Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**Пермский национальный исследовательский
политехнический университет**

Факультет прикладной математики и механики
Кафедра «Высшая математика»

УТВЕРЖДАЮ
Проректор по учебной работе
д-р техн. наук, проф.
_____ Н. В. Лобов
«_03_» _02_ 2017 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Криптографические методы защиты информации»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программа бакалавриата (специалитета) – академическая
Направление бакалавриата (специалитета):
10.03.01 «Информационная безопасность»
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль программы бакалавриата: «Комплексная защита объектов информатизации»

Профиль программы специалитета: «Обеспечение информационной безопасности распределенных информационных систем»

Квалификация выпускника: Бакалавр, специалист по защите информации

Выпускающая кафедра: «Автоматика и телемеханика»

Форма обучения: очная

Курс: 3. **Семестр**: 6
Трудоёмкость:
Кредитов по рабочему учебному плану: 6 ЗЕ
Часов по рабочему учебному плану: 216 ч.

Виды контроля:
Экзамен: **- 6** Зачёт: **-** Курсовой проект: **-** Курсовая работа: **- 6**

Пермь
2017

Рабочая программа дисциплины «Криптографические методы защиты информации» разработана на основании:

- федеральных государственных образовательных стандартов высшего образования, утверждённых приказами Министерства образования и науки Российской Федерации по направлениям подготовки:

«1» декабря 2016 г. номер приказа «1515» по направлению 10.03.01 «Информационная безопасность (уровень бакалавриата)»;

«1» декабря 2016 г. номер приказа «1509» по направлению 10.05.03 «Информационная безопасность автоматизированных систем (уровень специалитета)»;

- компетентностной модели выпускника ОПОП по направлению 10.03.01 «Информационная безопасность (уровень бакалавриата)», профиль программы бакалавриата «Комплексная защита объектов информатизации», утвержденной «24» июня 2013 г (с изменениями в связи с переходом на ФГОС ВО);
- компетентностной модели выпускника ОПОП по направлению 10.05.03 «Информационная безопасность автоматизированных систем (уровень специалитета)», профиль программы специалитета «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г (с изменениями в связи с переходом на ФГОС ВО);
- базового учебного плана очной формы обучения по направлению 10.03.01 «Информационная безопасность (уровень бакалавриата)», профиль подготовки бакалавров «Комплексная защита объектов информатизации», утвержденного «22» декабря 2016 г.;
- базового учебного плана очной формы обучения по направлению 10.05.03 «Информационная безопасность автоматизированных систем (уровень специалитета)», профиль программы специалитета «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «22» декабря 2016 г.

Рабочая программа согласована с рабочими программами дисциплин:

- для направления 10.03.01 «Информационная безопасность (уровень бакалавриата)», профиль подготовки бакалавров «Комплексная защита объектов информатизации»: Теория вероятностей, математическая статистика и случайные процессы, Математика 1 (Математический анализ), Математика 2 (Алгебра и геометрия), Дискретная математика, Начертательная геометрия, инженерная и компьютерная графика, Физические основы микроэлектроники, Математическая логика и теория алгоритмов, Теория систем массового обслуживания, Подготовка к защите выпускной квалификационной работы, Вычислительная техника и информационные технологии, Технические средства охраны, Физические основы микроэлектроники, Математические основы теории систем, Прикладные задачи в области инфокоммуникационных и информационно-управляющих систем, Программно-аппаратные средства защиты информации, Техническая защита информации;
- для направления 10.05.03 «Информационная безопасность автоматизированных систем (уровень специалитета)», профиль программы специалитета «Обеспечение информационной безопасности распределенных информационных систем»: Математика 1 (Математический анализ), Теория вероятностей, математическая статистика и случайные процессы, процессы, Математика 2 (Алгебра и геометрия), Дискретная математика, Техническая защита информации 2, Математическая логика и теория алгоритмов, Инженерная и компьютерная графика, Исследование операций и теории игр, Теория графов и ее приложения, Математические основы теории систем, Прикладные задачи в области инфокоммуникационных и информационно-управляющих систем, Физико-технические эффекты, Физика колебаний и волн, Подготовка к защите выпускной квалификационной работы, Разработка и эксплуатация защищенных автоматизированных систем, Преддипломная практика;

