Программа утверждена на заседании кафедры _____
Протокол № _____

Рабочая программа дисциплины (модуля)

1. Код и наименование дисциплины (модуля): «Криптографические методы защиты информации»

2. Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре.

3. Направление подготовки: «10.06.01 Информационная безопасность». Направленность программы: «Методы и системы защиты информации, информационная безопасность» (научная специальность 05.13.19).

4. Место дисциплины (модуля) в структуре ООП: вариативная часть ООП, элективный курс по выбору кафедры, обязателен для освоения не позднее второго года обучения.

5. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

Формируемые компетенции *(код компетенции)*	**Планируемые результаты обучения по дисциплине (модулю)**
УК-1, УК-3	З1 (УК-1) ЗНАТЬ: методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях У1 (УК-1) УМЕТЬ: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов У2 (УК-1) УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений З1 (УК-3) ЗНАТЬ: особенности представления результатов научной деятельности в устной и письменной форме при

	работе в российских и международных исследовательских коллективах У1 (УК-3) УМЕТЬ: следовать нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач У2 (УК-3) УМЕТЬ: осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом
ОПК-1	З1 (ОПК-1) ЗНАТЬ: основные понятия, результаты и задачи информационной безопасности У1 (ОПК-1) УМЕТЬ: применять основные математические методы и алгоритмы для решения стандартных задач информационной безопасности В1 (ОПК-1) ВЛАДЕТЬ: методами математического моделирования
ПК-051319	З8 (ПК-051319) ЗНАТЬ: основные понятия, решаемые задачи, нормативные основы и программно-технические методы криптографической защиты информации З9 (ПК-051319) ЗНАТЬ: теоретические основы и подходы к практической реализации криптографических примитивов и протоколов. З10 (ПК-051319) ЗНАТЬ: основные принципы, режимы работы и особенности практической реализации симметричных и асимметричных криптосистем в задачах шифрования и электронной цифровой подписи З11 (ПК-051319) ЗНАТЬ: основные принципы и особенности реализации криптографических методов идентификации и аутентификации в компьютерных системах

6. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:
объем дисциплины (модуля) составляет 2 зачетные единицы, всего 80 часов, из которых 44 часа составляет контактная работа аспиранта с преподавателем (36 часов — занятия лекционного типа, 8 часов — мероприятия промежуточной аттестации), 36 часов составляет самостоятельная работа аспиранта.

7. Входные требования для освоения дисциплины (модуля), предварительные условия:
- знание основных направлений, проблем, теорий и методов информатики, программирования, дискретной математики, математической логики, теории вероятностей;
- умение решать стандартные задачи дискретной математики, математической логики, теории вероятностей и применять идеи, использованные в их решениях, для решения аналогичных задач.

8. Формат обучения: спецкурс по выбору кафедры.

9. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и виды учебных занятий

Наименование и краткое содержание разделов и тем дисциплины (модуля), **форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа обучающегося, 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. Основные понятия, решаемые задачи, нормативные основы и программно-технические методы криптографической защиты информации. Криптография и криптоанализ. Обзор решаемых задач и основных методов. Понятия криптографической системы, криптографического алгоритма, криптографического протокола. Обзор нормативной базы в области криптографии. Обзор типовых областей применения криптографических систем, алгоритмов и протоколов. Криптографическая стойкость. Обзор распространенных методов атак.	8	4					4	4		4

Тема 2. Теоретические основы и подходы к практической реализации криптографических примитивов и протоколов. Обзор и примеры криптографических примитивов и протоколов. Роль генераторов псевдослучайных чисел в криптосистемах. Методы генерации псевдослучайных последовательностей чисел. Криптографически стойкие генераторы псевдослучайных чисел. Методы реализации хеш-функций. Однонаправленные хеш-функции. Однонаправленные хеш-функции на основе симметричных блочных алгоритмов. Обзор алгоритмов хеширования семейств MD и SHA. Отечественный стандарт хеш-функции. Протоколы идентификации с нулевой передачей знаний.	20	10					10	10		10
Тема 3. Основные принципы, режимы работы и особенности практической реализации симметричных криптосистем. Обзор методов криптографии с симметричным ключом и криптографии с открытым ключом. Виды блочных и поточных шифров. Примеры традиционных симметричных криптосистем. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Обзор основных принципов и режимов работы алгоритма шифрования данных DES. Обзор основных принципов и режимов работы алгоритма шифрования данных AES. Общие положения отечественного стандарта шифрования данных ГОСТ 28147-89 на примере режимов простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки.	16	8					8	8		8

