Министерство образования и науки РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«Новосибирский национальный исследовательский государственный университет» (Новосибирский государственный университет, НГУ)
Гуманитарный факультет

Программа рассмотрена
на заседании кафедры
фундаментальной и прикладной
лингвистики
29.08.2014
_____
Зав. кафедрой, проф. М.К. Тимофеева

Утверждаю

_____
декан гуманитарного
факультета, профессор
1.09.2014
Л.Г. Панин

Основная образовательная программа
высшего образования

Направление подготовки
035800 – Фундаментальная и прикладная лингвистика

Квалификация (степень) выпускника –
бакалавр

ПРОГРАММА УЧЕБНОГО КУРСА «КРИПТОГРАФИЯ»

(72 часа, 2 з.е.)

1. **Наименование дисциплины**

ПРОГРАММА УЧЕБНОГО КУРСА
«КРИПТОГРАФИЯ»

Программа дисциплины «Криптография» составлена в соответствии с требованиями к обязательному минимуму содержания и уровню подготовки дипломированного бакалавра по направлению 035800 «Фундаментальная и прикладная лингвистика» в целях обеспечения реализации учебного процесса в НГУ.

Содержание курса направлено на ознакомление студентов с математическими основами теории информации, методами защиты информации, методами кодирования, историей развития криптографии, ее современным состоянием и тенденциями развития. Рассматриваются основные методы шифрования и криптографические протоколы обмена информацией. Прослеживается естественная связь с моделями и методами теоретической и прикладной лингвистики. Используются современные информационные технологии.

Курс позволяет овладеть основными методами, применяемыми в современных системах защиты информации. Теория информации имеет важное методологическое значение в познавательном и исследовательском процессах. Методы защиты информации и современные информационные технологии имеют важное прикладное значение.

Курс соответствует двум приоритетным направлениям Программы развития НГУ: математика, гуманитарные науки.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Цели освоения дисциплины

Главной целью дисциплины является ознакомление с основными принципами защиты информации с помощью криптографических методов и примерами реализации этих методов на практике. о методах и критериях оценки надежности защиты информации.

Студенты могут получить представление об основных методах и средствах криптографического анализа, об использовании в криптографическом анализе слабостей криптосистем, о принципиальных подходах к созданию современных технических средств криптографической защиты информации; о современных тенденциях развития средств и методов криптографической защиты.

В результате изучения дисциплины студент должен:

иметь представление:
- об основных этапах исторического развития криптографии;
- о методах и критериях оценки надежности защиты информации;
- об основных методах и средствах криптографического анализа;
- об использовании в криптографическом анализе слабостей криптосистем;
- о современных тенденциях развития средств и методов криптографической защиты

знать и уметь использовать:
- основные характеристики открытых текстов;
- математические модели открытых текстов;
- основные классы шифров и их характеристики;
- математические модели шифров;
- системы шифрования с открытым ключом;
- основные требования, предъявляемые к системам криптографической защиты информации с учетом возможных угроз;

владеть:
- методами анализа простейших шифров (простая замена, гаммирование);
- навыками использования систем шифрования с закрытым ключом;
- навыками использования систем шифрования с открытым ключом.

Перечисленные результаты образования являются основой для формирования следующих общекультурных и общепрофессиональных компетенций:

***а) общекультурными* (*ОК*)**

– владением культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения	ОК-1
– умением логически верно, аргументировано и ясно строить устную и письменную речь	ОК-2
– осознанием социальной значимости своей будущей профессии, обладанием высокой мотивацией к выполнению профессиональной деятельности	ОК-8
– способностью применять методы математического анализа и моделирования в профессиональной деятельности	ОК-10

***б) профессиональными (ПК)*:**

общепрофессиональными:

– знанием основ математических дисциплин, которые используются при формализации лингвистических знаний и процедур анализа и синтеза лингвистических структур: теории множеств, математического анализа, теории вероятностей и математической статистики, теории информации и кодирования, математической логики, математической теории грамматик	ПК-2

дополнительными:

- способностью работать в междисциплинарной команде ПК-26
- способностью общаться с экспертами в других областях знаний ПК-27
- умением видеть междисциплинарные связи изучаемых дисциплин и пониманием их значения для будущей профессиональной деятельности ПК-28

3. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Криптография» является частью вариативной составляющей (курсы по выбору) математического и естественнонаучного цикла ООП по направлению подготовки Фундаментальная и прикладная лингвистика опирается на дисциплину «Теория вероятностей и математическая статистика» данной ООП.