Разработчики	канд. физ.-мат.наук, доц. (учёная степень, звание)	 (подпись)	Е.Л. Кротова (инициалы, фамилия)
Рецензент	канд. физ.-мат.наук, доц. (учёная степень, звание)	 (подпись)	Е.Г. Цылова (инициалы, фамилия)

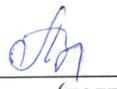
Рабочая программа рассмотрена и одобрена на заседании кафедры

«Высшая математика» « 27 » 12 20 16 г., протокол № 5

Заведующий кафедрой «Высшая математика», ведущей дисциплину д-р физ.-мат. наук, проф. (учёная степень, звание)	 (подпись)	А.Р. Абдуллаев (инициалы, фамилия)

Рабочая программа одобрена учебно – методической комиссией факультета

прикладной математики и механики « 19 » января 20 17 г., протокол № 7

Председатель учебно-методической комиссии факультета прикладной математики и механики канд. физ.-мат. наук, доц. (учёная степень, звание)	 (подпись)	Э.В. Плехова (инициалы, фамилия)

СОГЛАСОВАНО Заведующий выпускающей кафедрой «Автоматика и телемеханика» д-р техн. наук, проф. (учёная степень, звание)	 (подпись)	А.А. Южаков (инициалы, фамилия)
Начальник управления образовательных программ, канд. техн. наук, доц.		Д.С. Репецкий

1. Общие положения

1.1. Цель учебной дисциплины

Овладение основным математическим аппаратом исследования формализованных структур, формирование логического и системного мышления студентов. Целью преподавания дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

В процессе изучения данной дисциплины студент формирует части следующих компетенций по направлениям подготовки:

Таблица 1.1 –*Общепрофессиональные и профессиональные компетенции, заданные ФГОС ВО по направлениям подготовки*

№	Код направления	Наименование направления, профиля	Компетенции, формируемые на основании базовых учебных планов	
			Код компетенции	Формулировка компетенции
1	10.03.01	Информационная безопасность, Комплексная защита объектов информатизации	ОПК-2	- Способность применять соответствующий математический аппарат для решения профессиональных задач;
			ПК-1	- Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
2	10.05.03	Информационная безопасность автоматизированных систем, Обеспечение информационной безопасности распределенных информационных систем	ОПК-2	- Способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники;
			ПК-9	- Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;

В целях унификации на основании базовых компетенций выпускника, определенных ФГОС ВО по направлениям подготовки, разработаны следующие унифицированные компетенции (УК)

– способность применять соответствующий математический аппарат при решении профессиональных задач, в том числе с использованием вычислительной техники; (УК-1);

– способность выполнять работы по установке, настройке и обслуживанию защищенных автоматизированных систем (УК-2).

Таблица 1.2. - *Обоснование разработки унифицированных компетенций*

№	Направление подготовки		Соответствие унифицированной компетенции и базовой компетенции ФГОС ВО	
	Код направления	**Наименование направления, профиля подготовки**	**способность применять соответствующий математический аппарат при решении профессиональных задач, в том числе с использованием вычислительной техники; (УК-1)**	**способность выполнять работы по установке, настройке и обслуживанию защищенных автоматизированных систем (УК-2)**
1	10.03.01	Информационная безопасность, Комплексная защита объектов информатизации	Способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
2	10.05.03	Информационная безопасность автоматизированных систем, Обеспечение информационной безопасности распределенных информационных систем	Способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

1.2. Задачи учебной дисциплины

- ***Формирование знаний в области:***
  - принципов синтеза и анализа шифров;
- ***Формирование умений:***
  - применять математические методы, используемые в криптоанализе;
- ***Формирование навыков:***
  - системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов.

1.3 Предметом освоения учебной дисциплины являются следующие объекты:

– алгоритмы поточного шифрования;

- алгоритмы блочного шифрования;
- алгоритмы вероятностного шифрования;
- криптографические протоколы.

1.4 Место учебной дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к *базовой* части Блока 1. «Дисциплины (модули)» и является *обязательной* при освоении ОПОП по направлениям подготовки.