Тема 4. Основные принципы, режимы работы и особенности практической реализации асимметричных криптосистем. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах. Концепция криптосистемы с открытым ключом. Однонаправленные функции. Комбинированные методы шифрования. Криптосистема шифрования данных RSA. Схема шифрования Полига—Хеллмана. Схема шифрования эль-Гамаля.	16	8					8	8		8
Тема 5. Основные принципы, режимы работы и особенности практической реализации электронной цифровой подписи. Методы реализации электронной цифровой подписи. Электронная цифровая подпись на примере алгоритмов RSA, EGSA, DSA. Отечественный стандарт цифровой подписи.	8	4					4	4		4
Тема 6. Основные принципы и особенности реализации криптографических методов идентификации и аутентификации в компьютерных системах. Обзор и примеры использования криптографических методов идентификации и аутентификации в компьютерных системах. Взаимная аутентификация.	4	2					2	2		2
Промежуточная аттестация в форме экзамена	8	8								
Итого	80	44					44	36		36

10. Перечень учебно-методического обеспечения для самостоятельной работы аспирантов по дисциплине (модулю).

Литература:

1) Основы информационной безопасности: учебное пособие. / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.: ил. – (Серия «Основы информационных технологий»).

2) Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.

3) Б. Шнайер. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С. 2-е изд. / Под редакцией П. В. Семьянова. – М.: Триумф, 2002.

4) Методы дискретной математики в криптологии. / В. М. Фомичев. – М.: Диалог-МИФИ, 2010. – 424 с.

5) Введение в криптографию. 3-е изд., дополненное. / Под редакцией Ященко В.В. - М.: МЦНМО, 2000.

11. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю).

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	**КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю) и ШКАЛА оценивания**					**ПРОЦЕДУРЫ ОЦЕНИВАНИЯ**
	1	2	3	4	5	
З1 (УК-1) ЗНАТЬ: методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Отсутствие знаний	Фрагментарные знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач	Общие, но не структурированные знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач	Сформированные, но содержащие отдельные пробелы знания основных методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных	Сформированные систематические знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных	
У1 (УК-1) УМЕТЬ: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	Отсутствие умений	Частично освоенное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	В целом успешно, но не систематически осуществляемые анализ альтернативных вариантов решения исследовательских и практических задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов	В целом успешно, но содержащие отдельные пробелы анализ альтернативных вариантов решения исследовательских задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов	Сформированное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	

У2 (УК-1) УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	Отсутствие умений	Частично освоенное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	В целом успешное, но не систематически осуществляемое умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	В целом успешное, но содержащее отдельные пробелы умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	Сформированное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	
З1 (УК-3) ЗНАТЬ: особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах	Отсутствие знаний	Фрагментарные знания особенностей предоставления результатов научной деятельности в устной и письменной форме	Неполные знания особенностей представления результатов научной деятельности в устной и письменной форме, при работе в российских и международных коллективах	Сформированные, но содержащие отдельные пробелы знания основных особенностей представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах	Сформированные и систематические знания особенностей представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах	
У1 (УК-3) УМЕТЬ: следовать нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	Отсутствие умений	Фрагментарное следование нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	В целом успешное, но не систематическое следование нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	В целом успешное, но содержащее отдельные пробелы умение следовать основным нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	Успешное и систематическое следование нормам, принятым в научном общении, для успешной работы в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	

