2001. – 320 с.

2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

3. 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.

4. Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, ”ЧеРо”, 1998. – 272 с.

5. Гатчин Ю. А., Коробейников А. Г. Основы криптографических алгоритмов. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. – 29 с.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ

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

– контроль выполнения практических заданий

– устный экспресс контроль по блоку тем

– блиц-опрос по рассмотренной теме

– отчет о выполнении заданий самостоятельного цикла

– контроль выполнения самостоятельной работы по темам

– зачетное занятие с учетом результатов рейтинг-листа, составленного по данным прохождения дисциплины в семестре.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
факультативной дисциплины
«Математические основы защиты 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)
Технологии программирования и методы алгоритмизации	Кафедра информатики и методики преподавания информатики	Формировать навыки математической оценки сложности вычислений и эффективности алгоритмов и сопоставление их с практическими реализациями в компьютерных системах	Протокол №11 от 23.06.2016