В таблице 1.2 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.2 – *Дисциплины, направленные на формирование компетенций*

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины
УК-1	способность применять соответствующий математический аппарат при решении профессиональных задач, в том числе с использованием вычислительной техники	Математика 2 (Алгебра и геометрия), Математика 1 (Математический анализ), Теория вероятностей, математическая статистика и случайные процессы, Дискретная математика, Начертательная геометрия, инженерная и компьютерная графика, Физические основы микроэлектроники, Математическая логика и теория алгоритмов, Математические основы теории систем, Прикладные задачи в области инфокоммуникационных и информационно-управляющих систем, Физико-технические эффекты, Физика колебаний и волн, Инженерная и компьютерная графика	Теория систем массового обслуживания, Подготовка к защите выпускной квалификационной работы, Исследование операций и теории игр, Теория графов и ее приложения
УК-2	способность выполнять работы по установке, настройке и обслуживанию защищенных автоматизированных систем	Технические средства охраны, Вычислительная техника и информационные технологии Программно-аппаратные средства защиты информации, Техническая защита информации	Подготовка к защите выпускной квалификационной работы, Разработка и эксплуатация защищенных автоматизированных систем, Техническая защита информации 2, Преддипломная практика

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

Учебная дисциплина обеспечивает формирование унифицированных компетенций УК-1, УК-2.

2.1. Дисциплинарная карта компетенции УК-1

КОД	Формулировка унифицированной дисциплинарной компетенции:
УК-1.Б1.Б.24	*способность применять соответствующий математический аппарат при решении профессиональных задач, в том числе с использованием вычислительной техники*

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения дисциплины студент должен **Знать:** – алгебру в кольце вычетов на поле целых чисел; – основные алгебраические действия в кольце целочисленных вычетов; – основные методы факторизации;	*Лекция.* *Практические занятия.* *Самостоятельная работа студентов по изучению теоретического материала.*	*Контрольные вопросы к текущему и промежуточному контролю.*
Уметь: – вычислять вычет в целочисленном кольце; – формулировать постановки задач криптоанализа и находить подходы к их решению;	*Практические занятия.* *Самостоятельная работа студентов (подготовка к лекциям, практическим занятиям).*	*Типовые задания к контрольным работам.* *Курсовая работа* *Типовые задачи к экзамену.*
Владеть: – методами криптоанализа простейших шифров.	*Практические занятия.* *Самостоятельная работа студентов по подготовке к экзамену.*	*Курсовая работа* *Типовые задачи к экзамену.*

2.2. Дисциплинарная карта компетенции УК-2:

КОД	Формулировка унифицированной дисциплинарной компетенции:
УК-2.Б1.Б.24	*способность выполнять работы по установке, настройке и обслуживанию защищенных автоматизированных систем*

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент должен **Знать:** – основные принципы построения криптоалгоритмов; – основные методы дешифрования; стандарты систем шифрования; – теорему Кука, *NP*-полноту; – вероятностное шифрование;	*Лекция.* *Практические занятия.* *Самостоятельная работа студентов по изучению теоретического материала.*	*Контрольные вопросы к текущему и промежуточному контролю.*
Уметь: – строить современные шифрсистемы; – формулировать постановки задач криптоанализа и находить подходы к их решению;	*Практические занятия.* *Самостоятельная работа студентов (подготовка к лекциям, практическим занятиям).*	*Типовые задания к контрольным работам.* *Курсовая работа* *Типовые задачи к экзамену.*
Владеть: – криптографической терминологией; методами криптоанализа простейших шифров; современной научно-технической литературой в области криптографической защиты.	*Практические занятия.* *Самостоятельная работа студентов по подготовке к экзамену.*	*Курсовая работа* *Типовые задачи к экзамену.*

3. Структура учебной дисциплины по видам и формам учебной работы

Объем дисциплины в зачетных единицах составляет 6 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.

