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

РАБОЧАЯ ПРОГРАММА 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

Курс 1 семестр 1

Москва 2025

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью дисциплины является 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-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-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-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 части, формируемой участниками образовательных отношений. Она является базой для дальнейшего освоения таких дисциплин, как:

- Техническая защита информации,
- Защита в операционных системах,
- Архитектура сетевой безопасности и управление процессом обеспечения безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Криптографические протоколы» составляет 6 зачетных единиц/216 часов:

Вид учебной работы	Всего, часов	Очная форма Курс, часов 1 курс, 1 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*30*	*30*
Лекции	8	8
Практические занятия	22	22
Лабораторные занятия		
Самостоятельная работа обучающихся	78	78
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа	36	36
Курсовая работа		
Зачет с оценкой		
Экзамен	+	+
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	144\4	144\4

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции
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	ПК-6,ПК-1,ПК-9

		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. 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	Контроль	Всего часов	Формы текущего контроля успеваемости
1.	Криптографические алгоритмы	4	10	39	18	71	Устный опрос
2.	Криптографические протоколы	4	12	39	18	73	Устный опрос
Экзамен		2					
	Итого:	8	22	78	36	144\4	

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.	1
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.	1
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.	2
1. Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. 2. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. 3. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. 4. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных	2

шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров.	
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.	2
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".	6
1. Управление открытыми ключами. 2. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. 3. Стандарт X.509. Сервисы инфраструктуры открытых ключей	6

2.6. Планы лабораторных работ – не предусмотрено.

Задания, вопросы, для самостоятельного изучения (задания)	**Всего часов**
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.	13
Основные алгоритмы с открытым ключом и управление ключами	13
Симметричные криптосистемы	13
Протоколы цифровых денег Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.	13

Протокол электронного голосования Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.	13
Постквантовая 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.	13

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, 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 РГУ СоцТех.

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

5.1 **Перечень основной литературы**

1. Соколов, А. В. Криптографические конструкции на основе функций многозначной логики : монография / А.В. Соколов, О.Н. Жданов. — Москва : ИНФРА-М, 2022. — 192 с. — (Научная мысль). — DOI 10.12737/1045434. - ISBN 978-5-16-015667-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1816421 (дата обращения: 09.04.2025). – Режим доступа: по подписке.
2. Кобылянский, В. Г. Сетевые информационные технологии. Моделирование и основные протоколы компьютерных сетей : учебное пособие / В. Г. Кобылянский. - Новосибирск : Изд-во НГТУ, 2021. - 131 с. - ISBN 978-5-7782-4341-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1866923 (дата обращения: 09.04.2025). – Режим доступа: по подписке.
3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И.

Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560426 (дата обращения: 09.04.2025).

5.2 **Перечень дополнительной литературы**

1. Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/991903 (дата обращения: 09.04.2025). – Режим доступа: по подписке.
2. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 09.04.2025). – Режим доступа: по подписке.

5.3 **Программное обеспечение**

1. Astra Linux Special Edition – операционная система со встроенными верифицированными средствами защиты информации.
2. Почта VK WorkMail – корпоративная почта для бизнеса.
3. КонтурТолк – российский сервис для видеоконференцсвязи
4. КонсультантПлюс – кроссплатформенная справочная правовая система, разработанная в России.
5. Антиплагиат ВУЗ – система проверки текстов на уникальность.
6. МАРК-SQL – автоматизированная информационно-библиотечная система (АИБС).
7. Антивирус Касперского – антивирусное программное обеспечение, разрабатываемое «Лабораторией Касперского».

5.4 **Электронные ресурсы**

1. Национальный открытый университет ИНТУИТ [Электронный ресурс]. URL: http://www.intuit.ru
2. Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/
3. http://www.lessons-tva.info/ - На сайте представлены различные учебные материалы, в том числе онлайн учебники (авторские курсы) по дисциплинам: экономическая информатика, компьютерные сети и телекоммуникации, основы электронного бизнеса, информатика и компьютерная техника.
4. Java портал Sun Microsystems – http://java.sun.com
5. Programmer’s Forum: http://www.programmist.net
6. Портал разработчиков андроид: http://developer.android.com
7. Библиотека ТехНэт: http://technet.microsoft.com/ru-ru/library/aa991542
8. Электронная библиотечная система «Лань»: https://e.lanbook.com/
9. Электронная библиотечная система «Znanium»: https://znanium.ru/
10. Образовательная платформа «Юрайт»: https://urait.ru/
11. Научная электронная библиотека eLIBRARY.RU: https://elibrary.ru/
12. Справочно-правовая система «КонсультантПлюс»: http://www.consultant.ru/
13. Polpred.com. Обзор СМИ: https://polpred.com/news
14. Национальная электронная библиотека: https://rusneb.ru/
15. Электронная Библиотека РГУ СоцТех: https://portal.rgust.ru/biblio_cat

