МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования
**«Российский государственный
университет социальных технологий»**
(ФГБОУ ИВО «РГУ СоцТех»)

УТВЕРЖДАЮ

Проректор по образовательной деятельности

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.05 КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

образовательная программа направления подготовки
09.04.03 «Прикладная информатика»

Профиль подготовки
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:
Магистр

Форма обучения очная

Москва 2025

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Криптографические протоколы»

Оценочные средства составляются в соответствии с рабочей программой дисциплины и представляют собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.), предназначенных для измерения уровня достижения обучающимися установленных результатов обучения.

Оценочные средства используются при проведении текущего контроля успеваемости и промежуточной аттестации.

Таблица 1 - Перечень компетенций, формируемых в процессе освоения дисциплины

Код и содержание компетенции	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ПК-6 Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	ПК-6.1 Знает различные методы решения задач при создании экономических информационных систем; методы проектирования автоматизированных и информационных систем для решения прикладных задач; информационные технологии, применяемые на этапах разработки, производства, испытаний и эксплуатации
	ПК-6.2 Умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации; использовать программные средства, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции. этапах разработки,
	ПК-6.3 Владеет методами описания информационных систем; навыками сбора, формализации и обработки информации; навыками использования инструментальных средств прикладной информатики создания высоконагруженных информационных систем; классами, пакетами и возможностями автоматизированных средств обеспечения; навыками работы с информационными технологиями, применяемыми на этапах разработки, производства, испытаний и эксплуатации продукции.
ПК-1 Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными	ПК-1.1 Знает основные подходы, методы в области проектирования и управления информационными системами в прикладных областях; возможности современных инструментальных средств для проектирования и управления информационными системами в прикладных областях; способы представления научно-технической информации.

системами в прикладных областях	ПК-1.2 Умеет использовать и развивать методы научных исследований в области проектирования и управления информационными системами в прикладных областях; анализировать иностранные источники в области проектирования и управления ИС в прикладных областях; использовать и развивать методы инструментарий в области проектирования и управления информационными системами в прикладных областях; правильно подготавливать научно-технические отчеты; оформлять результаты исследований в виде статей и докладов на научных конференциях в предметной области.
	ПК-1.3 Владеет практическими навыками использования и развития инструментальных средств в области проектирования и управления информационными системами в прикладных областях; навыками работы в системах поиска информации, текстовых процессорах, электронных таблицах, базах данных и системах подготовки презентаций.

Конечными результатами освоения дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование дескрипторов происходит в течение всего семестра по этапам в рамках контактной работы, включающей различные виды занятий и самостоятельной работы, с применением различных форм и методов обучения (табл.2).

Таблица 2 - Формирование компетенций в процессе изучения дисциплины:

Код компетенции	Уровень освоения компетенций	Индикаторы достижения компетенций	Вид учебных занятий[1], работы, формы и методы обучения, способствующие формированию и развитию компетенций[2]	Контролируемые разделы и темы дисциплины[3]	Оценочные средства, используемые для оценки уровня сформированности компетенции[4]
ПК-6	***Знает***				
	Недостаточный уровень	ПК-6. Студент не усвоил следующие знания: основы построения систем и сетей электросвязи и особенностей их эксплуатации технические характеристики основных телекоммуникационных систем и протоколов информационного обмена перспективы развития систем и сетей связи	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной информации 4. Мультиплексирование и методы доступа в канал 5. Принципы аналого-цифрового и цифро-аналогового преобразования	Текущий контроль – устный опрос.
	Базовый уровень	ПК-6.1. Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания по темам:	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача	1. 1. Классификация типов передаваемой информации 2. Передача	Текущий контроль – устный опрос.

[1] Лекционные занятия, практические занятия, лабораторные занятия, самостоятельная работа…

[2] Необходимо указать активные и интерактивные методы обучения (например, интерактивная лекция, работа в малых группах, методы мозгового штурма и т.д.), способствующие развитию у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

[3] Наименование темы (раздела) берется из рабочей программы дисциплины.