Таблица 3.1 – *Объём и виды учебной работы*

№ п/п	Виды учебной работы	Трудоемкость	
		по семестрам	всего
1	2	3	4
		6 семестр	
1	**Аудиторная (контактная) работа**	**60**	**60**
	-в том числе в интерактивной форме	27	27
	Лекции (ЛК)	28	28
	-в том числе в интерактивной форме	16	16
	Практические занятия (ПЗ)	32	32
	-в том числе в интерактивной форме	11	11
2	**Контроль самостоятельной работы (КСР)**	**4**	**4**
3	**Самостоятельная работа (СРС)**	**116**	**116**
	- изучение теоретического материала	49	**49**
	- курсовая работа	18	**18**
	- подготовка к аудиторным занятиям (лекциям, практическим)	49	**49**
4	**Промежуточная аттестация (итоговый контроль) по дисциплине:** ***экзамен***	36	**36**
5	**Трудоемкость дисциплины, всего:** **в часах (Ч)** **в зачётных единицах (ЗЕ)**	**216** **6**	**216** **6**

4 Содержание учебной дисциплины

4.1 Модульный тематический план

Таблица 4.1 – *Тематический план по модулям учебной дисциплины*

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов и виды занятий (очная форма обучения)							Трудоемк., ч./ з.е.
			Аудиторная работа				КСР	Итоговый контроль	Самостоятельная работа (СРС)	
			Всего	Лк	ПЗ	ЛР				
1	2	3	4	5	6	7	8	9	10	
1	1	Тема 1	3	1	1				6	**9**
		Тема 2	3	1	1				6	**9**
		Тема 3	3	2	2				6	**9**
	2	Тема 4	3	1	1				6	**9**
		Тема 5	3	1	1				6	**9**
		Тема 6	6	2	2		2		6	**14**
	Всего по модулю		**18**	**8**	**8**		**2**		**36**	**56/1,5**
2	3	Тема 7	6	1	2				6	**12**
		Тема 8	6	1	1				6	**12**
		Тема 9	3	1	1				6	**9**
	4	Тема 10	6	2	2				6	**12**
		Тема 11	6	2	2				6	**12**
		Тема 12	3	2	2				6	**9**
		Тема 13	6	2	2				6	**12**
		Тема 14	9	2	2				6	**15**
	Всего по модулю		**27**	**13**	**14**				**48**	**75/2**
3	5	Тема 15	6	1	2				6	**12**
		Тема 16	6	1	2				6	**12**
		Тема 17	9	2	2				6	**15**
		Тема 18	9	1	2		2		6	**17**
	6	Тема 19	6	2	2				8	**14**
	Всего по модулю		**19**	**7**	**10**		**2**		**32**	**53/1,5**
Промежуточная аттестация (итоговый контроль): ***экзамен***								**36**		**36/1**
ИТОГО			**64**	**28**	**32**		**4**	**36**	**116**	**216/6**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Введение в криптографию. Основные классы шифров и их свойства.

Раздел 1. Введение в криптографию.

ЛК - 4 часа, ПЗ - 4 часа, СРС – 18 часов.

Введение. Основные понятия, термины, определения. Предмет и задачи дисциплины.

Тема 1. ИЗ ИСТОРИИ КРИПТОГРАФИИ. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности.

Тема 2. ОТКРЫТЫЕ СООБЩЕНИЯ И ИХ ХАРАКТЕРИСТИКИ. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.

Тема 3. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИИ. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.

Раздел 2. Основные классы шифров и их свойства.

ЛК - 4 часа, ПЗ - 4 часа, СРС - 18 часов.

Тема 4. ШИФРЫ ПЕРЕСТАНОВКИ. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки.

Тема 5. ШИФРЫ ЗАМЕНЫ. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические).

Тема 6. ПОТОЧНЫЕ ШИФРЫ. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.

Модуль 2. Надежность шифров. Принципы построения криптографических алгоритмов.

Раздел 3. Надежность шифров.

ЛК – 3 часа, ПЗ – 4 часа, СРС – 18 часов.

Тема 7. ТЕОРИЯ К.ШЕННОНА. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности.

Тема 8. ИМИТОСТОЙКОСТЬ ШИФРОВ. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования.

Тема 9. ПОМЕХОУСТОЙЧИВОСТЬ ШИФРОВ. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.

Раздел 4. Принципы построения криптографических алгоритмов.

ЛК – 10 часов, ПЗ – 10 часов, СРС – 30 часов.

Тема 10. РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ. Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров.

Тема 11. ВОПРОСЫ СИНТЕЗА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ. Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Проверка построенной последовательности на случайность.

Тема 12. МЕТОДЫ УСЛОЖНЕНИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ. Связь между качеством

последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнений последовательности. Различные способы задания дискретных функций.