6 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Аудитория №109	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 16 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 11 Системных блоков IRu, 11 Мониторов Acer, 11 клавиатур Mitsumi KFK-EA4XT, 11 мышей Gemberd MUSOKTI9-905U; Акустическая система Sven; Свитч; Вебкамера Sven; Интерактивная панель AnTouch ANTP-86-20i; Видеокамера Dahua DH-IPC.
1.	Аудитория №111	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 11 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: Моноблок Lenovo; клавиатура Lenovo EKB-536A; мышь Lenovo EMS-537A; доска меловая. Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
	Аудитория №302б	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: Рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 9 Системный блок, Монитор 10, клавиатура 9, мышь 10; Мультимедийный проектор Epson EH-TW535W; Акустическая система Topdevice TDE210 Вебкамера AuTech PK910K; Доска меловая; Интерактивная панель Smart; Видеокамера Dahua DH-IPC.
2.	Аудитория №303	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 20 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием:

		1 компьютер – Системный блок Soprano, Монитор Samsung 940NW, клавиатура Logitech K120, мышь Logitech M100; Мультимедийный проектор NEC NP15LP; Акустическая система Sven SPS-605; Вебкамера Microsoft F/2.0HD; Проекционный экран; Меловая доска; Видеокамера Dahua DH-IPC.
3.	Аудитория №304	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 13 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 10 моноблоков – Lime, 10 - клавиатур, 10 - компьютерных мышей, 10 – трэкболов, 10 – специальных клавиатур для инвалидов
4.	Аудитория №305	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 32 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок, Монитор DELL, клавиатура Logitech DeLuxe 250, мышь Logitech M100; Мультимедийный проектор Epson EH-TW535W; Акустическая система SVEN 230; Вебкамера PK910P; Интерактивная доска Smart Board; Проекционный экран; Меловая доска; Видеокамера Dahua DH-IPC.
5.	Аудитория №306	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 23 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 12 Системных блоков IR, 12 Монитор Acer , 12 клавиатур, 12 мышей; Мультимедийный проектор Epson EH-TW535W; Акустическая система Gembird; Смарт доска Panasonic UBT880W; Вебкамера Logi; Меловая доска; Видеокамера Dahua DH-IPC.
6.	Аудитория №308	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 22 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 12 Моноблоков DEPO; 12 Клавиатур DEPO K-0105U; 12 Мышей DEPO MRV-1190U;

		Мультимедийный проектор EPSON EB-440W; Акустическая система Topdevice TDE 210/2.1; Интерактивная панель AnTouch ANTP-86-20i; Видеокамера Dahua DH-IPC.
7.	Аудитории № 309	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 17 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 моноблок Lenovo V530-24ICB AIO, клавиатура Lenovo EKB-536A, мышь Lenovo EMS-537A; 11- системных блоков, 11 – мониторов Acer, 11 – клавиатур, 11- компьютерных мышей; Свитч; Меловая доска; Видеокамера Dahua DH-IPC.
8.	Аудитории № 310	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 18 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 Моноблок Lenovo V530-24ICB, клавиатура Lenovo EKB-536A, мышь Logitech M100; Меловая доска; Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
9.	Аудитории № 311	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 20 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 Моноблок Lenovo V530-24ICB, клавиатура Lenovo EKB-536A, мышь Lenovo EMS-537A; Меловая доска; Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
10.	Аудитория №402	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 26 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 12 компьютер – Системный блок, Монитор Asus, клавиатура, мышь; Клавиатура для слабовидящих BNC Distribution; Мультимедийный проектор Epson EH-TW535W; Акустическая система Sven;

		Вебкамера AuTech PK910K; Видеокамера Dahua DH-IPC.
11.	Аудитория №403	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 24 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок IN WIN, Монитор Samsung 940NW, клавиатура Mitsumi KFK-EA4XY, мышь 3D Optical Mouse; Акустическая система Sven 245; Вебкамера A4Tech PK910K; Интерактивная панель Geckotouch. Видеокамера Dahua DH-IPC – 2 шт.
12.	Аудитория №404 (учебный зал судебных заседаний)	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 24 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок IN WIN, Монитор Samsung, клавиатура Genius GK04006, мышь Logitech M100; Мультимедийный проектор Epson EH-TW535W; Акустическая система Sven 245; Вебкамера PK-910M; Интерактивная панель Geckotouch; Видеокамера Dahua DH-IPC – 2 шт. Материально-техническое оснащение: Герб 1 Флаг 1 Трибуна для выступлений участников процесса 1 Молоток 1 Стол судейский 3 Стул судейский 3 Столы ученические 12 Стулья ученические 24 Доска трехстворчатая 1 Стол прокурора 1 Стол адвоката 1 Микрофон 1 Скамья подсудимых 1 Ограждение скамьи подсудимых 1 Табличка «Список дел, назначенных к слушанию» 1 Плакаты Судебное следствие (гл.37 УПК РФ (извлечение) 12 Технологии в зале судебных заседаний 5 ФЗ «О статусе судей в РФ» (извлечение) 3
13.	Аудитория №405	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации:

