МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль **Криптографические методы защиты информации**	Код модуля **1135855** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Траектория образовательной программы	**Не предусмотрена**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль
В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Объем модуля, 7 з.е.

1.2. Аннотация содержания модуля

Модуль относится к базовой части образовательной программы. В модуль входит одна дисциплина «Криптографические методы защиты информации», посвященная изучению современных симметричных и асимметричных криптосистем и основ криптоанализа.

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).	Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
		Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
		Лекции	Практические занятия	Лабораторные работы	Всего			Час.	Зач. ед.
1 **(Б)** Криптографические методы защиты информации	6, 7, 8	102		17	119	93	18(Э) 4(З) 18(Э)	252	7
Всего на освоение модуля		102		17	119	93	40	252	7

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	-
3.2.	**Кореквизиты**	-

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

4.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля	Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля
10.05.01/01.02	РО2. Способность применять основополагающие принципы и современные достижения физико-математических наук, математического описания и построения компьютерных систем, а также современные информационные технологии в	ПК-4, способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач;

	разработке технологических решений с использованием программного кода.	ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов; ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.
	РО3. Способность осуществлять проектирование систем защиты информации с учётом актуальных информационных угроз и с использованием современных достижений науки и техники.	ОК-2, способность использовать основы экономических знаний в различных сферах деятельности; ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной

		деятельности, работать с программными средствами общего и специального назначения; ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации; ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем; ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.
	РО6. Способность осуществлять планирование работ по защите	ОК-2, способность использовать основы экономических знаний в

	информации в компьютерных системах.	различных сферах деятельности; ОК-4, способность использовать основы правовых знаний в различных сферах деятельности; ОПК-7, способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; ОПК-8, способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации; ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-13, способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности; ПК-14, способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа; ПК-15, способность разрабатывать предложения по совершенствованию системы управления информационной

		безопасностью компьютерной системы; ПСК-2.2, способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение; ДПК-2, способность к разработке требований и критериев информационной безопасности, согласованных со стратегией развития предприятия.
	РО7. Способность проводить аудит и аттестацию объектов, обеспечивающих информационную безопасность, на соответствие требованиям государственных и/или корпоративных документов, а также устанавливать режим информационной безопасности на предприятии и контролировать его соблюдение.	ОК-4, способность использовать основы правовых знаний в различных сферах деятельности; ОПК-5, способностью использовать нормативные правовые акты в своей профессиональной деятельности; ПК-1, способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности; ПК-2, способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований; ПК-3, способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; ПК-4, способность проводить анализ и участвовать в разработке математических моделей

		безопасности компьютерных систем; ПК-9, способность участвовать в проведении аттестации объектов с учетом требований к уровню защищенности компьютерной системы; ПК-11, способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации; ДПК-3, способность проводить аудит информационной безопасности и составлять итоговые документы аудита, содержащие выводы и рекомендации.
	РО8. Способность к разработке, анализу и обоснованию адекватности математических моделей процессов, возникающих при функционировании программно-аппаратных средств защиты информации, а также к разработке математических моделей для оценки безопасности компьютерных систем.	ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов; ОПК-7, способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; ОПК-8, способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации; ОПК-10, способность к

		самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

		ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

4.2.Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ОК 2,4	ОПК 1,2,4,5,7, 8,9,10	ПК 1,2,3,4,5,6,7,8,9, 11,13,14,15	ПСК 2.1,2.2,2.3, 2.4, 2.5	ДПК 1,2,3
1	**(Б)** Криптографические методы защиты информации	*	*	*	*	*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

Не предусмотрено

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль **Криптографические методы защиты информации**	Код модуля **1135855** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль
В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1.Аннотация содержания дисциплины

Дисциплина «Криптографические методы защиты информации» является единственной дисциплиной одноименного модуля базовой части.

Курс «Криптографические методы защиты информации» посвящен изучению базовых принципов разработки, функционирования, оценок стойкости и эффективности современных симметричных и асимметричных криптосистем. Подробно рассматриваются наиболее употребительные блочные и поточные шифры, а также криптосистемы с публичным ключом. Также изучаются основы создания и наиболее употребительные криптографические хеш-функции, протоколы распределения ключей, идентификации, защиты целостности данных и разделения секрета. Кроме того, изучаются основы криптоанализа.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОК-2, способность использовать основы экономических знаний в различных сферах деятельности;

ОК-4, способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач;

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-5, способностью использовать нормативные правовые акты в своей профессиональной деятельности;

ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач;

ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ПК-1, способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;

ПК-2, способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;

ПК-3, способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности;

ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;
ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
ПК-6, способность участвовать в разработке проектной и технической документации;
ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем;
ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;
ПК-9, способность участвовать в проведении аттестации объектов с учетом требований к уровню защищенности компьютерной системы;
ПК-11, способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации;
ПК-13, способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности;
ПК-14, способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа;
ПК-15, способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы;
ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение;
ДПК-2, способность к разработке требований и критериев информационной безопасности, согласованных со стратегией развития предприятия.
ДПК-3, способность проводить аудит информационной безопасности и составлять итоговые документы аудита, содержащие выводы и рекомендации.
ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;
ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;
ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;
ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

В результате освоения дисциплины студент должен:

Знать:

- основные понятия современной криптологии (криптосистема, симметричная криптосистема, асимметричная криптосистема, совершенный шифр, имитостойкость, помехоустойчивость, протокол, хеш-функция, подпись, атака);
- способы решения основных задач современной криптографии (сохранение секретности, обеспечение целостности, идентификация, создание цифровой подписи, разделение секрета);\
- основные конструкции, используемые в построении современных симметричных

шифров и криптографических хеш-функций, и их свойства (конструкция Файстеля, одношаговый генератор, линейный регистр сдвига, итерационная схема хеш-функции, усиление Меркля-Дамгарда, конструкции Матиаса-Мейера-Осеаса, Девиса-Мейера и Миягучи-Пренеля);

- устройство современных блочных шифров, поточных шифров и криптографических хэш-функций (DES, ГОСТ-28147-89, IDEA, AES, A5, RC4, MDC-2,MDC-4, MD4,MD5, SHA, ГОСТ Р 34.11-94);

Уметь:

- производить анализ шифра на совершенство и имитостойкость;
- реализовывать алгоритмы для работы с современными асимметричными криптосистемами (КС) и подписями на их основе (КС RSA, КС Рабина, КС Эль-Гамаля, КС Блюма-Голдвассер, КС Голдвассер-Микали, КС Мак-Элиса. ЭЦП RSA, SHA, ГОСТ 34.10-94, ГОСТ 34.10-2012);
- реализовывать алгоритмы идентификации с нулевым разглашением и распределения ключей в системе Блома и на основе пересечения множеств;

Владеть:

- навыками криптоанализа базовых исторических шифров, и выработки пар ключей в современных асимметричных криптосистемах;

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)		
		Всего часов	В т.ч. контактная работа (час.)*	6 семестр	7 семестр	8 семестр
1.	**Аудиторные занятия**	**119**	**119**	**51**	**34**	**34**
2.	Лекции	102	102	34	34	34
3.	Практические занятия					
4.	Лабораторные работы	17	17	17		
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**93**	**17,85**	**39**	**34**	**20**
6.	**Промежуточная аттестация**	**40**	**4,91**	**Э(18)**	**З(4)**	**Э(18)**
7.	**Общий объем по учебному плану, час.**	**252**	**141,76**	**108**	**72**	**72**
8.	**Общий объем по учебному плану, з.е.**	**7**		**3**	**2**	**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1. Основы традиционной криптографии		
Р1.1	**История, основные понятия и задачи криптографии.**	Способы защиты информации (защита носителя, стеганография, криптография). Понятие криптоситемы (шифра). Шифр перестановки. Шифр «скитала». Маршрутные транспозиции. Столбцовые перестановки. Решетки Кардано и Ришелье. Шифр замены. Квадрат Полибия. Шифр Цезаря. Многоалфавитная замена. Диск Алберти. Таблица Тритемия и шифр Виженера. Самоключевой шифр Кардано. Диаграммный шифр Уитстона-Плэйфера. Блочные шифры Хилла. Шифр Вернама (одноразовый щит). Дисковые шифраторы. Понятие криптоанализа. Классификация атак. Частотный криптоанализ. Криптоанализ шифра замены, шифра перестановки и шифра Виженера (метод Казиски и методы Фридмана).
Р1.2	**Теория Шеннона.**	Информация и энтропия, свойства энтропии. Условная энтропия. Взаимная информация. Взаимная информация между открытым текстом и криптограммой. Остаточная неопределенность ключа и сообщения. Совершенная секретность (абсолютная стойкость) шифра. Описание эндоморфных совершенных криптосистем. Типичные и редкие последовательности в стационарной модели открытого текста. Избыточность языка. Расстояние единственности шифра. Имитостойкость шифра.
Р1.3	**Помехоустойчивые шифры.**	Эндоморфные шифры не распространяющие искажений типа “замена” (Теорема Маркова). Эндоморфные шифры не распространяющие искажений типа “пропуск” (Теорема Глухова).
Р1.4	**Блочные шифры.**	Понятие. Усложнение и рассеивание, Конструкция Файстеля. DES. ГОСТ-28147-89. IDEA. AES. Понятия линейного и дифференциального криптоанализа. Уровень нелинейности булевой функции. Булевы функции, удовлетворяющие строгому лавинному критерию. Режимы использования блочных шифров.
Р2. Поточные шифры и асимметричные криптосистемы		
Р2.1	**Поточные шифры.**	Общая схема поточного шифра. Требования к управляющему блоку. Линейные регистры сдвига и линейные рекуррентные последовательности (ЛРП). Характеристическая матрица и характеристический многочлен однородной ЛРП. Финально-периодические последовательности. Вычисление минимального многочлена и периода ЛРП. ЛРП максимального периода. Их статистические свойства. Усложнения линейных регистров сдвига. Шифр A5. Алгоритм RC4.
Р2.2	**Асимметричные криптосиситемы.**	Новые задачи криптографии и недостаточность традиционных криптосистем. Общие принципы построения криптосистем с открытым ключом. Создание односторонней функции ловушки из сложной задачи на примере рюкзач-