Тема 13. МЕТОДЫ АНАЛИЗА КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ. Понятие криптоатаки. Виды криптоатак. Классификация криптоатак. Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уравнений шифрования, бесключевые методы. Особенности криптоанализа блочных шифров. Криптографические параметры узлов и блоков шифраторов. Основные принципы построения криптоалгоритмов (выбор группы шифра, параметров ПСП, параметров функции усложнения)

Тема 14. СИСТЕМЫ ШИФРОВАНИЯ С ОТКРЫТЫМИ КЛЮЧАМИ. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Секретные характеристики в системах с открытым ключом. Преимущества ассиметричных систем шифрования. Вероятностное шифрование.

Модуль 3. Криптографические протоколы.

Раздел 5. Криптографические протоколы.

ЛК - 5 часов, ПЗ – 8 часов, СРС – 24 часа.

Тема 15. МОДЕЛИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ. Сложность криптографических алгоритмов (теорема Кука, NP-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов.

Тема 16. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения.

Тема 17. ПРОТОКОЛЫ УСТАНОВЛЕНИЯ ПОДЛИННОСТИ. Парольные системы разграничения доступа и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и ЭЦП.

Тема 18. ПРОТОКОЛЫ УПРАВЛЕНИЯ КЛЮЧАМИ. Протоколы сертификации ключей. Протоколы распределения ключей. Открытое распределение ключей Диффи-Хэлмана и его модификация. Протоколы Oakley, ISAKMP.

Раздел 6. Заключение.

ЛК - 2 часа, ПЗ - 2 часа, СРС - 8 часов.

Тема 19. ЗАКЛЮЧЕНИЕ. Проблемы и перспективы исследований в области современной криптографии. Квантовая криптография. Стеганография. Нерешенные задачи. Итоги изучения курса.

4.3. Перечень тем практических занятий.

Таблица 4.2 – *Темы практических занятий*

Модуль	№ ПЗ	Номер темы дисциплины	Наименование темы практического занятия
1	1	1,2	Простейшие шифры и их свойства. Типы атак. Атаки, в основе которых лежит парадокс задачи о днях рождения. Двусторонние атаки. Уровень безопасности. Освоение процессов зашифрования и расшифрования для простейших шифров.

1	2	2,3	Частотные свойства осмысленных сообщений.
1	3	3,4	Криптоанализ шифра однобуквенной простой замены.
1	4	4,5	Криптоанализ шифра «решетка Кардано».
1	5	5,6	Вскрытие шифра Вернама при повторном использовании ключа. Криптоанализ шифра Виженера.
2	6	7,8	Шифры, основанные на алгоритме Файстеля. Функция раунда. Реализация функции раунда. Традиционные симметричные блочные шифры.
2	7	9,10	Расчет метода встречных атак.
2	8	10,11	Канальное и сквозное шифрование. Управление секретными ключами. Криптоанализ рассмотренных алгоритмов симметричного шифрования. Размер ключа.
2	9	12,13	Цифровые подписи. Управление ключами. Взлом ключа. Согласование ключей с помощью пароля. Защищенные функции хэширования. HMAC. SHA. MD5. RIPEMD. UMAC.Криптография с открытым ключом.
3	10	14,15	Обмен ключами. Схема Диффи-Хеллмана. Протокол обмена ключами Oakley, ISAKMP.
3	11	15,16	Серверы ключей. Система Kerberos. Сервис аутентификации X.509.
3	12	17,18	Стохастическое преобразование информации. R-блоки. Гаммирование. Вероятностное шифрование.
3	13	18,19	Изучение системы PGP.

4.4 Перечень тем лабораторных работ

Не предусмотрены.

