Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Богдалова Елена Вячеславовна
Должность: Проректор по образовательной деятельности
Дата подписания: 22.07.2025 14:01:18
Уникальный программный ключ:
ec85dd5a839619d48ea76b2d23dba88a9c82091a

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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ОСВОЕНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

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. Аннотация
2. Методические рекомендации к лекциям
3. Методические рекомендации к практическим занятиям
4. Методические рекомендации к самостоятельной работе

АННОТАЦИЯ

Настоящие методические рекомендации разработаны для обучающихся очной формы обучения с учетом ФГОС ВО и рабочей программы дисциплины.

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.

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций:

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.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ЛЕКЦИЯМ

Лекция 1 по теме: «Понятие криптографического протокола»

Вопросы:

1. Основные определения.
2. Свойства, характеризующие безопасность протоколов.
3. Виды криптографических протоколов.
4. Основные атаки на безопасность протоколов.

Методические рекомендации

Лекция проводится как с применением традиционных технологий (обзорная лекция), так и интерактивных технологий (проблемная лекция).

В ходе лекционных занятий студентам рекомендовано вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Дорабатывать конспект лекции рекомендовано в соответствии рабочей программой дисциплины.

Источники и литература для подготовки:

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.

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

Лекция 2 по теме: «Криптографические хеш-функции»

Вопросы:

1. Функции хеширования и целостность данных.
2. Хеш-функции, задаваемые ключом.
3. Хеш-функции, не зависящие от ключа.
4. Возможные атаки на функции хеширования.

Методические рекомендации

Лекция проводится как с применением традиционных технологий (обзорная лекция), так и интерактивных технологий (проблемная лекция).

В ходе лекционных занятий студентам рекомендовано вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Дорабатывать конспект лекции рекомендовано в соответствии рабочей программой дисциплины.

Источники и литература для подготовки:

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.

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

Лекция 3 по теме «Коды аутентификации»
Вопросы:

1. Определения и свойства.
2. Ортогональные массивы.

Методические рекомендации

Лекция проводится как с применением традиционных технологий (обзорная лекция), так и интерактивных технологий (проблемная лекция).

В ходе лекционных занятий студентам рекомендовано вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Дорабатывать конспект лекции рекомендовано в соответствии рабочей программой дисциплины.

Источники и литература для подготовки:

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.

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

Лекция 4 по теме «Протоколы идентификации»
Вопросы:

1. Виды протоколов идентификации;
2. Протоколы идентификации, использующие пароли (слабая аутентификация);
3. Протоколы идентификации, использующие технику «запрос — ответ» (сильная аутентификация).

Методические рекомендации

Лекция проводится как с применением традиционных технологий (обзорная лекция), так и интерактивных технологий (проблемная лекция).

В ходе лекционных занятий студентам рекомендовано вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Дорабатывать конспект лекции рекомендовано в соответствии рабочей программой дисциплины.

Источники и литература для подготовки:

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.

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

Лекция 5 по теме «Управление ключами»

Вопросы:

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.

Методические рекомендации

Лекция проводится как с применением традиционных технологий (обзорная лекция), так и интерактивных технологий (проблемная лекция).

В ходе лекционных занятий студентам рекомендовано вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Дорабатывать конспект лекции рекомендовано в соответствии рабочей программой дисциплины.

Источники и литература для подготовки:

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.

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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Практическое занятие 1 по теме 1: «Криптографические протоколы»
Вопросы:

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.

Практические задания:

1. Исследовать процесс шифрования с помощью простой замены.
2. Исследовать процесс шифрования с помощью решетки Кардано.
3. Исследовать процесс шифрования с помощью таблицы Виженера.

Методические рекомендации

При подготовке к практическим занятиям студент должен придерживаться следующих рекомендаций:

- внимательно изучить основные вопросы темы и план практического занятия,
- определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных нормативных документах, учебниках и дополнительной литературе;
- после ознакомления с теоретическим материалом ответить на вопросы по теме курса;
- продумать пути и способы решения проблемных вопросов;
- продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

В ходе практического занятия необходимо выполнить практическое задание, а затем объяснить методику его решения.

Источники и литература для подготовки:

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.

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

Практическое занятие 2 по теме «Криптографическая защита информации»

Вопросы:

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.

Практические задания:

1. Исследовать процесс вычисления ключей в блочном шифре с использованием программной реализации.

Источники и литература для подготовки:

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.

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

Практическое занятие 3 по теме «Управление ключами»

Вопросы:

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.

Практические задания:

1. Исследование процесса Шифрования сообщений с помощью упрощенного S-DES с использованием программной реализации.

Методические рекомендации

При подготовке к практическим занятиям студент должен придерживаться следующих рекомендаций:

- внимательно изучить основные вопросы темы и план практического занятия,
- определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных нормативных документах, учебниках и дополнительной литературе;
- после ознакомления с теоретическим материалом ответить на вопросы по теме курса;
- продумать пути и способы решения проблемных вопросов;
- продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

В ходе практического занятия необходимо выполнить практическое задание, а затем объяснить методику его решения.

