РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Математическая криптография

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в магистратуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 01.04.02 «Прикладная математика и информатика». Направленность (профиль) «Математические методы обработки информации и принятия решений». Образовательная программа «Информационная безопасность компьютерных систем».

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть магистерской образовательной программы «Информационная безопасность компьютерных систем», изучается во 2-м семестре.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность и умение использовать принципы построения и сравнени надежности базовых криптографических алгоритмов; владение навыка ми, обеспечивающими критическую оценку криптографических алго- ритмов, примитивов, стандартов; представление о современных метод криптографической защиты информации и государственных стандарта на криптографические алгоритмы (СПК-56)	З1 (СПК-56) Знать: основные математические модели криптографических протоколов и криптографических примитивов У1 (СПК-56) Уметь формулировать требования к стойкости для различных криптографических протоколов и моделей противника (атаки и угрозы) В1 (СПК-56) Владеть методами доказательства стойкости криптографических протоколов и криптографических примитивов на основе демонстрации сводимо-

	стей к криптографическим предположениям

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов.

72 часа составляет контактная работа с преподавателем – 70 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 2 часа групповых консультаций, 0 часов мероприятий текущего контроля успеваемости, 0 часа промежуточной аттестации.

36 часа составляет самостоятельная работа учащегося.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по дискретной математике, теории вероятностей, теории сложности вычислений и теории информации в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения для самостоятельной работы магистрантов используются ресурсы сайта cryptography.ru.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе изучаются математические модели криптографических протоколов и примитивов, особое внимание уделяется моделям противника, а именно атакам и угрозам информационной безопасности. Изучаются математически строгие определения стойкости наиболее важных криптографических протоколов. Доказываются фундаментальные результаты о необходимых и достаточных условиях существования стойких криптографических протоколов.

The course studies mathematical models of cryptographic protocols and primitives, special attention is paid to model of adversary, mainly to attacks and threats to information security. The course provides mathematically rigorous definitions of security for most important cryptographic protocols. Certain fundamental results on the necessary and sufficient conditions for existence of secure protocols are proven.

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	**Всего (часы)**	В том числе							
			Контактная работа (работа во взаимодействии с преподавателем), часы из них	**Самостоятельная работа учащегося, часы** из них					
Занятия лекционного типа		Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости: коллоквиумы, практические контрольные занятия и др.	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п..	**Всего**
Тема 1. Односторонняя функция. Понятия сильной и слабой односторонней функции. Теорема Яо об эквивалентности предположений о их существовании. Од-	**6**	6	-	-	-	4	-	-	-

носторонняя перестановка.									
Тема 2. Понятие трудного бита односторонней функции. Теорема Гольдрайха–Левина.	**9**	6	-	-	-	**4**	3	-	3
Тема 3. Псевдослучайные последовательности. Определение криптографически стойкого псевдослучайного генератора. Тест следующего бита. Теорема Яо об универсальном тесте. Необходимые и достаточные условия существования псевдослучайных генераторов.	**9**	6	-	-	-	**4**	3	-	3
Тема 4. Задача обеспечения конфиденциальности. Понятие криптосистемы с секретным ключом. Понятие стойкости криптосистемы. Доказуемо стойкие потоковые криптосистемы.	**7**	4	-	-	-	**4**	3	-	3
Тема 5. Генераторы	**9**	6	-	-	-	**4**	3	-	3

псевдослучайных функций и псевдо-случайных перестановок. Блоковые криптосистемы с секретным ключом.									
Тема 6. Криптосистемы с открытым ключом. Криптосистема Рабина. Доказательство стойкости. Криптосистемы вероятностного шифрования.	**7**	4	-	-	-	**4**	3	-	3
Тема 7. Задача обеспечения целостности. Понятие схемы электронной подписи. Определение стойкости.	**9**	6	-	-	-	**4**	3	-	3
Тема 8. Хэш-функции. Семейства односторонних хэш-функций. Необходимые и достаточные условия существования.	**9**	6	-	-	-	**4**	3	-	3
Тема 9. Необходимые и достаточные условия существования стойких схем электронной подписи.	**7**	4	-	-	-	**4**	3	-	3
Тема 10. Протоколы	**9**	6	-	-	-	**4**	3	-	3

интерактивного доказательства. Класс IP. Интерактивное доказательство с нулевым разглашением.									
Тема 11. Протокол привязки к биту (bit commitment). Понятие блоба. Конструкция Наора.	**9**	6	-	-	-	**4**	3	-	3
Тема 12. Теорема Гольдрайха, Микали и Вигдерсона о существовании доказательств с нулевым разглашением для всех языков из класса NP.	**9**	6	-	-	-	**4**	3	-	3
Тема 13. Задача обеспечения неотслеживаемости. Системы электронных платежей. Электронная монета.	**9**	4	-	-	2	**4**	3	-	3
Итого	**108**	**72**	**36**						

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к практическим заданиям текущего контроля и промежуточной аттестации.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная учебно-методическая литература

1) O. Goldreich. Foundations of cryptography. Volume 1 (Basic tools). Volume 2 (Basic applications). Cambridge University Press, 2001 (v. 1), 2004 (v 2).
2) M. Luby. Pseudorandomness and cryptographic applications. Princeton University Press, 1996.

Дополнительная учебно-методическая литература

1) Введение в криптографию. Под общ. ред. В. В. Ященко. 4-е изд., доп. М.: МЦНМО, 2012.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1) http://cryptography.ru

Информационные технологии, используемые в процессе обучения

Не используются.

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

с. н. с. Варновский Николай Павлович (barnaba.np@gmail.com)

Приложение

Оценочные средства для промежуточной аттестации по дисциплине «Математическая криптография»

Промежуточная аттестация состоит из индивидуального собеседования, проверяющего приобретенные знания.
Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ из соответствующих карт компетенций**	**ОЦЕНОЧНЫЕ СРЕДСТВА**				**ОЦЕНОЧНЫЕ СРЕДСТВА**
	1	2	3	4	5	
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**	
З1 (СПК-56) Знать: основные математические модели криптографических протоколов и криптографических примитивов	Отсутствие знаний	Фрагментарные представления об основных математических моделях криптографических протоколов и криптографических примитивов	В целом сформированные, но неполные знания об основных математических моделях криптографических протоколов и криптографических примитивов	Сформированные, но содержащие отдельные пробелы знания об основных математических моделях криптографических протоколов и криптографических примитивов	Сформированные систематические знания об основных математических моделях криптографических протоколов и криптографических примитивов	индивидуально собеседование
У1 (СПК-56) Уметь формулировать требования к стойкости для различных криптографических протоколов и моделей против-	Отсутствие умений	Фрагментарные умения формулировать требования к стойкости для различных криптографических протоколов и моделей противника (атаки и	В целом сформированное, но не систематическое умение формулировать требования к стойкости для различных криптографических про-	Сформированное, но содержащее отдельные пробелы умение формулировать требования к стойкости для различных крипто-	Сформированное систематическое умение формулировать требования к стойкости для различных криптографических про-	индивидуально собеседование

ника (атаки и угрозы)		угрозы)	токолов и моделей противника (атаки и угрозы)	графических протоколов и моделей противника (атаки и угрозы)	токолов и моделей противника (атаки и угрозы)	
В1 (СПК-56) Владеть методами доказательства стойкости криптографических протоколов и криптографических примитивов на основе демонстрации сводимостей к криптографическим предположениям	Отсутствие навыков	Фрагментарное владение методами доказательства стойкости криптографических протоколов и криптографических примитивов на основе демонстрации сводимостей к криптографическим предположениям	В целом сформированное, но не систематическое владение методами доказательства стойкости криптографических протоколов и криптографических примитивов на основе демонстрации сводимостей к криптографическим предположениям	Сформированное, но содержащее отдельные пробелы владение методами доказательства стойкости криптографических протоколов и криптографических примитивов на основе демонстрации сводимостей к криптографическим предположениям	Сформированное систематическое владение методами доказательства стойкости криптографических протоколов и криптографических примитивов на основе демонстрации сводимостей к криптографическим предположениям	индивидуально собеседование

Фонды оценочных средств

Примерные контрольные задания для текущего контроля успеваемости.

1. Доказать, что если для языка L существует протокол интерактивного доказательства, то для L существует протокол интерактивного доказательства с детерминированным доказывающим.
2. Доказать, что если для языка L существует протокол интерактивного доказательства с детерминированным проверяющим, то L принадлежит NP.
3. Доказать, что если для языка L существует протокол интерактивного доказательства с вычислительно нулевым разглашением, в котором пересылается лишь одно сообщение от доказывающего к проверяющему, то L принадлежит BPP.

Список вопросов для экзамена на промежуточной аттестации.

1) **Односторонняя функция. Понятия сильной и слабой односторонней функции. Теорема Яо об эквивалентности предположений о их существовании. Односторонняя перестановка.**
2) **Понятие трудного бита односторонней функции. Теорема Гольдрайха–Левина.**

3) **Псевдослучайные последовательности. Определение криптографически стойкого псевдослучайного генератора. Тест следующего бита. Теорема Яо об универсальном тесте. Необходимые и достаточные условия существования псевдослучайных генераторов.**
4) **Задача обеспечения конфиденциальности. Понятие криптосистемы с секретным ключом. Понятие стойкости криптосистемы. Доказуемо стойкие потоковые криптосистемы.**
5) **Генераторы псевдослучайных функций и псевдослучайных перестановок. Блоковые криптосистемы с секретным ключом.**
6) **Криптосистемы с открытым ключом. Криптосистема Рабина. Доказательство стойкости. Криптосистемы вероятностного шифрования.**
7) **Задача обеспечения целостности. Понятие схемы электронной подписи. Определение стойкости.**
8) **Хэш-функции. Семейства односторонних хэш-функций. Необходимые и достаточные условия существования.**
9) **Необходимые и достаточные условия существования стойких схем электронной подписи.**
10) **Протоколы интерактивного доказательства. Класс IP. Интерактивное доказательство с нулевым разглашением.**
11) **Протокол привязки к биту (bit commitment). Понятие блоба. Конструкция Наора.**
12) **Теорема Гольдрайха, Микали и Вигдерсона о существовании доказательств с нулевым разглашением для всех языков из класса NP.**
13) **Задача обеспечения неотслеживаемости. Системы электронных платежей. Электронная монета.**

Примерное практическое контрольное задание для промежуточной аттестации.

1. В предположении $P \neq NP$ построить полиномиально вычислимую функцию, которая трудно инвертируема в худшем случае, но не является односторонней.

2. Доказать, что если f — односторонняя функция, то $|f(\{0,1\}^n)|$ имеет суперполиномиальный рост.

3. В предположении существования односторонних функций доказать, что не существует предиката, являющегося трудным для любой односторонней функции.

4. Доказать, что если $f_{n,d} : \{0,1\}^n \to \{0,1\}^n$, где n — натуральное число, а d из $\{0,1\}^n$, образуют полномиально вычислимое семейство функций, то семейства однократных и двукратных композиций образов $f_{n,d}$ при преобразовании Файстеля не является псевдослучайным семейством перестановок.

Методические материалы для проведения процедур оценивания результатов обучения

Оценивание результатов обучения осуществляется посредством устного экзамена по окончании курса. Критерии оценки приведены в таблице выше.