[4] Оценочное средство должно выбираться с учетом запланированных результатов освоения дисциплины, например:

«Знать» – собеседование, коллоквиум, тест…

«Уметь», «Владеть» – индивидуальный или групповой проект, кейс-задача, деловая (ролевая) игра, портфолио…

		подготовки информации к принятию управленческих решений систему сбора, обработки и подготовки информации по предприятию и его структурным подразделениям.	промежуточной аттестации, подготовка и сдача зачета с оценкой	2. Программно-алгоритмические требования к адаптации биомедицинских информационных систем.	
	Средний уровень	ПК-6.1. Студент способен самостоятельно выделять главные положения в изученном материале. Знает основы построения систем и сетей электросвязи и особенностей их эксплуатации	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной	Текущий контроль – устный опрос.
	Высокий уровень	ПК-6.1. Студент знает, понимает, выделяет главные положения в изученном материале и Знает:, основы построения систем и сетей электросвязи и особенностей их эксплуатации технические характеристики основных телекоммуникационных систем и протоколов информационного обмена перспективы развития систем и сетей связи защиты объектов информатизации	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной информации 4. Мультиплексирование и методы доступа в канал 5. Принципы аналого-цифрового и цифро-аналогового	Текущий контроль – устный опрос.
	Умеет				

Базовый уровень	ПК-6.2. Студент испытывает затруднения при творческом применении знаний о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем отслеживании тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи разрабатывать структурные схемы систем связи с заданными характеристиками читать структурные и функциональные схемы систем и сетей связи	Лекционные и практические занятия, работа в малых группах, интерактивная	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной информации 4. Мультиплексирование и методы доступа в канал 5. Принципы аналого-цифрового и цифро-аналогового преобразования	Текущий контроль – устный опрос.

	Средний уровень	ПК-6.2. Студент умеет творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной	Текущий контроль – устный опрос.
	Высокий уровень	ПК-6.2. Студент умеет творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи разрабатывать структурные схемы систем связи с заданными характеристиками читать структурные и функциональные схемы систем и сетей связи	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной	Текущий контроль – устный опрос.
	Владеет				
	Средний уровень	ПК-6.3. Студент владеет знаниями о принципах организации и устройства современных телекоммуникационных сетей знаниями о способах передачи информации в телекоммуникационных сетях	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной	Текущий контроль – устный опрос.

	Высокий уровень	ПК-6.3. Студент владеет знаниями о принципах организации и устройства современных телекоммуникационных сетей знаниями о способах передачи информации в телекоммуникационных сетях основами для проектирования и развертывания локальных вычислительных сетей профессиональной терминологией	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета с оценкой	1. Классификация типов передаваемой информации 2. Передача сигналов через канал связи. Базовые виды модуляций. 3. Теоретические основы передачи дискретной	Текущий контроль – устный опрос.
ПК-1		*Знает*			
	Недостаточный уровень	ПК-1. Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает новые научные результаты и предысторию их появления; классические методы, применяемые в прикладной математике	Лекционные ипрактические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия 2. математического моделирования Задачи 3. идентификация Реализация математически 4. х моделей в 5. технике: 6. гидродинамические модели Марковские модели систем массового обслуживания Немарковские модели Марковские сети	Текущий контроль – устный опрос.
	Базовый уровень	ПК-1.1. Студент усвоил основноесодержание материала дисциплины, но	Лекционные и практические занятия,	1. Основные понятия математического моделирования	Текущий контроль – устный опрос.

		имеет пробелы в усвоении материала. Имеет несистематизированные знанияо новых научных результатах и предыстории их появления.	самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовкаи сдача экзамена.	2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	
	Средний уровень	ПК-1.1. Студент способен самостоятельно выделять главные положения в изученном материале. Знает новые научные результаты и предысторию их появления; классические методы, применяемые в прикладной математике и информатике.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	Текущий контроль – устный опрос.