Источники и литература для подготовки:

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.

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

Практическое занятие 4 по теме «Протоколы передачи ключей»

Вопросы:

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".

Практические задания:

1. Исследование поточного шифрования сообщений в самосинхронизующихся системах на основе многотактовых кодовых фильтров с использованием программной реализации.

Методические рекомендации

При подготовке к практическим занятиям студент должен придерживаться следующих рекомендаций:

- внимательно изучить основные вопросы темы и план практического занятия,
- определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных нормативных

документах, учебниках и дополнительной литературе;

- после ознакомления с теоретическим материалом ответить на вопросы по теме курса;

- продумать пути и способы решения проблемных вопросов;

-продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

В ходе практического занятия необходимо выполнить практическое задание, а затем объяснить методику его решения.

Источники и литература для подготовки:

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.

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

Практическое занятие 5 по теме «Управление открытыми ключами»

Вопросы:

1. Управление открытыми ключами.
2. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа.
3. Стандарт X.509. Сервисы инфраструктуры открытых ключей

Практические задания:

1. Исследование процесса ассиметричного шифрования без передачи ключа.
2. Исследование процесса ассиметричного шифрования RSA.
3. Исследование процесса ассиметричного шифрования Эль-Гамаля.

Методические рекомендации

При подготовке к практическим занятиям студент должен придерживаться следующих рекомендаций:

- внимательно изучить основные вопросы темы и план практического занятия,
- определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных нормативных документах, учебниках и дополнительной литературе;
- после ознакомления с теоретическим материалом ответить на вопросы по теме курса;

- продумать пути и способы решения проблемных вопросов;
- продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

В ходе практического занятия необходимо выполнить практическое задание, а затем объяснить методику его решения.

Источники и литература для подготовки:

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.

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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ

Самостоятельная работа по теме «Вычислительная и безусловная связанность, секретность.»

Вопросы:

1. Критерии безопасности компьютерных систем.
2. Преимущества и недостатки Оранжевой книги.

Методические рекомендации

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Самостоятельная работа студентов при подготовке к лекции заключается в рассмотрении общих научных основ и анализе конкретных процессов и факторов, определяющих содержание темы.

Самостоятельная работа студентов при подготовке к практическому занятию включает подбор материала, данных и специальных источников, с которыми предстоит учебная работа, а также решение ситуационных и практических заданий. В связи с этим студентам рекомендуется детально разобрать теоретические вопросы лекционного курса, а затем закрепить материал в процессе решения проблемных ситуаций, задач.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Решение проблемных задач следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями и схемами. Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра, а не за несколько дней до его проведения. При подготовке к зачету студентам рекомендуется:

- перечитать все лекции, а также материалы, которые готовились к практическим занятиям в течение семестра.

- соотнести эту информацию с вопросами, которые даны к зачету. Если информации недостаточно, ответы находят в предложенной преподавателем литературе.

При подготовке к зачету рекомендуется делать краткие записи для формирования четкой логической схемы ответа на вопрос.

Источники и литература для подготовки:

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.

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

Самостоятельная работа по теме «Протоколы привязки к биту на основе проблемы дискретного логарифмирования, на основе симметричной криптосистемы, на основе односторонней функции, односторонней перестановки»

Вопросы:

1. Протоколы конфиденциальных вычислений.
2. Проверяемое разделение секрета.
3. Протоколы идентификации. Классификация. Требования

Методические рекомендации

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Самостоятельная работа студентов при подготовке к лекции заключается в рассмотрении общих научных основ и анализе конкретных процессов и факторов, определяющих содержание темы.

Самостоятельная работа студентов при подготовке к практическому занятию включает подбор материала, данных и специальных источников, с которыми предстоит учебная работа, а также решение ситуационных и практических заданий. В связи с этим студентам рекомендуется детально разобрать теоретические вопросы лекционного курса, а затем закрепить материал в процессе решения проблемных ситуаций, задач.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Решение проблемных задач следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями и схемами. Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра, а не за несколько дней до его проведения. При подготовке к зачету студентам рекомендуется:

- перечитать все лекции, а также материалы, которые готовились к практическим занятиям в течение семестра.

- соотнести эту информацию с вопросами, которые даны к зачету. Если информации недостаточно, ответы находят в предложенной преподавателем литературе.

При подготовке к зачету рекомендуется делать краткие записи для формирования четкой логической схемы ответа на вопрос.

Источники и литература для подготовки:

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.

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

Самостоятельная работа по теме «Аутентификация источника данных. Аутентификация сущности.»

Вопросы:

1. Понятие аутентификации источника данных.
2. Как происходит ауетнтификация источника данных и сущности.
3. Цель аутентификации источника данных.