		ной криптосистемы. RSA: построение, связь параметров, бит-безопасность, известные виды атак. КС Рабина (Доказательство надежности). КС Блюма-Голдвассер, КС Голдвассер-Микали, КС Мак-Элиса. КС Эль-Гамаля. Подписи: RSA, Эль-Гамаля, Ниберга-Руппеля, DSS, ГОСТ 34.10-94, ГОСТ 34.10-2012.
Р3. Хеш-функции и базовые протоколы		
Р3.1	**Хеш-функции.**	Понятие и мотивы использования в подписи. Требования к криптографической хеш-функции. Из взаимосвязь. Итерационная схема построения. Усиление Меркля-Дамгарда, конструкции Матиаса-Мейера-Осеаса, Девиса-Мейера и Миягучи-Пренеля. Примеры: MDC-2,MDC-4, MD4,MD5, SHA, ГОСТ Р 34.11-94. Парадокс дней рождений и предельная устойчивость к коллизиям. Атаки на криптографические хеш-функции. Проблема защиты целостности и способы ее решения. Ключевые хеш-функции. Способы построения ключевых хеш-функций из бесключевых.
Р3.2	**Идентификация.**	Протокол идентификации. Пароли. Многоразовые: атаки, правила использования, способы хранения. Одноразовые: обновляемый, запасаемые, схема Лампорта. Проблемы при использовании. Идентификация типа запрос-ответ. Классификация по требованиям и применяемым средствам. Атаки, роль меток времени и случайных чисел. Протоколы с нулевым разглашением. Протокол Фиата-Шамира. Протокол Гвиллоу-Квискватера. Протокол Шнорра. Протокол без установки.
Р3.3	**Распределение ключей.**	Распределение ключей с помощью симметричных криптосистем. Бесключевой протокол Шамира. Распределение ключей с помощью асимметричных криптосистем. Роль доверенных центров. X.509. STS. Распределение ключей Диффи-Хеллмана. Атаки с противником посередине. Протоколы Мацумото-Такашима-Имаи. Предварительное распределение ключей в сети. Схема Блома. Теорема Блома. Схема на основе пересечений множеств. Оценка параметров на основе леммы Шпернера.
Р3.4	**Разделение секрета.**	Задача разделения секрета. Структура доступа и схема разделения секрета. Общая конструкция и матричная форма схемы разделения секрета. Пороговые схемы. Схема Шамира. Пороговые схемы с лгунами. Визуальное разделение секрета. Примеры. Проблема расширяющего множителя. Конструкция на основе квадратичных вычетов.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

6 семестр

Объем модуля (зач.ед.): 3
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязычной литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1.1	История, основные понятия и задачи криптографии.	27,2	14	8		6	13,2	5,2	1,6		3,6		6	1										2	1					
Р1.2	Теория Шеннона.	32,8	18	10		8	14,8	6,8	2,0		4,8		6	1										2	1					
Р1.3	Помехоустойчивые шифры.	9,6	8	8		0	1,6	1,6	1,6		0		0											0						
Р1.4	Блочные шифры.	20,4	11	8		3	9,4	3,4	1,6		1,8		6	1										0						
	Всего (час), без учета промежуточной аттестации**:**	**90,0**	**51**	**34**	**0**	**17**	**39,0**	**17**	**6,8**	**0**	**10,2**	**0**	**18**	**18**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4**	**4**	**0**				
	Всего по дисциплине (час.):	**108**	**51**				**57**	В т.ч. промежуточная аттестация																**0**	**18**	**0**	**0**				