		32 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок, Монитор Samsung, клавиатура Genius GK04006, мышь Logitech M100; Мультимедийный проектор Epson EB-440W; Акустическая система Sven; Вебкамера Logi; Интерактивная доска Smart Board; Меловая доска; Видеокамера Dahua DH-IPC.
14.	Аудитория №409	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 32 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок Tiger X-510, Монитор, клавиатура Logitech Y-UT76, мышь Logitech B100; Мультимедийный проектор EPSON EH-TW5300; Акустическая система Sven 312; Вебкамера Genius; Меловая доска; Интерактивная доска Smart; Видеокамера Dahua DH-IPC.
15.	Аудитории № 410	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 11 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 13 моноблоков Depo MF524, 13 клавиатур Depo K-0105U, 13 мышей Depo M-RV1190U; Свитч; Маркерная доска; Видеокамера Dahua DH-IPC.
16.	Аудитории № 411	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 15 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок Tiger X-510, Монитор Loc M2470S, клавиатура Logitech Y-SU61, мышь Gembid MUSOPTI99054; Колонки Microlab B53; Вебкамера Logi; Меловая доска; Видеокамера Dahua DH-IPC.
17.	Аудитории № 412	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 13 посадочных мест, рабочее место преподавателя,

		оснащенные учебной мебелью, оборудованием: 1 моноблок HP 24 in One PC, клавиатура, мышь Genius GM12001U; Акустическая система Sven; Вебкамера Logi; Меловая доска; Видеокамера Dahua DH-IPC.
18.	Библиотека	Помещения для самостоятельной работы: 20 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 2 Системных блока; 7 Мониторов Samsung 920NW; 10 Клавиатур;11 Мышей; 6 ноутбуков RBook; Моноблок Lenovo; МФУ-Kyocera M2040DN.
19.	Актовый Зал (студенческое пространство)	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 6 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 2 Системных блока; 2 Монитора Acer; 2 Клавиатуры; 3 Мыши; Веб камера Genius; Колонки Defender, интерактивная панель Nova
20.	Аудитория №2-120	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 36 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок, Монитор Asus, клавиатура, мышь; Клавиатура для слабовидящих BNC Distribution; Мультимедийный проектор Epson EH-TW535W; Акустическая система Sven; Вебкамера AuTech PK910K; Интерактивная доска Smart Board; Меловая доска.
21.	Аудитория № 3-210	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 16 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: Ноутбук Asus K53E; Мышь Logitech B100; Доска меловая; Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
22.	Аудитория № 3-212	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 19 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием:

		Ноутбук HP Probook; Мышь Logitech B100; Доска меловая; Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
23.	Аудитория № 3-214	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 12 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: Ноутбук HP RTL8822CE; Мышь Logitech B100; Доска меловая; Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
24.	Аудитория № 3-216	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 19 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 9 компьютер – Системный блок, 9 Монитор Samsung, 9 клавиатура Logitech Y-SU61, 9 мышь 3D Optical Mouse; Веб камера A4Tech; Колонки Gembird; Доска меловая; Проектор; Экран для проектора; Видеокамера Dahua DH-IPC.
25.	Аудитория № 3-219	Помещение для лекционных, практических занятий (семинаров), групповых и индивидуальных консультаций, самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации: 19 посадочных мест, рабочее место преподавателя, оснащенные учебной мебелью, оборудованием: 1 компьютер – Системный блок, Монитор BENQ, клавиатура Logitech K120, мышь Logitech M100; Веб камера Genius; Колонки Gembird; Проектор Epson H551B; Проекционный экран; Доска меловая; Видеокамера Dahua DH-IPC.

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 структуре	Студент умеет использовать стандартные программноаппаратные средства, реализующие тот или иной стандарт криптографического протокола; оценить применимость того или иного стандарта. использовать симметричные и асимметричны е криптосистем ы для построения криптографич еских протоколов; распознавать структуру протокола, выделять составляющие его примитивы.	Студент умеет самостоятельн о реализовать стандартный криптографиче ский протокол. оценить применимость того или иного протокола. использовать симметричные и 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 (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество 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	36
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	146
Итого:			216\6

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 – экзамен.

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.

9.5. 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