У2 (УК-3) УМЕТЬ: осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	Отсутствие умений	Частично освоенное умение осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	В целом успешное, но не систематическое умение осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	В целом успешное, но содержащее отдельные пробелы умение осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	Успешное и систематическое умение осуществлять личностный выбор в процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	
З1 (ОПК-1) ЗНАТЬ: основные понятия, результаты и задачи информационной безопасности	Отсутствие знаний	Фрагментарные представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях	Неполные представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях	Сформированные, но содержащие отдельные пробелы представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях	Сформированные систематические представления о результатах, проблемах, методах научных исследований в области информационной безопасности и смежных областях	
У1 (ОПК-1) УМЕТЬ: применять основные математические методы и алгоритмы для решения стандартных задач информационной безопасности	Отсутствие умений	Фрагментарное умение разработки и применения методов и алгоритмов научных исследований	В целом успешное, но не систематическое умение разработки и применения методов и алгоритмов научных исследований	В целом успешное, но содержащее отдельные пробелы умение разработки и применения методов и алгоритмов научных исследований	Сформированное умение разработки и применения методов и алгоритмов научных исследований	

В1 (ОПК-1) ВЛАДЕТЬ: методами математического моделирования	Отсутствие навыков	Фрагментарное применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств	В целом успешное, но не систематическое применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств	В целом успешное, но содержащее отдельные пробелы применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств	Успешное и систематическое применение навыков построения и анализа математических моделей, решения задач при помощи современных программных средств	
З8 (ПК-051319) ЗНАТЬ: основные понятия, решаемые задачи, нормативные основы и программно-технические методы криптографической защиты информации	Отсутствие знаний о предмете	Фрагментарные представления о предмете	Неполные представления о предмете	Сформированные, но содержащие отдельные пробелы представления о предмете	Сформированные систематические представления о предмете	Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале)
З9 (ПК-051319) ЗНАТЬ: теоретические основы и подходы к практической реализации криптографических примитивов и протоколов	Отсутствие знаний о предмете	Фрагментарные представления о предмете	Неполные представления о предмете	Сформированные, но содержащие отдельные пробелы представления о предмете	Сформированные систематические представления о предмете	Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале)
З10 (ПК-051319) ЗНАТЬ: основные принципы, режимы работы и особенности практической реализации симметричных и асимметричных криптосистем в задачах шифрования и электронной цифровой подписи	Отсутствие знаний о предмете	Фрагментарные представления о предмете	Неполные представления о предмете	Сформированные, но содержащие отдельные пробелы представления о предмете	Сформированные систематические представления о предмете	Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале)

З11 (ПК-051319) ЗНАТЬ: основные принципы и особенности реализации криптографических методов идентификации и аутентификации в компьютерных системах	Отсутствие знаний о предмете	Фрагментарные представления о предмете	Неполные представления о предмете	Сформированные, но содержащие отдельные пробелы представления о предмете	Сформированные систематические представления о предмете	Экзамен в форме индивидуального собеседования (оценка по пятибалльной шкале)

12. Ресурсное обеспечение:

- Перечень основной и дополнительной учебной литературы.

1) Основы информационной безопасности: учебное пособие. / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.: ил. – (Серия «Основы информационных технологий»).

2) Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.

3) Б. Шнайер. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С. 2-е изд. / Под редакцией П. В. Семьянова. – М.: Триумф, 2002.

4) Методы дискретной математики в криптологии. / В. М. Фомичев. – М.: Диалог-МИФИ, 2010. – 424 с.

5) Введение в криптографию. 3-е изд., дополненное. / Под редакцией Ященко В.В. - М.: МЦНМО, 2000.

13. Язык преподавания: русский.

14. Преподаватель (преподаватели):

д.ф.-м.н., проф. В.А.Васенин; к.ф.-м.н., с.н.с. А.В.Галатенко; к.ф.-м.н., с.н.с. Ф.М.Пучков; к.ф.-м.н., с.н.с. К.А.Шапченко.