Дисциплина «Криптография» используется в курсе «Стилометрия».

4. Объем дисциплины в зачетных единицах с указанием количества академических, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.

Общая трудоемкость дисциплины составляет 1 зачетных единицы, 54 часа. Из них на контактную работу с преподавателем 36 часов (лекции), на самостоятельную работу студентов – 18 часов. Интерактивных занятий – 1 час.

5. Содержание дисциплины “Криптография”, структурированное по темам с указанием отведенного на них количества астрономических часов и видов учебных занятий

Программа курса

Лекции	Раздел, тема, содержание занятий	Количество часов			Литература
		Лекций (часы)	упражнений	Самост. занятий	(пункты учебников)
1	*Тема 1.* —История развития криптографии	2		2	Носов
2	*Тема 2.* — Простейшие криптосистемы	2		2	Введение, гл 1
3	*Тема 3.* — Основные понятия криптографии	2		2	Введение, гл 1
4	*Тема 4.* — Криптография и теория сложности	2		2	Введение, гл.2
5	*Тема 5.* — Криптографические протоколы	2		2	Введение, гл.3
6	*Тема 6.* — Элементы теории чисел	2		2	Введение, гл.4
7	*Тема 7.* — Криптосистемы с открытым ключом	2		2	Введение, гл.5
8	*Тема 8.* — Компьютеры и криптография	2		2	Введение, гл 6
9	*Тема 9.* — Элементы теории информации	2		2	Файнстейн, гл.1-2
10	*Тема 10.* —Вероятностные модели текстов	4		4	Харин, гл 5
11	*Тема 11.* —.Методы теории информации в криптографии	2		2	Харин,, гл 6
12	*Тема 12.* —Статистическое тестирование случайных текстов	2		2	Харин,, гл 7
13	*Тема 13.* —Поточные криптосистемы	2		2	Харин,, гл 9
14	*Тема 14.* Предсказание и энтропия печатного английского текста	2		2	Шеннон, 669-686
15	*Тема 15.* —Электронная цифровая подпись	2		2	Харин,, гл 14
16	*Тема 16.* —Новые направления в криптографии	2		2	Харин,, гл 17
17	*Дискуссия по тематике курса*	2		2	
		36		36	
ЗАЧЕТ					

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Слушателям предоставляются презентации лекций с перечнями доступных материалов и источников

7. Фонд оценочных средств для промежуточной аттестации обучающихся по дисциплине.

Примеры вопросов для зачёта:

1. Шифр Цезаря.

2. Шифр перестановки.
3. Шифр простой замены.
4. Сложение по модулю.
5. Гаммирование по модулю 2.
6. Гаммирование по модулю n.
7. Малая теорема Ферма.
8. Теорема Эйлера
9. Шифр RSA.
10. Электронная подпись RSA.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Рябко, Борис Яковлевич. Криптографические методы защиты информации : [учеб. пособие для вузов по спец. "Многокан. телекоммуникац. системы", "Радиосвязь, радиовещание и телевидение", "Защищенные системы связи"] / Б.Я. Рябко, А.Н. Фионов .— М. : Горячая линия - Телеком, 2005 .— 229 с.

б) дополнительная литература:

1. Введение в криптографию. Под ред. В.В. Ященко. Серия «Новые математические дисциплины». Москва, МЦНМО – ЧеРо, 2000.
2. Файнстейн А. Основы теории информации. Москва, ИЛ, 1960.
3. Харин Ю.С., Берник В.И., Матвеев Г.В., Агневич С.В. Математические и компьютерные основы криптологии**.** Минск, 2003.
4. Шеннон К. Работы по теории информации и кибернетике. Москва, ИЛ, 1963.
5. Носов В.А. Краткий исторический очерк развития криптографии. В сб. Московский университет и развитие криптографии в России. Материалы конференции в МГУ 17-18 октября 2002 г. Москва, МЦИМО, 2003.
6. Николенко С. О криптографии. Криптография — АУ РАН, осень 2011 (презентация).
7. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО «Полиграф-Консалтинг», 2005. – 215 с.
8. Richard A. Mollin. Codes: The Guide to Secrecy From Ancient to Modern Times. — 1 edition. — Chapman & Hall/CRC, 2005. — 679 p.
9. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.
10. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source code in C. — John Wiley & Sons, 1996. — 675 p.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Программное обеспечение для демонстрации слайд-презентаций. Программа «Математика» для операций с характеристиками текстов и кодов.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Ноутбук, медиапроектор, мультемидийные презентации