БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе БГУ
_____ А.Л.Толстик
(подпись) (И.О.Фамилия)
29.01.2015
(дата утверждения)

Регистрационный № УД-1078 /уч.

Математические основы защиты информации

Учебная программа учреждения высшего образования по учебной дисциплине для специальностей:

1-31 80 03 (код специальности) **Математика** (наименование специальности)

2015 г.

Учебная программа составлена на основе ОСВО 1-31 80 03-2012 (24.08.2012) и учебного плана (регистрационный № G31-183/уч.; 09.06.2014) для специальности 1-31 80 03 Компьютерная математика и системный анализ.

СОСТАВИТЕЛИ:

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

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа Белорусского государственного университета
(протокол №10 от 23.04.2015);

Учебно-методической комиссией механико-математического факультета Белорусского государственного университета
(протокол № 6 от 26.05.2015).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью дисциплины «Математические основы защиты информации» является подготовка специалистов, способных использовать фундаментальные математические знания в качестве основы при проведении прикладных исследований.

Преподавание дисциплины ***решает следующие задачи***:

– формирование у студентов способностей самостоятельно разрабатывать алгоритмы решения задач и их анализировать;

– развивать и использовать инструментальные средства, информационные среды, автоматизированные системы;

– использовать математические и компьютерные методы исследований при анализе современных естественнонаучных, экономических, социально-политических процессов;

– приобретение способностей самостоятельно расширять компьютерные математические знания с дальнейшим их использованием при анализе математических моделей широкого круга прикладных задач.

В результате изучения 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.

Дисциплина «Математические основы защиты информации» является дисциплиной по выбору и преподается во втором семестре. Она является ярким примером использования математики в информационных технологиях. При изучении дисциплины «Математические основы защиты информации» в значительной мере используются знания, умения и навыки, полученные при изучении дисциплины «Компьютерная математика».

Данная дисциплина является дисциплиной по выбору магистранта и изучается во втором семестре. Общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины в соответствии с учебным планом учреждения высшего образования по специальности, составляет соответственно 112 и 36 часов. Аудиторные часы состоят из 18 часов лекций, 18 часов лабораторных занятий.

Формой текущей аттестации по учебной дисциплине является экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Введение.

Основные определения криптографии. Классические криптосистемы: шифр Сциталя, криптосистема Цезаря, шифр Виженера. Полиномиальный, субэкспоненциальный 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. Генерирование больших простых чисел.

Решето Эратосфена. Малая теорема Ферма. Псевдопростые числа. Числа Кармайкла. Свидетели простоты. Вероятностный тест на простоту Миллера-Рабина. Гипотеза Римана. Теорема Диемитко. Детерминированный полиномиальный алгоритм проверки простоты чисел. Детерминированный и недетерминированный алгоритмы. Алгоритмы с нулевой, односторонней и двусторонней ошибками.

Тема 3. Факторизация чисел.

Метод пробных делений. Ро-метод Полларда. Классы P и NP. Китайская теорема об остатках. Факторизация Ферма и факторные базы. Метод Диксона. Метод квадратичного решета.

Тема 4. Криптосистемы с открытым ключом.

Криптосистемы с открытым ключом. Односторонние функции. Криптосистема RSA. Задача о рюкзаке. Задача о сумме подмножества. Задача о рюкзаке с быстрорастущим вектором. Рюкзачная криптосистема Меркля-Хеллмана. NP-полнота задачи о рюкзаке. Квадратичный вычет. Критерий Эйлера. Символ Лежандра. Извлечение квадратного корня в кольце классов вычетов. Криптосистема Рабина.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

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
1.	**Математические основы защиты информации**	**18**			**18**			
1.1	Введение	4			4			Отчеты по лабораторным работам с их устной защитой
1.2	Генерирование больших простых чисел	4			4			Отчеты по лабораторным работам с их устной защитой
1.3	Факторизация чисел	4			4			Отчеты по лабораторным работам с их устной защитой
1.4	Криптосистемы с открытым ключом	6			6			Отчеты по лабораторным работам с их устной защитой

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Литература

Основная:

1. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.
2. Введение в криптографию / Под ред. В.В. Ященко. – М.: МЦНМО-ЧеРоб, 1998, 271 с.
3. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: Научное изд-во ТВП, 2001. – 254 с.
4. 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.
5. Маховенко Е.Б. Теоретико-числовые методы в криптографии / Е.Б. Маховенко. – М.: Гелиос АРВ, 2006. – 320с.
6. Тилборг, Х.К.А. ван. Основы криптологии / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.
7. Харин, Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Минск: БГУ, 1999. – 319 с.
8. 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.
9. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. 2-е издание / Брюс Шнайер. — М.: Триумф, 2002. — 816 с.

Дополнительная:

10. Menezes, A Handbook of Applied Cryptography / A. Menezes, P. van Oorschot and S. Vanstone. CRC Press, 1997. – 780 p.
11. 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.
12. 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.
13. Дориченко, С.А. 25 этюдов о шифрах / С.А. Дориченко, В.В. Ященко. – М.: ТЕИС, 1994. – 69 с.

14. Кнут, Д. Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е издание. / Д. Кнут. – М.-СПб.-Киев: Вильямс, 2003.
15. Молдовян, А. А. Криптография / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. – СПб. : Лань, 2001. – 224 с.
16. Нестеренко, Ю.В. Теория чисел: учебник для студ. высш. учеб. заведений / Ю.В. Нестеренко. – М.: Издательский центр «Академия», 2008. – 272 с.
17. Острик, В.В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые / В.В. Острик, М.А. Цфасман. – М.: МЦНМОб 2001. – 48 с.
18. 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.
19. Саломаа, А. Криптография с открытым ключом / – М.: Мир, 1996. – 320 с.
20. Птицын, Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – М.: МГТУ им. Н.Э. Баумана, 2002. – 80 с.

Перечень используемых средств диагностики результатов учебной деятельности

Контроль работы магистранта проходит в форме собеседования, контрольной работы в аудитории или над выполнением лабораторных работ в лаборатории и самостоятельно вне аудитории с предоставлением отчета по лабораторным работам с его устной защитой. Задания к контрольным и лабораторным работам составляются согласно содержанию учебного материала.

Для совершенствования педагогического мастерства и способностей учиться самостоятельно магистрантам могут выдаваться темы докладов, с которыми они выступают на занятиях.

Во время самостоятельной работы магистрант выполняет задания, полученные на лабораторных занятиях, а также изучает рекомендуемую литературу.

Экзамен по дисциплине проходит в устной или письменной форме.

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]
Компьютерная математика	Кафедра дифференциальных уравнений и системного анализа	нет	Вносить изменения не требуется (протокол № 10 от 23.04.2015)

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

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 201_ г.)
(название кафедры)

Заведующий кафедрой

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)