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

7 семестр

Объем модуля (зач.ед.): 2
Объем дисциплины (зач.ед.): 2

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)															Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*				
P2.1	Поточные шифры.	30	16	16			14	3,2	3,2				6,8	1									4	1					
P2.2	Асимметричные криптосистемы.	38	18	18			20	3,6	3,6				12,4	2									4	1					
	Всего (час), без учета промежуточной аттестации:	**68**	**34**	**34**	**0**	**0**	**34**	**6,8**	**6,8**	**0**	**0**	**0**	**19,2**	**19,2**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**8**	**8**	**0**				
	Всего по дисциплине (час.):	**72**	**34**				**38**	В т.ч. промежуточная аттестация																		**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

8 семестр

Объем модуля (зач.ед.): 2
Объем дисциплины (зач.ед.): 2

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р3.1	Хеш-функции.	14,6	8	8			6,6	1,6	1,6				3	1										2	1					
Р3.2	Идентификация.	15,0	10	10			5,0	2,0	2,0				3	1										0						
Р3.3	Распределение ключей.	11,8	8	8			3,8	1,8	1,8				0											2	1					
Р3.4	Разделение секрета.	12,6	8	8			4,6	1,6	1,6				3	1										0						
	Всего (час), без учета промежуточной аттестации**:**	**54**	**34**	**34**	**0**	**0**	**20**	**7**	**7**	**0**	**0**	**0**	**9**	**9**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4**	**4**	**0**				
	Всего по дисциплине (час.):	**72**	**34**				**38**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
P1.1	1	Криптоанализ шифра простой замены.	2
P1.1	2	Криптоанализ шифра перестановки.	2
P1.1	3	Криптоанализ шифра Виженера.	2
P1.2	4	Энтропия и взаимная информация случайных величин.	2
P1.2	5	Энтропия и избыточность языка.	2
P1.2	6	Расстояние единственности шифра.	2
P1.2	7	Вычисление вероятностей успеха имитации и подмены шифров.	2
P1.4	8	Проведение линейного криптоанализа упрощенного блочного шифра.	3
		Всего:	17

4.2. Практические занятия

«не предусмотрено»

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

P1. Основы традиционной криптографии

1. Криптоанализ исторических шифров.
2. Определение свойств и параметров шифра.
3. Проведение линейного криптоанализа упрощенного блочного шифра.

P2. Поточные шифры и асимметричные криптосистемы

1. Вычисление минимального многочлена и периода ЛРП.
2. Создание односторонней функции ловушки из сложной задачи на примере рюкзачной криптосистемы.
3. Выработка пары секретный ключ-публичный ключ для ассиметричных криптосистем.

P3. Хеш-функции и базовые протоколы

1. Проверка базовых свойств хеш-функции.
2. Создание примера протокола идентификации с нулевым разглашением.
3. Создание примера схемы разделения секрета.

4.3.2. Примерный перечень тем графических работ

«не предусмотрено»

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

«не предусмотрено»

4.3.4 Примерная тематика индивидуальных или групповых проектов

«не предусмотрено»

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

«не предусмотрено»

4.3.6. Примерный перечень тем расчетно-графических работ

«не предусмотрено»

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

«не предусмотрено»

4.4.1. Примерная тематика контрольных работ

Р1. Основы традиционной криптографии

1. Проведение атаки с известным ОТ для шифра простой замены и шифра перестановки.
2. Определение вероятности успеха имитации и подмены шифра.

Р2. Поточные шифры и асимметричные криптосистемы

1. Вычисление минимального многочлена и периода ЛРП.
2. Выполнение расшифрования в криптосистемах Рабина и Эль-Гамаля.

Р3. Хеш-функции и базовые протоколы

1. Проверка базовых свойств хеш-функции.
2. Создание примера схемы распределения ключей в сети на основе пересечений множеств.