4.5. Виды самостоятельной работы студентов

Таблица 4.3. – *Виды самостоятельной работы студентов (СРС)*

Номер темы дисциплины	Вид самостоятельной работы студентов	Трудоемкость, часов
1	2	3
1	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
2	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
3	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
4	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
5	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
6	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
7	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
8	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
9	Изучение теоретического материала	3

	Подготовка к аудиторным занятиям	3
10	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
11	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
12	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
13	Изучение теоретического материала	3
	Подготовка к аудиторным занятиям	3
14	Изучение теоретического материала	3
	Подготовка курсовой работы	3
15	Изучение теоретического материала	3
	Подготовка курсовой работы	3
16	Изучение теоретического материала	3
	Подготовка курсовой работы	3
17	Подготовка к аудиторным занятиям	1
	Подготовка курсовой работы	3
18	Подготовка к аудиторным занятиям	3
	Подготовка курсовой работы	3
19	Изучение теоретического материала	1
	Подготовка к аудиторным занятиям	3
	Подготовка курсовой работы	3
	Итого: в ч./в ЗЕ	116/3,2

4.5.1. Изучение теоретического материала

Тематика для самостоятельного изучения дисциплины:

Тема 1. Классификация видов информации подлежащей шифрованию.

Тема 2. Частотные характеристики открытых текстов, содержащих информацию на английском языке.

Тема 3. Режим электронного сцепления блоков. Самосинхронизирующиеся поточные шифры.

Тема 6. Статистические тесты на проверку распределения гаммы.

Тема 7. Теорема об избыточности. Подходы к доказательству.

Тема 9. Варианты случайного распределения помех.

Тема 10. Альтернативные варианты алгоритмов шифрования, основанных на схеме Файстеля, их основные характеристики.

Тема 13. Классические варианты криптоатак, распространенные в сети.

Тема 14. Недостатки систем шифрования с открытым ключом.

Тема 15. P-полные языки.

Тема 16. ЭЦП Эль-Гамаля.

Тема 17. Протокол POP3.

4.5. 2 Курсовая работа

Перечень тем курсовых работ:

1. Пример реализации защиты информации на предприятии (представить свой вариант ПО позволяющего защитить секретные данные от несанкционированного копирования, в качестве варианта использовать предприятие, работающее на 1С, не исключать использование копирования информации на электронные носители и выход в Интернет).

2. Брандмауэры.
3. Троянские кони. Принцип действия. Защита
4. Черви. Принцип действия. Защита
5. Криптосистемы с открытым ключом (ассиметричные).
6. Свойства конструкции безусловно стойких шифров, названных К.Шенноном совершенными, по отношению к различным криптоатакам.
7. Квантовая криптография.
8. Цифровая подпись. Реализация. Плюсы и минусы ее использования.
9. Вероятностное шифрование.
10. Криптографическое сжатие. Алгоритмы сжатия данных. Арифметическое кодирование.
11. Беспроводные сети. Атаки. Механизмы обеспечения защиты информации. Протокол WEP.
12. Последние разработки в криптографии (разбор современнейших подходов к шифрованию, исключая квантовое).
13. Модель обработки сообщений и защиты пользователя. Управление доступом на основе представлений.
14. Режим сцепления шифрованных блоков. Электронная шифровальная книга.

5. Методические указания для обучающихся по изучению дисциплины

5.1. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению курсовой работы, выполнению домашних заданий по практическим занятиям.
4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п.7.
5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

5.2. Образовательные технологии, используемые для формирования компетенций

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

Лекция – передача учебной информации от преподавателя к студентам, как правило, с использованием компьютерных и технических средств, направленная в основном на приобретение студентами знаний.

Практическое занятие – решение конкретных задач на основании теоретических и фактических знаний, направленное в основном на приобретение новых знаний и умений.

Самостоятельная работа – изучение студентами теоретического материала, подготовка к лекциям, практическим занятиям, решение расчетно-графических работ.

Консультация – индивидуальное общение преподавателя со студентом, руководство его деятельностью с целью передачи опыта, углубления знаний, приобретенных студентом на лекциях, в результате самостоятельной работы.

Информационные технологии – обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки и объективного контроля и мониторинга знаний студентов.

6. Фонд оценочных средств дисциплины

6.1. Текущий контроль освоения заданных дисциплинарных частей компетенций

Текущий контроль освоения унифицированных дисциплинарных компетенций проводится в следующих формах:

- опрос, текущая контрольная работа по теории для анализа усвоения предыдущей лекции;

6.2 Рубежный контроль освоения заданных дисциплинарных частей компетенций

Рубежный контроль освоения дисциплинарных частей компетенций проводится по окончании модулей дисциплины в следующих формах:

- контрольные работы;

Перечень контрольных работ

Таблица 6.1. – *Перечень контрольных работ*

№ п/п	Номер модуля	Номера разделов	Наименование материалов контроля
1.	1	1	Коллоквиум по классическим системам шифрования: решетка Кардано, шифр Вернама, шифр Виженера, гаммы.
2.	1	1	Контрольная работа по симметричным шифрам (DES, тройной DES, IDEA, BLOWFISH).
3.	2	1	Коллоквиум по надежности шифров (теорема К.Шеннона, совершенные шифры, безусловно стойкие шифры, имитостойкость, помехоустойчивость).
3.	2	1	Коллоквиум по криптоанализу (синтез шифров, линейный конгруэнтный метод, перебор ключей, «встреча посередине», атака по неполным данным, функции усложнения).
3.	3	1	Контрольная работа по ЭЦП и протоколам обмена ключами.

6.3. Итоговый контроль освоения заданных дисциплинарных компетенций.

а) Зачет не предусмотрен.

б) Экзамен.

Экзамен проводится в устной форме по билетам. До экзамена допускаются студенты, положительно сдавшие все виды рубежного контроля (3 предусмотренных коллоквиума и 2 контрольные работы). Билет содержит два теоретических вопроса и одно практическое задание.

Фонды оценочных средств, включающие типовые задания к расчетно-графическим работам, контрольные работы, тесты, перечень вопросов к экзамену, практические задания к экзамену, методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, позволяющие оценить результаты освоения данной дисциплины, входят в состав РПД в виде приложения.

6.4. Виды текущего, промежуточного и итогового контроля освоения компонентов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	**Вид контроля**			
	Текущий	**Рубежный**	**Итоговый**	
	ТК	**РКР**	**КР**	**Экзамен**
Знает:				
алгебру в кольце вычетов на поле целых чисел.	+			+
основные алгебраические действия в кольце целочисленных вычетов.	+			+
основные методы факторизации.	+			+
основные принципы построения криптоалгоритмов	+			+
основные методы дешифрования; стандарты систем шифрования	+			+
теорема Кука, *NP*-полнота	+			+
вероятностное шифрование	+			+
Умеет:				
вычислять вычет в целочисленном кольце.		+ +	+	+
формулировать постановки задач криптоанализа и находить подходы к их решению.		+ +	+	+
строить современные шифрсистемы		+ +	+	+
формулировать постановки задач криптоанализа и находить подходы к их решению		+ +	+	+
Владеет:				
методами криптоанализа простейших шифров		+	+	+
криптографической терминологией; методами криптоанализа простейших шифров; современной научно-технической литературой в области криптографической защиты		+	+	+

ТК – текущий контроль в форме контрольных работ по теории (оценка знаний);

КР- курсовая работа (оценка умений и владений);

РКР – рубежный контроль в форме контрольных работ по практическим занятиям (оценка умений, навыков).

7. График учебного процесса по дисциплине

Таблица 7.1. - *График учебного процесса по дисциплине*

Виды работ	1 семестр. Распределение по учебным неделям.																		Итого
	24	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	
Разделы	Р1		Р2		Р3		Р4				Р5						Р6		
Лекции	2	2	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	28
Практ. занятия	2	2	2	2	2	2	2	2	2	2	2	1	2	1	2	1	2	1	32
КСР										2								2	4
Подготовка к занятиям	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	1	49
Изучение теоретического материала	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	2	49
КР									4				3	3	3	3	3	3	18
Модули	М1				М2						М3								
Рубежный контроль					+						+							+	
Промежуточная аттестация *экзамен*																			36

8. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б1.Б.24 *Криптографические методы защиты информации*	***Блок1. Дисциплины (модули)*** (*цикл дисциплины*)			
(*полное название дисциплины*)	[x]	базовая часть цикла	[x]	обязательная
	[ ]	вариативная часть цикла	[ ]	по выбору студента

10.03.01 ***10.05.03*** (*код направления / специальности*)	***Информационная безопасность/Комплексная защита объектов информатизации*** ***Информационная безопасность автоматизированных систем/Обеспечение информационной безопасности распределенных информационных систем*** (*полное название направления подготовки / специальности*)

ИБ/КЗИ КОБ/КОБ (*аббревиатура направления / специальности*)	Уровень подготовки			Форма обучения		
	[x]	специалист		[x]	очная	
	[x]	бакалавр		[ ]	заочная	
	[ ]	магистр		[ ]	очно-заочная	