	Высокий уровень	ПК-1.1. Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Показывает глубокое знание ипонимание новых научных результатови предыстории их появления; классических методов, применяемых в прикладной математике и информатике, необходимые и достаточные условия их реализации.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	Текущий контроль – устный опрос.
		Умеет			
	Базовый уровень	ПК-1.2. Студент испытывает затруднения при систематизации научных результатов. Студент непоследовательно выделяетиз научных результатов главное и удаляет второстепенное.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	Текущий контроль – устный опрос.

	Среднийуровень	ПК-1.2. Студент умеет систематизировать научные результаты, выделять из них главное,и удалять второстепенное; самостоятельно выбирать эффективные методы решения поставленных задач.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	Текущий контроль – устный опрос.
	Высокийуровень	ПК-1.2. Студент умеет самостоятельно систематизировать научные результаты, выделять из них главное,и удалять второстепенное; самостоятельно выбирать эффективные методы решения поставленных задач и разрабатывать новые методы для получения новых научных и прикладных результатов.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 5. Марковские сети	Текущий контроль – устный опрос.
		Владеет			

	Базовый уровень	ПК-1.3. Студент владеет навыками сбора и анализа научной информации.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	Текущий контроль – устный опрос.
	Среднийуровень	ПК-1.3. Студент владеет навыками сбора и анализа научной информации; навыками работы с математическими источниками информации.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские моделисистем массового обслуживания 5. Немарковские модели 6. Марковские сети	Текущий контроль – устный опрос.
	Высокийуровень	ПК-1.3. Студент владеет знаниями всего изученного материала, владеет навыками сбора и анализа научной информации; навыками работы с математическими источниками информации; наукоемкими технологиями и пакетами прикладных программ для решения прикладных задач	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,дискуссия, самостоятельная работа обучающихся, подготовка и сдача	1. Основные понятия математического моделирования 2. Задачи идентификация и оптимизации 3. Реализация математических моделей в технике: гидродинамические модели 4. Марковские модели	Текущий контроль – устный опрос.

			промежуточной аттестации, подготовка и сдача экзамена.	систем массового обслуживания 5. Немарковские модели 6. Марковские сети	

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ[5]

Таблица 3

№	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
2	Экзамен	Средство контроля усвоения учебного материала разделов дисциплины	Вопросы к экзамену

[5] Указываются оценочные средства, применяемые в ходе реализации рабочей программы данной дисциплины.

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценивание результатов обучения по дисциплине «Криптографические протоколы» осуществляется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся.

Предусмотрены следующие виды контроля: текущий контроль (осуществление контроля всех видов аудиторной и внеаудиторной деятельности обучающегося с целью получения первичной информации о ходе усвоения отдельных элементов содержания дисциплины) и промежуточная аттестация (оценивается уровень и качество подготовки по дисциплине в целом).

Показатели и критерии оценивания компетенций, формируемых в процессе освоения данной дисциплины, описаны в табл. 4.

Таблица 4.

Код компетенции	Уровень освоения компетенции	Индикаторы достижения компетенции	Критерии оценивания результатов обучения
ПК-6		Знает	
	Недостаточный уровень Оценка «неудовлетворительно»	*ПК-6.1.*	*Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины*
	Базовый уровень Оценка «удовлетворительно»	*ПК-6.1.*	*Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении*
	Средний уровень Оценка «хорошо»	*ПК-6.1.*	*Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач*
	Высокий уровень Оценка «отлично»	*ПК-6.1.*	*Показывает глубокое знание и понимание материала, способен применить изученный материал на практике*
		Умеет	
	Базовый уровень	*ПК-6.2.*	*Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач*
	Средний уровень	*ПК-6.2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач*
	Высокий уровень	*ПК-6.2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки*
		Владеет	
	Базовый уровень	*ПК-6.3.*	*Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.*
	Средний уровень	*ПК-6.3.*	*Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.*
	Высокий уровень	*ПК-6.3.*	*Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала*
		Знает	
	Недостаточный уровень Оценка «неудовлетворительно»	ПК-1.1.	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины

	Базовый уровень Оценка «удовлетворительно»	ПК-1.1.	Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении
	Средний уровень Оценка «хорошо»	ПК-1.1.	Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач
	Высокий уровень Оценка «отлично»	ПК-1.1.	Показывает глубокое знание и понимание материала, способен применить изученный материал на практике
		Умеет	
	Базовый уровень	ПК-1.2.	Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач
	Средний уровень	ПК-1.2.	Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач
	Высокий уровень	ПК-1.2.	Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки
		Владеет	
	Базовый уровень	ПК-1.3.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных
	Средний уровень	ПК-1.3.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.
	Высокий уровень	ПК-1.3.	Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала

4. Методические материалы, определяющие процедуры оценивания результатов обучения

Задания в форме устного опроса:

Устный опрос используется для текущего контроля успеваемости обучающихся по дисциплине в качестве проверки результатов освоения терминологии. Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

5. Материалы для проведения текущего контроля и промежуточной аттестации

Задания в форме устного опроса

1. История криптографии. Классические алгоритмы шифрования. Стойкость классических шифров.
2. Симметричное и ассиметричное шифрование.
3. Модель угрозы Долева-Яо.
4. Протокол Нидхема-Шредера. Возможные атаки. Понятия аутентификации сущности и аутентификации сообщений.
5. Ассиметричная версия протокола Нидхема-Шредера.
6. Обобщенный алгоритм Евклида.
7. Понятие группы. Фактор-группа. Теорема Лагранжа. Порядок группы.
8. Циклические группы.
9. Мультипликативные группы.
10. Конечные поля. Поле с простым числом элементов.
11. Поле неприводимых полиномов.
12. Поля, построенные с помощью полиномиального базиса.

Контролируемые компетенции: ПК-1,ПК-2,ПК-3,ПК-6

Оценка компетенций осуществляется в соответствии с таблицей 4.

Вопросы к экзамену

1. Модулярная арифметика в фактор-группе Zn.
2. Алгоритм модулярного возведения в степень. Аддитивные цепочки.
3. Решение линейного уравнения в фактор-группе Zn.
4. Китайская теорема об остатках.
5. Функция Эйлера. Теоремы Ферма и Эйлера.
6. Понятие квадратичных вычетов. Символы Лежандра-Якоби.
7. Вычисление квадратных корней по простому модулю.
8. Вычисление квадратных корней по составному модулю.
9. Симметричные алгоритмы шифрования. Сеть Файстеля.
10. Алгоритм DES. Тройной DES.
11. Дифференциальный криптоанализ. Понятие характеристик.
12. Алгоритм AES. Основные принципы.
13. Основные режимы шифрования (электронная кодовая книга, сцепление блоков, обратная связь по шифртексту, обратная связь по выходу).
14. Протокол обмена ключами Диффи-Хеллмана. Возможные атаки.
15. Криптосистема RSA. Стойкость системы RSA. Задача о разложении чисел на простые множители.
16. Алгоритмы генерации больших простых чисел (Соловэй-Штрассен, Миллер-Рабин, ГОСТ 34.10-94).
17. Криптосистема Эль-Гамаля. Описание. Возможные атаки.
18. Битовая стойкость алгоритма RSA. Понятие оракула.

19. Методы защиты целостности данных. Хэш-функции.
20. Ассиметричные методы защиты целостности. Электронная цифровая подпись. Подпись RSA.
21. Цифровая подпись Эль-Гамаля. Потенциальные уязвимости.
22. Некоторые понятия из теории оптимизации.
23. Кодирование Грея.
24. NP-полные (универсальные) задачи.
25. Тестовые функции.
26. Общий подход к генетическим алгоритмам.
27. Основные понятия генетических алгоритмов.
28. Операторы выбора родителей.
29. Дискретная рекомбинация.
30. Кроссинговер.
31. Мутация.
32. Операторы отбора особей в новую популяцию.
33. Представление данных в генах.
34. Генетические операторы.
35. Репродукция.
36. Операторы кроссоввера.
37. Операторы мутации

Контролируемые компетенции: ПК-1,ПК-2,ПК-3,ПК-6

Оценка компетенций осуществляется в соответствии с таблицей 4.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Измененные пункты	Решение Учебно-методического совета