4.3.9. Примерная тематика коллоквиумов

«не предусмотрено»

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1.1		+		+	+							
Р1.2		+		+	+							
Р1.3		+		+	+							
Р1.4		+		+	+							
Р2.1		+		+	+							
Р2.2		+		+	+							
Р3.1		+		+	+							
Р3.2		+		+	+							
Р3.3		+		+	+							
Р3.4		+		+	+							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1) Menezes A., van Oorschot P. Handbook of cryptography. CRC Press, 1997. http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptography.pdf
2) Тилборг, Хенк К. А. ван. Основы криптологии. Профессиональное руководство и интерактивный учебник / Х. К. А. ван Тилборг ; пер. с англ. Д. С. Ананичева, И. О. Корякова ; под ред. И. О. Корякова. — М. : Мир, 2006. — 471 с. : ил. — Библиогр.: с. 448-456

9.1.2.Дополнительная литература

1) Баричев, С. Г. Основы современной криптографии : Учеб. курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — М. : Горячая линия - Телеком, 2001. — 120 с. : ил. — ISBN 5-93517-022-1 : 55-00.
2) Нечаев, Василий Ильич. Элементы криптографии. Основы защиты информации : Учеб. пособие / В. И. Нечаев ; Под ред. В. А. Садовничего. — М. : Высшая школа, 1999. — 109 с. — Библиогр.: с. 104-106. — Коллекция: Важенин Ю. М. : 1365164. — ISBN 5-06-003644-8 : 16-00.
3) Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. — М. : Горячая линия - Телеком, 2010. — 232 с. : ил. — ISBN 978-5-9912-0150-6
4) Математические и компьютерные основы криптологии : Учеб. пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич ; Пер. с нем. О. В. Игольникова, А. В. Соколова. — Минск : Новое знание, 2003. — 382 с. — Библиогр.: с. 371-378 (196 назв.)

9.2. Методические разработки

Не используются

9.3.Программное обеспечение

Не используется

9.4. Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/
Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/
Сайт издательства Elsevier http://www.sciencedirect.com/
Сайт кафедры: http://kma.imkn.urfu.ru
Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index
Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитория с проектором

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины –

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

Р1. Основы традиционной криптографии

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,6**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа № 1	**6, 1-10**	**30**
Домашняя работа № 3	**6, 1-17**	**30**
Контрольная работа № 1	**6, 1-10**	**40**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрены		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,4		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа № 2	**6, 1-14**	**50**
Контрольная работа № 2	**6, 1-14**	**50**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
Промежуточная аттестация по лабораторным занятиям – не предусмотрена **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

Р2. Поточные шифры и асимметричные криптосистемы

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 1**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа № 1	**1, 1-10**	**20**
Домашняя работа № 2	**1, 1-14**	**20**
Домашняя работа № 3	**1, 1-17**	**20**
Контрольная работа № 1	**1, 1-14**	**20**
Контрольная работа № 2	**1, 1-17**	**20**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрены		

3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрены

Р3. Хеш-функции и базовые протоколы

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 1**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа № 1	**1, 1-10**	**20**
Домашняя работа № 2	**1, 1-14**	**20**
Домашняя работа № 3	**1, 1-17**	**20**
Контрольная работа № 1	**1, 1-14**	**20**
Контрольная работа № 2	**1, 1-17**	**20**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрены		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 6	0,4
Семестр 7	0,3
Семестр 7	0,3

*В случае проведения промежуточной аттестации по дисциплине (экзамена, зачета) методом тестирования используются официально утвержденные ресурсы: АПИМ УрФУ, СКУД УрФУ, имеющие статус ЭОР УрФУ; ФЭПО (www.фэпо.рф); Интернет-тренажеры (www.i-exam.ru).

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не применяется

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

«не предусмотрено»

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Раздел 1. Основы традиционной криптографии

Контрольная работа № 1.

Задание 1. Криптограмма о криптоанализе, получена с помощью шифра простой замены для русского текста без пробелов. Найти отрытый текст.

```
П В Е Р О У Н Ы Ы В З А В В О Ы В Ч Н Ы Щ Б Х Ш Й Е Й Я Н Х
П Щ А О В Й Ы Й Ъ Щ Ш Й Р Щ Ш У Н Р О Ы И Ф В О Х П И О И Ф
О Н Х Р О В Ф Ю У Ъ Ю Н О Р Ю Ш Й Е Й Я Й Х П Щ А О В Й Ы Й
Ъ Щ Ш Й Р У Н П В Ю О Ы В Щ Ш У Н Р О Ы И Ф Щ Р Ъ В У Й Ф Щ
```

Задание 2. Криптограмма о криптографии, получена с помощью шифра перестановки для русского текста. Найти отрытый текст.

```
ТОПГРРКИА
ЭТ О ИФЯА
РАБИЧГЛЕЕ
 ПЯСЕКСАВ
УКАА ОДН
```

Контрольная работа № 2.

Задание 1. Шифрование задается следующей таблицей, в которой строки занумерованы открытыми текстами, а столбцы -- ключами.

```
 12345
115432
221543
332154
```

а) Проверьте, действительно ли данная таблица задает функцию шифрования.
б) В предположении, что ключи равновероятны, проверьте, является ли данный шифр совершенным.
в) В предположении, что ключи равновероятны, найдите, вероятность успешной имитации и вероятность успешной подмены.

Задание 2. При шифровании 15-битовой строки сначала добавляется 1 бит так, чтобы сумма битов была четной, а затем к полученной 16-битовой строке применяется одноразовый щит. Найдите вероятности успешной имитации и успешной подмены для такого шифра.

Раздел 2. Поточные шифры и асимметричные криптосистемы

Контрольная работа № 1.

Задание 1. Линейная рекуррентная последовательность над полем Z_3 с характеристическим многочленом $F(x)=x^6+x^4+x^3+1$ начинается с 0,2,0,2,0,0.

Найти ее минимальный многочлен и период.
Задание 2. Найти минимальный многочлен линейной рекуррентной последовательности над полем Z_2:
1,0,1,1,0,0,1,1,0,1,1,0,1,1,1,0,1,0,1,1,0,0,1,0,0,1,1,0,0,...

Контрольная работа № 2.
Задание 1. Расшифровать сообщение **174**, зашифрованное в криптосистеме Рабина с секретным ключом **(11,23)**.
Задание 2. Расшифровать сообщение **(0101011,1010100)**, зашифрованное в криптосистеме Эль-Гамаля с секретным ключом **(9)** в мультипликативной группе поля $\mathbf{Z_2(x)}$, где $\mathbf{x^7+x+1=0}$, с порождающим **x**. (Считать, что полиномиальный базис $\mathbf{Z_2(x)}$ над $\mathbf{Z_2}$ упорядочен по возрастанию степеней.)

Раздел 3. Хеш-функции и базовые протоколы
Контрольная работа № 1.
Задание. Хеш-функция ***h*** построена по итерационной схеме с шаговой сжимающей функцией $\boldsymbol{f(x,y)=xy^2}$ **MOD** ***N***, где ***N*** произведение двух "забытых" больших простых чисел. Покажите, что ***h*** не устойчива к взятию второго прообраза.

Контрольная работа № 2.
Задание. Создайте схему распределения ключей на 12 участников на основе 9 секретных ключей.

8.3.3. Примерные контрольные кейсы
«не предусмотрено»
8.3.4. Перечень примерных вопросов для зачета

Зачет в 7 семестре

1. Общая схема поточного шифра. Требования к управляющему блоку.
2. Линейные регистры сдвига и линейные рекуррентные последовательности (ЛРП). Характеристическая матрица и характеристический многочлен однородной ЛРП.
3. Финально-периодические последовательности. Вычисление минимального многочлена и периода ЛРП.
4. ЛРП максимального периода. Их статистические свойства.
5. Усложнения линейных регистров сдвига.
6. Шифр A5.
7. Алгоритм RC4.
8. Новые задачи криптографии и недостаточность традиционных криптосистем.
9. Общие принципы построения криптосистем с открытым ключом.
10. Создание односторонней функции ловушки из сложной задачи на примере рюкзачной криптосистемы.
11. RSA: построение, связь параметров, бит-безопасность, известные виды атак.
12. КС Рабина (Доказательство надежности).
13. КС Блюма-Голдвассер.
14. КС Голдвассер-Микали.
15. КС Мак-Элиса.
16. КС Эль-Гамаля.
17. Подписи: RSA, Эль-Гамаля, Ниберга-Руппеля, DSS, ГОСТ 34.10-94, ГОСТ 34.10-2012.

8.3.5. Перечень примерных вопросов для экзамена

Экзамен в 6 семестре

1. Исторические шифры перестановки. Криптоанализ шифра перестановки при длине сообщения много больше длины блока перестановки.
2. Исторические шифры замены. Криптоанализ шифра простой замены.
3. Определение длины ключа шифра Виженера. Метод Казиски. Подсчет числа совпадений.
4. Теорема об индексе совпадений в криптограмме, защифрованной шифром Виженера.
5. Информация и энтропия. Свойства энтропии.
6. Условная энтропия. Цепное правило и следствие.
7. Взаимная информация.
8. Взаимная информация между открытым текстом и криптограммой. Совершенная секретность.
9. Описание эндоморфных совершенных криптосистем.
10. Теорема Шеннона о типичных и редких последовательностях.
11. Теорема Шеннона о доле типичных последовательностей.
12. Избыточность языка.
13. Расстояние единственности.
14. Имитация и подмена для шифров с равновероятными ключами.
15. Имитация для шифров с произвольно распределенными ключами.
16. Эндоморфные шифры, не распространяющие искажения типа "замена" (по модулю теоремы Маркова).
17. Теорема Маркова, описывающая биекции изометрии.
18. Эндоморфные шифры, не распространяющие искажения типа "пропуск" на языке перестановочности отношений.
19. Определяемость слова набором всех его подслов на единицу меньшей длины.
20. Теорема Глухова, описывающая биекции, перестановочные с отношением вычеркивания символа.
21. Стандарт шифрования ГОСТ 28147-89.
22. Алгоритм шифрования IDEA.
23. Стандарт шифрования DES.
24. Стандарт шифрования AES.
25. Режимы использования блочных шифров.

Экзамен в 8 семестре

1. Общая схема поточного шифра. Требования к блокам.
2. Линейный регистр сдвига. Характеристический и минимальный многочлен последовательности. Вычисление периода и предпериода ЛРП.
3. Статистические свойства линейной рекуррентной последовательности.
4. Восстановление минимального многочлена по линейной рекуррентной последовательности.
5. Общие принципы построения криптосистемы с открытым ключом. Криптосистема на основе задачи о рюкзаке.
6. Криптосистема RSA. Взаимосвязь секретных параметров в RSA.
7. Создание RSA. Требования к параметрам.
8. Атаки на RSA.
9. Криптосистема Рабина.
10. Криптосистема Эль-Гамаля.
11. Криптосистема Мак-Элиса.
12. Криптосистема Голдвассер-Микали.
13. Криптосистема Блюма-Голдвассер.
15. Функции хэширования. Общая схема итеративной бесключевой хэш-функции. Усиление Меркля-Дамгарда.

16. Общая схема работы MD4, MD5, SHA-1. Их индивидуальные характеристики.
17. MDC-2 и MDC-4. Функция хэширования ГОСТ Р 34.11--94. (Общая схема)
18. Ключевые хэш-функции на симметричных криптосистемах в режиме сцепления блоков.
19. Создание ключевых хэш-функций из бесключевых.
20. Схемы защиты целостности данных.
21. Построение коллизий на основе парадокса ``дней рождений".
22. Схема подписывания на основе асимметричной криптосистемы
и хэш-функции (RSA, система Эль-Гамаля).
23. Протоколы распределения ключей с использованием симметричного шифрования.
Протокол Шамира.
24. Протоколы распределения ключей с использованием асимметричного шифрования.
25. Протоколы открытого согласования ключей.(От Диффи и Хеллмана до MTI и STS)
26. Схема Блома. Теорема о стойкости.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

«не используются»

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

«не используются»

8.3.8. Интернет-тренажеры

«не используются»

8.3.9. Примерные задания для домашних работ

Раздел 1. Основы традиционной криптографии

Домашняя работа № 1.

Задание 1. С помощью частотного анализа (отдельных букв, биграмм , триграмм и сочетаний гласных и согласных) провести атаку с известным шифртекстом на следующую криптограмму, полученную с помощью шифра простой замены для русского текста без пробелов.

Т С М З Т И Ь Ч К Х Ч Ж Т С У Т Б М Ь Б Ч Е С Г К Л И Б М Л
Б П С Л Б Л С М П Б Ч М Ь П С О Б Ь З Т И Ь Б Д Б Ь К З М Ь
С Е У Ь М Б О Т С Л В Ф Я Ч О М В П Х Ч Ж Т Ь К З М Ь К Ь Б
Ш З С

Задание 2. С помощью запрещённых биграмм провести атаку с известным шифртекстом на следующую криптограмму, полученную с помощью шифра перестановки с известной длиной ключа для русского текста.

```
ЯТНОТАЛМ
ШИИИОКК Р
РОИ ЕКЕПС
МОЫСЕТ АЛ
УЖВКТ  РА
ЛА ОАХ БК
ЫСЕЕКОНВО
ЛНОСШК ОЫ
ЕНАО З СИ
АЕГИ ОЖГТ
НАЫИШТН
 МРА ПКХЫ
КЛРВ БИЫИ
ТЬСТЯ ААС
БЕИПАМ ОД
ОП ИТЬ  Я
```

```
ПРСЫНОМ О
В  МОЮИ Б
ДОАООГП Р
СХН ЖЕМИО
 ДМЫДАНМЕ
РАЗ НОИКС
ДНСЕЮ ВЗУ
У ЮАВОЛВС
```

Задание 3. Провести атаку с известным шифртекстом на следующую криптограмму, полученную с помощью решетки Кардано известного размера для русского текста без пробелов.

```
ВМСОЕЛМЕКТ
ИПИВПЗАРЖЕ
РАДКАРТАЛЕ
ТИТШИЮТТЬП
 И ОТКЬС Т
ПАРАЫСЖА М
```

Домашняя работа № 2.