2016 (*год утверждения учебного плана ОПОП*)

Семестр *6*

Количество групп 2

Количество студентов 50

Кротова Е. Л. (*фамилия, инициалы преподавателя*)	Доцент (*должность*)
ФПММ (*факультет*)	
Высшая математика (*кафедра*)	239-16-97 (*контактная информация*)

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

№	**Библиографическое описание** *(автор, заглавие, вид издания, место, издательство, год издания, количество страниц)*	**Количество экземпляров** в библиотеке+на кафедре; **местонахождение электронных изданий**
1	2	3
	1 Основная литература	
1.	Данилов, Александр Николаевич. Математические основы криптологии и криптографические методы и средства обеспечения информационной безопасности: учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин; Пермский государственный технический университет. - Пермь: Изд-во ПГТУ, 2008. - 363 с.	100
2.	Данилов, Александр Николаевич. Практикум по курсам «Математические основы криптологии» и «Криптографические методы и средства обеспечения информационной безопасности»: учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин; Пермский государственный технический университет. - Пермь: Изд-во ПГТУ, 2008. - 238 с.	100
3.	Смарт, Найджел. Криптография: пер. с англ. / Н. Смарт. - М.: Техносфера, 2006. - 525 с	5
	Рябко, Борис Яковлевич. Криптографические методы защиты информации: учебное пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - Москва: Горячая линия-Телеком, 2015. - 229 с.	25
	Гашков, Сергей Борисович. Криптографические методы защиты информации: учебное пособие для вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва: Академия, 2010. - 298 с.	8
	2 Дополнительная литература	
	2.1 Учебные и научные издания	
1.	Розанов, Юрий Анатольевич. Случайные процессы. Краткий курс: учебное пособие для вузов / Ю. А. Розанов. - Москва: Наука, 1971. - 286 с.	4
2.	Росошек, С. К. Специальные главы математики. (Математические основы криптографии): учебное пособие / С.К. Росошек; Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС). - Томск: В-Спектр: Изд-во ТУСУР, 2006. Ч. 1. - 2006. - 92 с.	5
	Росошек, С. К. Специальные главы математики. (Математические основы криптографии): учебное пособие / С.К. Росошек; Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной	5

	информационной безопасности электронно-вычислительных систем (КИБЭВС). - Томск: Изд-во ТУСУР, 2005. Ч. 2. - 2005. - 190 с.	
2.2 Периодические издания		
	Не используются.	
2.3 Нормативно-технические издания		
	Не используются.	
2.4 Официальные издания		
	Не используются.	
2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины		
1.	Электронная библиотека Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс: полнотекстовая база данных электрон. документов, изданных в Изд-ве ПНИПУ]. - Электрон. дан. (1 912 записей). - Пермь, 2014. - Режим доступа: http://elib.pstu.ru/. - Загл. с экрана.	

Основные данные об обеспеченности на _____
(*дата составления рабочей программы*)

основная литература [*x*] обеспечена [ ] не обеспечена

дополнительная литература [*x*] обеспечена [ ] не обеспечена

Зав. отделом комплектования
Научной библиотеки _____ Н. В. Тюрикова

Текущие данные об обеспеченности на _____
(*дата составления рабочей программы*)

основная литература [ ] обеспечена [ ] не обеспечена

дополнительная литература [ ] обеспечена [ ] не обеспечена

Зав. отделом комплектования
Научной библиотеки _____ Н. В. Тюрикова

8.3 Компьютерные обучающие и контролирующие программы

Таблица 8.1 – *Программы, используемые для обучения и контроля*

№ п/п	Вид учебного занятия	Наименование библиотечно-информационных ресурсов и средств обеспечения дисциплины	Количество экземпляров, точек доступа	Назначение
1	СР	Электронный каталог АБИС “Руслан”. Универсальное средство поиска	Доступен в сети Интернет	Самостоятельное изучение студентами материала по предмету.

8.4 Аудио- и видео-пособия

Не используются.

9 Материально-техническое обеспечение дисциплины

9.1 Специализированные лаборатории и классы

Не требуется.

9.2 Основное учебное оборудование

Интерактивные доски, проекторы.

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.		
2.		
3.		
4.		
5.		