ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Цифровых технологий

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Сахарчук Е.С.
«27» 04 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

образовательная программа направления подготовки
09.04.03 "Прикладная информатика"
Б1.В.06 «Дисциплины (модули)», Часть, формируемая участниками образовательных отношений, Дисциплины (модули) по выбору

Профиль подготовки
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:

Магистр

Форма обучения: очная

Курс 1 семестр 1

Москва 2022

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования направления 09.04.03 "Прикладная информатика", утвержденного приказом Министерства науки и высшего образования Российской Федерации № 916 от «19» сентября 2017 г.

Разработчик рабочей программы:
к.т.н., доцент кафедры цифровых технологий МГТЭУ
место работы, занимаемая должность

подпись	А.А. Белоглазов И.О. Фамилия	«14» 03 2022 г. Дата

Рабочая программа утверждена на заседании кафедры цифровых технологий
(протокол № 4 от «21» 03 2022 г.)

Декан факультета

« 21 » 03 2022 г. (дата)	(подпись)	Е.В. Петрунина (Ф.И.О.)

СОГЛАСОВАНО
Начальник
управления по социальной
работе

« » 2022 г. (дата)	(подпись)	(Ф.И.О.)

СОГЛАСОВАНО
Председатель
совета обучающихся

«21» 04 2022 г. (дата)	(подпись)	Корги И. (Ф.И.О.)

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью дисциплины является сформирование формирование профессиональных компетентностей специалиста по защите информации, специализирующегося в области компьютерной безопасности, в использовании современных криптографических протоколов при решении задач обеспечения целостности, конфиденциальности, неотслеживаемости информации.

Задачи дисциплины:

• формирование способности квалифицированно использовать возможности современных криптографических протоколов в решении различных задач защиты информации: аутентификации сущностей и источников данных, распределении аутентичных криптографических ключей, электронной цифровой подписи, разделении секрета, электронном тайном голосовании;

• формирование навыков использования современных прикладных криптографических протоколов аутентификации, используемых при защите данных в Internet;

• развитие критического подхода к решению задач с использованием криптографических протоколов через понимание отсутствия абсолютной защищенности распределенной информационной системы со многими участниками;

• ознакомление будущего специалиста с криптографическими протоколами, закрепленными национальными и международными стандартами.

Требования к результатам освоения дисциплины

Код компетенции	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 продукции.
		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.
		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 системами в прикладных областях	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.
		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.
ПК-9	Способен принимать эффективные проектные решения в условиях неопределенности и риска	ПК-9.1 Знает принципы, методы, положения, определения эффективности проектных решений в условиях неопределенности и риска; возможности современных инструментальных средств для анализа, моделирования, оценки информационных процессов предприятий прикладной области в условиях неопределенности и риска.
		ПК-9.2 Умеет принимать эффективные проектные решения в условиях неопределенности и риска; правильно использовать возможности современных инструментальных средств для анализа, моделирования, оценки информационных процессов предприятий прикладной области в условиях неопределенности и риска.
		ПК-9.3 Владеет навыками принятия эффективных проектных решений на основе приобретенных знаний и умений и их применения в условиях неопределенности и риска; навыками использования современных инструментальных средств при моделировании, оценке и оптимизации информационных процессов предприятий прикладной области; русскоязычной и англоязычной терминологией методов, моделей, инструментария в сфере информационных технологий.