Методические рекомендации

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Самостоятельная работа студентов при подготовке к лекции заключается в рассмотрении общих научных основ и анализе конкретных процессов и факторов, определяющих содержание темы.

Самостоятельная работа студентов при подготовке к практическому занятию включает подбор материала, данных и специальных источников, с которыми предстоит учебная работа, а также решение ситуационных и практических заданий. В связи с этим студентам рекомендуется детально разобрать теоретические вопросы лекционного курса, а затем закрепить материал в процессе решения проблемных ситуаций, задач.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Решение проблемных задач следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями и схемами. Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра, а не за несколько дней до его проведения. При подготовке к зачету студентам рекомендуется:

- перечитать все лекции, а также материалы, которые готовились к практическим занятиям в течение семестра.

- соотнести эту информацию с вопросами, которые даны к зачету. Если информации недостаточно, ответы находят в предложенной преподавателем литературе.

При подготовке к зачету рекомендуется делать краткие записи для формирования четкой логической схемы ответа на вопрос.

Источники и литература для подготовки:

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.

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

Самостоятельная работа по теме «Генерация аутентифицированных ключей»

Вопросы:

1. Генерация аутентифицированных ключей.
2. Основные методы и механизмы аутентификации.
3. Стратегия «оклик-отзыв».

Методические рекомендации

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Самостоятельная работа студентов при подготовке к лекции заключается в рассмотрении общих научных основ и анализе конкретных процессов и факторов, определяющих содержание темы.

Самостоятельная работа студентов при подготовке к практическому занятию включает подбор материала, данных и специальных источников, с которыми предстоит учебная работа, а также решение ситуационных и практических заданий. В связи с этим студентам рекомендуется детально разобрать теоретические вопросы лекционного курса, а затем закрепить материал в процессе решения проблемных ситуаций, задач.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Решение проблемных задач следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями и схемами. Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра, а не за несколько дней до его проведения. При подготовке к зачету студентам рекомендуется:

- перечитать все лекции, а также материалы, которые готовились к практическим занятиям в течение семестра.

- соотнести эту информацию с вопросами, которые даны к зачету. Если информации недостаточно, ответы находят в предложенной преподавателем литературе.

При подготовке к зачету рекомендуется делать краткие записи для формирования четкой логической схемы ответа на вопрос.

Источники и литература для подготовки:

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.

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

Самостоятельная работа по теме «Схема разделения секрета»

Вопросы:

1. Понятие схемы разделения секрета (СРС).
2. Группа доступа. Структура доступа.
3. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках.

Методические рекомендации

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Самостоятельная работа студентов при подготовке к лекции заключается в рассмотрении общих научных основ и анализе конкретных процессов и факторов, определяющих содержание темы.

Самостоятельная работа студентов при подготовке к практическому занятию включает подбор материала, данных и специальных источников, с которыми предстоит учебная работа, а также решение ситуационных и практических заданий. В связи с этим студентам рекомендуется детально разобрать теоретические вопросы лекционного курса, а затем закрепить материал в процессе решения проблемных ситуаций, задач.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Решение проблемных задач следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями и схемами. Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует

условие, и по возможности с выводом.

Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра, а не за несколько дней до его проведения. При подготовке к зачету студентам рекомендуется:

- перечитать все лекции, а также материалы, которые готовились к практическим занятиям в течение семестра.

- соотнести эту информацию с вопросами, которые даны к зачету. Если информации недостаточно, ответы находят в предложенной преподавателем литературе.

При подготовке к зачету рекомендуется делать краткие записи для формирования четкой логической схемы ответа на вопрос.

Источники и литература для подготовки:

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.

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

Самостоятельная работа по теме «Разделение секрета для произвольной группы»

Вопросы:

1. Разделение секрета для произвольной группы доступа.
2. Совершенная СРС. Идеальное разделение секрета.
3. Проверяемое разделение секрета.

Методические рекомендации

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Самостоятельная работа студентов при подготовке к лекции заключается в рассмотрении общих научных основ и анализе конкретных процессов и факторов, определяющих содержание темы.

Самостоятельная работа студентов при подготовке к практическому занятию включает подбор материала, данных и специальных источников, с которыми предстоит учебная работа, а также решение ситуационных и практических заданий. В связи с этим студентам рекомендуется детально разобрать теоретические вопросы лекционного курса, а затем закрепить материал в процессе решения проблемных ситуаций, задач.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Решение проблемных задач следует излагать подробно, вычисления располагать в строгом порядке, отделяя

вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями и схемами. Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра, а не за несколько дней до его проведения. При подготовке к зачету студентам рекомендуется:

- перечитать все лекции, а также материалы, которые готовились к практическим занятиям в течение семестра.

- соотнести эту информацию с вопросами, которые даны к зачету. Если информации недостаточно, ответы находят в предложенной преподавателем литературе.

При подготовке к зачету рекомендуется делать краткие записи для формирования четкой логической схемы ответа на вопрос.

Источники и литература для подготовки:

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.

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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