Задание 1. Алфавит языка некоторого племени состоит из трех букв: О, Ы и У.
В языке всего два слова: ОЫО и УУЫ, причем они используются одинаково часто.
а) Найдите энтропии, приходящиеся на 1 символ, для отдельных букв, для биграмм и для триграмм.
б) Вычислите энтропию и избыточность языка.
в) Каково теоретическое расстояние единственности для шифра Цезаря, примененного к тексту на этом языке?

Задание 2. При шифровании 6-битовой строки сначала добавляется 00, 01, или 11 так, чтобы сумма битов была кратна 3, а затем к полученной 8-битовой строке применяется одноразовый щит. Найдите вероятности успешной имитации и успешной подмены для такого шифра.

Домашняя работа № 3.

Задание. Найти 10 наиболее вероятных линейных соотношений между битами ключа, открытого текста и криптограммы, для блочного шифра с длинами блока и ключа равными 3 битам, со следующей таблицей шифрования (ключи по столбцам, ОТ по строкам).

```
  01234567
0 12345670
1 23456701
2 34567012
3 45670123
4 01234567
5 70123456
6 67012345
7 56701234
```

Раздел 2. Поточные шифры и асимметричные криптосистемы

Домашняя работа № 1.

Задание 1. Линейная рекуррентная последовательность над полем Z_3 с характеристическим многочленом $F(x)=x^6+x^5+x^3+1$ начинается с 0,0,1,2,0,0.
Найти ее минимальный многочлен.

Задание 2. Найти минимальный многочлен линейной рекуррентной последовательности над полем Z_2:
1,0,0,1,1,1,1,1,1,0,1,1,0,0,0,1,0,0,0,1,1,1,0,0,1,1,1,1,1,...

Домашняя работа № 2.
Задание. Создайте пример функции с 20-битовым аргументом, являющейся элементом последовательности односторонних функций на основе задачи о рюкзаке.

Домашняя работа № 3.
Задание 1. Создайте модуль и секретный показатель для криптосистемы RSA, если публичный показатель равен 17, а часть секрета это простые числа 1483 и 4649.
Задание 2. Создайте публичный ключ для криптосистемы Голдвассер-Микали, если секретный ключ равен (4903,45319).
Задание 3. Создайте пару (секретный ключ, публичный ключ) для криптосистемы Эль-Гамаля на подгруппе простого порядка группы точек эллиптической кривой $E_{1,4}(Z_{29})$.

Раздел 3. Хеш-функции и базовые протоколы
Домашняя работа № 1.
Задание 1. Хеш-функция ***h*** построена по итерационной схеме с шаговой сжимающей функцией $f(x,y)=(x+y)^2$ **MOD** ***N***, где ***N*** произведение двух "забытых" больших простых чисел. Покажите, что ***h*** не устойчива к взятию второго прообраза.
Задание 2. Хеш-функция ***h*** построена по итерационной схеме с шаговой сжимающей функцией $f(x,y)=x^y$ **MOD** ***P***, где ***P*** большое простое число. Покажите, что ***h*** не устойчива к взятию второго прообраза.

Домашняя работа № 2.
Задание 1. Зная разложение 409091=1307*313 вычислите ответ доказывающего в протоколе без установки на запрос проверяющего 44447.
Задание 2. Публичный ключ доказывающего для протокола Фиата-Шамира с модулем 29781651707669144020655317736740675555653343264352295502501753 равен 24453575371304644771183251116058354402608811447758372394147261.
Выполните имитацию передач проверяющим без участия реального доказывающего с обоими возможными запросами проверяющего.

Домашняя работа № 3.

Задание 1. Создайте схему разделения секретного бита для совершенной структуры доступа на 7 участников (занумерованных от 1 до 7), в которой привилегированной группой является любая такая группа, в которой есть хотя бы одна подгруппа с суммой номеров участников кратной 15.
Задание 2. Создайте матрицы черной и белой точек для визуального разделения секрета в 3-пороговой схеме на 7 участников.