1.2. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)»

Настоящая дисциплина относится к дисциплинам по выбору блока дисциплин. Для освоения дисциплины необходимы компетенции, полученные в ходе изучения дисциплин:

− Теория информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Криптографические протоколы» составляет 4 зачетных единиц/144 часов:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		1 курс, 2 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*34*	*34*
Лекции	10	10
Практические занятия	24	24
Лабораторные занятия		
Самостоятельная работа обучающихся	146	146
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет с оценкой	6	6
Экзамен		
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	216\6	216\6

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Основные понятия криптографии. Предмет и задачи.	Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.	ПК-6,ПК-1,ПК-9
2.	Симметричные криптосистемы.	Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF.	ПК-6,ПК-1,ПК-9

		Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров.	
3	Контроль целостности	MAC. Определение, модель безопасности. Построение на базе Блоковых шифров: BCB-MAC, NMAC, PMAC. Хэш-функции. Стойкость к колизиям. Требования к хэш-функциям. Парадокс дней рождения. Примеры хэш-функций. HMAC. CCA модель атак и аутентифицированное шифрование. Способы построения AE. Стандарты.	ПК-6,ПК-1,ПК-9
4	Основные алгоритмы с открытым ключом.	Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности.	ПК-6,ПК-1,ПК-9
5	Управление ключами.	Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. K-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая криптография.	ПК-6,ПК-1,ПК-9
6	Протоколы цифровых денег и электронного голосования	Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.	ПК-6,ПК-1,ПК-9
7	Протоколы идентификации + личностная криптография.	Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).	ПК-6,ПК-1,ПК-9
8	Пост-квантовая криптография.	Понятия квантовых вычислений. Построение криптосистем на доказано сложных задачах. Линейные коды. Способы задания. Декодирование линейных кодов как «трудная» задача. Декодирование линейных кодов как «простая» задача. NP- полные задачи кодирования. Системы Макэлиса и Нидерайтора.	ПК-6,ПК-1,ПК-9

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости

1.	Криптографические алгоритмы	5	12	73	108	Устный опрос
2.	Криптографические протоколы	5	12	73	108	Устный опрос
Экзамен		6				
	Итого:	10	24	146	216\6	

2.4. Планы теоретических (лекционных) занятий

Тема лекции. Вопросы, отрабатываемые на лекции	**Всего часов**
Тема 1: Понятие криптографического протокола. **1. Основные определения;** **2. Свойства, характеризующие безопасность протоколов;** **3. Виды криптографических протоколов;** **4. Основные атаки на безопасность протоколов.**	2
Тема 2: Криптографические хеш-функции. **1. Функции хеширования и целостность данных;** **2. Хеш-функции, задаваемые ключом;** **3. Хеш-функции, не зависящие от ключа;** **4. Возможные атаки на функции хеширования.**	2
Тема 3: Коды аутентификации. **1. Определения и свойства;** **2. Ортогональные массивы.**	2
Тема 4: Протоколы идентификации. **1. Виды протоколов идентификации;** **2. Протоколы идентификации, использующие пароли (слабая аутентификация);** **3. Протоколы идентификации, использующие технику «запрос — ответ» (сильная аутентификация).**	2

Тема 5: Управление ключами. **1. Проблема управления ключами;** **2. Жизненный цикл ключей;** **3. Услуги, предоставляемые доверенной третьей стороной;** **4. Особенности управления ключами в симметричных системах шифрования;** **5. Особенности управления ключами в асимметричных системах шифрования.**	2

2.5. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	**Всего часов**
1. Понятие криптографического протокола. Отличия криптографического протокола от криптографического алгоритма. 2. Общая классификация криптографических протоколов: протоколы с посредником, протоколы с арбитром, самодостаточные протоколы. 3. Понятие атаки на криптографический протокол.	4
1. Концепция криптографической защиты информации на сетевом уровне модели ISO/OSI. Обмен сообщениями на уровне протокола IP. Протокол обеспечения безопасности в Internet – IPSec. 2. Протокол Authentication Header (AH). Протокол Encapsulation Security Payload (ESP). Параметры защиты IP-Sec. Протокол обмена ключами через Internet – IKE. 3. Первая фаза протокола IKE. Основной режим первой фазы протокола IKE, основанный на цифровой подписи. Отказ в аутентификации в основном режиме первой фазы протокола IKE, основанного на цифровой подписи. 4. Агрессивный режим первой фазы протокола IKE, основанного на цифровой подписи. Протокол удаленной регистрации SSH. Архитектура протокола SSH. Протокол транспортного уровня SSH. 5. Протокол SSL (TLS). Архитектура протокола SSL. Протокол квитирования SSL. Реализации SSL.	4

1. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами. 2. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. 3. Схемы Wide-MouthFrog, Yahalom, протокол Нидхема-Шредера, ОтвеяРииса. Бесключевой протокол Шамира. 4. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Протокол Kerberos.	4
1. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами. 2. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. 3. Схемы Wide-MouthFrog, Yahalom, протокол Нидхема-Шредера, ОтвеяРииса. Бесключевой протокол Шамира. 4. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Протокол Kerberos.	4
1. Протоколы передачи сеансовых секретных ключей. Протокол WideMouthFrog. Обмен зашифрованными ключами EKE. 2. Трехпроходный протокол Шамира. Протоколы предварительного распределения ключей. 3. Схема распределения ключей Блома. Протоколы совместной выработки общего ключа. 4. Протокол Диффи-Хеллмана. Протокол "станция-станция".	4
1. Управление открытыми ключами. 2. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. 3. Стандарт X.509. Сервисы	4

инфраструктуры открытых ключей	

2.6. Планы лабораторных работ – не предусмотрено.

Задания, вопросы, для самостоятельного изучения (задания)	**Всего Часов**
Вычислительная и безусловная связанность, секретность.	24
Протоколы привязки к биту на основе проблемы дискретного логарифмирования, на основе симметричной криптосистемы, на основе односторонней функции, односторонней перестановки.	24
Аутентификация источника данных. Аутентификация сущности.	25
Генерация аутентифицированных ключей. Основные методы и механизмы аутентификации. Стратегия «оклик-отзыв».	24
Понятие схемы разделения секрета (СРС). Группа доступа. Структура доступа. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках.	24
Разделение секрета для произвольной группы доступа. Совершенная СРС. Идеальное разделение секрета. Проверяемое разделение секрета.	25

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

2) для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Algebraic Geometry for Coding Theory and Cryptography: IPAM, Los Angeles, CA, February 2016 / Howe, Everett W; Lauter, Kristin E; Walker, Judy L. Springer. 2017

2. Фомичев В.М. Криптографические методы защиты информации В 2 Ч. ЧАСТЬ 1. Математические аспекты. Учебник для академического бакалавриат/В.М.Фомичев, Д.А.Мельникова; под ред. В.М.Фомичева.- М.: Издательство Юрайт,2018 - 209 с.

5.2 Перечень дополнительной литературы

1. Фомичев В.М.Криптографические методы защиты информации В 2 Ч. ЧАСТЬ 2. Системные и прикладные аспекты. Учебник для академического бакалавриат/В.М.Фомичев, Д.А.Мельникова; под ред. В.М.Фомичева.- М.: Издательство Юрайт,2018 - 245 с.

2. Understanding Cryptography / Christof Paar; Jan Pelzl; Nugent. Springer Berlin Heidelberg. 2010

3. Cryptography / Rubinstein-Salzedo; Amzad. Springer International Publishing. 2018

Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.3 Электронные ресурсы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2.	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
ЗНАТЬ				
1	Студент не усвоил следующие знания: наименование и область применения криптографических стандартов	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированны е знания по темам: наименование и область применения криптографиче ских стандартов; типовые криптографич еские протоколы и требования к ним	Студент способен самостоятельно выделять главные положения в изученном материале. Знает: внутреннюю структуру стандартных прикладных протоколов. отечественные и зарубежные стандарты в области криптографии	Студент знает, понимает, выделяет главные положения в изученном материале и Знает: внутреннюю структуру стандартов на криптографиче ские протоколы, их область применения и свойства. отечественные и зарубежные стандарты в области криптографии, перспективные криптографиче ские схемы
УМЕТЬ				
2	Студент не умеет проводить сравнительны й анализ криптографических протоколов, решающих сходные задачи; формулироват ь задачу по оцениванию безопасности криптографич еского протокола	Студент испытывает затруднения при определении разновидности протокола для решения конкретной задачи; оценивании применимости того или иного отечественного стандарта. верно определять вид протокола по его	Студент умеет использовать стандартные программноаппаратные средства, реализующие тот или иной стандарт криптографического протокола; оценить применимость того или иного стандарта. использовать симметричные и асимметричны е	Студент умеет самостоятельн о реализовать стандартный криптографиче ский протокол. оценить применимость того или иного протокола. использовать симметричные и

		структуре	криптосистем ы для построения криптографич еских протоколов; распознавать структуру протокола, выделять составляющие его примитивы.	асимметричны е криптосистем ы для построения криптографич еских протоколов; строить прикладные протоколы на основе криптографиче ских примитивов
ВЛАДЕТЬ				
3	Студент не владеет подходами к анализу безопасности криптографических протоколов. навыками оценки эффективности протокола. навыками программной реализации криптографич еских протоколов	Студент владеет методикой построения модели нарушителя. способностью описать свойства протокола, понятиями полноты и корректности. навыками использования библиотек криптографиче ских примитивов.	Студент владеет методикой выбора программноаппаратног о комплекса для решения конкретной задачи. способностью описать свойства протокола в рамках специальной терминологии, показать полноту протокола .навыками программной реализации криптографиче ских примитивов	Студент владеет навыками анализа безопасности криптографиче ских протоколов. навыками строгого доказательства свойств полноты и корректности протоколов. навыками программной реализации криптографиче ских протоколов
	Компетенции или их части не сформированы.	Компетенции или их части сформированы на базовом уровне.	Компетенции или их части сформированы на среднем уровне.	Компетенции или их части сформированы на высоком уровне.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия	Используемые интерактивные образовательные	Количество

	(Л, ПР, ЛР)	технологии	часов
1	Л	Лекция-беседа, ТСО (мультимедийный проектор, презентации PowerPoint)	10
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	24
	ЛР	Не предусмотрены	
	КР	Устный опрос	
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	146
Итого:			216

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос, защита отчетов по практическим работам, работа на компьютерах в парах, презентация в режиме диалога, работа в парах.

Промежуточная аттестация – зачет с оценкой.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к экзамену

1. Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы.
2. Понятие о криптографических протоколах. Полнота и корректность.
3. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.
4. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.
5. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.
6. Протоколы привязки к биту. Блоб.
7. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.
8. Совершенная СРС (система разделения доступа), идеальная СРС.
9. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.
10. Схема Блэкли. Вопрос о ее совершенности и идеальности.
11. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.
12. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.
13. Протоколы конфиденциальных вычислений.
14. Проверяемое разделение секрета.
15. Протоколы идентификации. Классификация. Требования.
16. Парольные схемы. Разновидности. Область применения.

17. Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».

18. Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».

19. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.

20. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.

21. Схема идентификации Окамото и теорема о ее условной стойкости.

22. Схема Гиллу-Кискатр. Ее полнота и корректность.

23. Слепая подпись.

24. Скрытый канал.

25. Протокол «Покер по телефону».

26. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.

27. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Разного достоинства. Схема с копилкой.

28. Протоколы голосования.

29. Протоколы установления подлинности.

30.Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.

31.Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.

32.Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.

33. Схемы Wide-Mouth Frog, Yahalom. Их анализ.

34. Протокол Нидхема-Шредера. Его анализ.

35. Протокол Отвея-Рииса. Его анализ.

36. Бесключевой протокол Шамира и атака «Человек посередине».

37.Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.

38. Протокол Нидхема-Шредера на основе шифра с открытым ключом.

39. Широковещательное распределение ключей.

40. Стандарт x.509.

41.Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-2*	ПК-6,ПК-1,ПК-9

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой