МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Российский государственный гуманитарный университет»**
**(ФГБОУ ВО «РГГУ»)**

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра комплексной защиты информации

# КРИПТОГРАФИЯ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

01.04.04 Прикладная математика

*Код и наименование направления подготовки/специальности*

Математические методы и модели обработки
и защиты информации в социотехнических системах

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *магистратура*

Форма обучения: *очная, очно-заочная, заочная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

КРИПТОГРАФИЯ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, доцент, доцент кафедры международной информационной безопасности ФГБОУ ВО МГЛУ М.В. Шептунов

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
фундаментальной и прикладной математики
№ 8 от 23.03.2023

ОГЛАВЛЕНИЕ

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины: развитие способностей к логическому и алгоритмическому мышлению; получение студентами знаний в сфере криптографии, по её вопросам системного характера, необходимым для решения теоретико-практических задач социотехнической направленности.
Задачи дисциплины:

- научиться определять основные требования к криптографической защите информации в их взаимосвязи применительно к социотехническим системам;
- научиться формировать множество целевых ориентиров при криптографической защите информации с учётом структурных особенностей среды;
- научиться определять и учитывать качественные и количественные особенности составляющих криптографической защиты;
- получить навыки оценки эффективности тех или иных криптографических преобразований;
- получить представление о механизмах смены параметров криптографической защиты для социотехнических систем;
- научиться решать основополагающие теоретико-практические задачи социотехнической направленности с применением необходимого математического аппарата.

### 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

| **Компетенция** (код и наименование) | **Индикаторы компетенций** (код и наименование) | **Результаты обучения** |
|---|---|---|
| ПК-2. Способен осуществлять поиск, изучение и разработку новых теоретических или практических проблем, сведений, относящихся к решению текущих научных исследований, производственных задач; в информационных средах находить, создавать основные элементы будущих математических структур или конструктивных математических моделей | ПК-2.3. Выделяет информационные потоки, определяет точки бифуркаций | *Знать*: основные модели, методы и средства криптографии<br>*Уметь*: применять методы и модели криптографии с необходимыми формулами для решения математических прикладных задач, характерных для социотехнических систем.<br>*Владеть*: методами проведения экспериментов в области синтеза и анализа криптографических систем и оценки их результатов. |

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Криптография в социотехнических системах» относится к дисциплинам части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: “Алгебра и ее современные приложения”, “Принципы построения математических моделей в социотехнических системах”.
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: “Криптографические приложения в социотехнических системах”, “Математические методы управления социотехническими системами”, Учебная практика (Научно-исследовательская работа), Производственная практика (Научно-исследовательская работа).

**2. Структура дисциплины**

Общая трудоёмкость дисциплины составляет 5 з.е., 180 академических часа(ов).

**Структура дисциплины для очной формы обучения**

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий | Количество часов |
|---|---|---|
| **3** | Лекции | **16** |
| **3** | Лабораторные занятия | **34** |
| | Всего: | **50** |

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 130 академических часа(ов).

**Структура дисциплины для очно-заочной формы обучения**

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий | Количество часов |
|---|---|---|
| **3** | Лекции | **16** |
| **3** | Лабораторные занятия | **24** |
| | Всего: | **40** |

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 140 академических часа(ов).

**Структура дисциплины для заочной формы обучения**

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий | Количество часов |
|---|---|---|
| **3** | Лекции | **8** |
| **3** | Лабораторные занятия | **12** |
| | Всего: | **20** |

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 160 академических часа(ов).

### 3. Содержание дисциплины

| № | Наименование раздела дисциплины | Содержание |
|---|---|---|
| 1 | **Криптография и её математические основы; идентификация и аутентификация** | ***Тема 1. Некоторые традиционные одноключевые криптосистемы и вопросы классификации систем, их закономерностей и ошибок операторов сложных социотехнических систем***<br>Основные понятия и определения криптографии и социотехнических систем. Обобщённая модель симметричной криптосистемы. Понятие криптографического протокола. Модель нарушителя информационной системы. Понятия идентификации и аутентификации. Принцип (правило) Кёркхоффа. Шифры простой замены; шифрующие таблицы Трисемуса. Шифры сложной замены; шифр Гронсфельда, система шифрования Вижинера, шифр “двойной квадрат” Уитстона. Шифрование перестановкой; использование маршрутов Гамильтона. Некоторые вопросы классификации систем и их закономерности. Компоненты и подсистемы. Надсистемы. Система и среда. Связи. Разделение алгоритма процесса на подсистемы. Классификация ошибок операторов сложных социотехнических систем<br>***Тема 2. Понятие о блочном и поточном шифровании***<br>Понятия блочного и поточного шифрования и их основные особенности. Шифрование методом гаммирования. Возможности использования сдвиговых регистров для генерации псевдослучайных последовательностей. Абонентское шифрование<br>***Тема 3. Теоретико-числовые основы криптографии и их применение***<br>Обратимость как важное свойство, используемое в криптографии. Алгоритм Евклида для отыскания наибольшего общего делителя. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение. Конечные поля. Поле Галуа. Вычеты, кольца вычетов. Решение сравнений и систем сравнений. Функция Эйлера, теорема Эйлера. Понятие дискретного логарифма. Основы двухключевых криптосистем. Обобщённая модель асимметричной криптосистемы<br>***Тема 4. Некоторые двухключевые асимметричные криптосистемы и их использование в режиме шифрования***<br>Криптосистема RSA и её использование в режиме шифрования. Криптосистема Эль-Гамаля и её использование в режиме шифрования. Условно стойкие, вычислительно стойкие и безусловно стойкие шифры. Понятия односторонней (однонаправленной) функции и односторонней (однонаправленной) функции с потайным ходом (лазейкой). Атака на криптосистему RSA методом факторизации.<br>***Тема 5. Использование известных двухключевых*** |

| | | |
|---|---|---|
| | | ***асимметричных криптосистем в режиме электронной цифровой подписи***<br>Понятия односторонней (однонаправленной) хеш-функции и электронной цифровой подписи и основные требования к ним. Некоторые вопросы аутентификации. Использование криптосистемы RSA в режиме электронной цифровой подписи. Использование криптосистемы Эль-Гамаля в режиме электронной цифровой подписи.<br>***Тема 6. Отечественный Стандарт шифрования данных***<br>Отечественный Стандарт шифрования данных, режимы: простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки.<br>***Тема 7. Некоторые современные подходы к шифрованию информации***<br>Возможности шифрования на основе метода укладки рюкзака (упаковки ранца). Криптосхема с перестановкой фиксированных процедур. Шифры на основе процедур и операций преобразования, зависящих от преобразуемых данных. Шифры: с управляемыми операциями, на основе управляемых перестановок, с управляемыми подстановками, на основе модифицирования подключей. Многоуровневая криптография. Шарады с временны*м* замком, их построение и решение.<br>***Тема 8. Идентификация и аутентификация и управление ключами***<br>Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Проблемы аутентификации данных. Отечественный Стандарт хэш-функции и отечественный Стандарт цифровой подписи. Генерация и хранение ключей. Распределение ключей с участием центра распределения ключей и прямой обмен ключами между пользователями. Криптографические методы аутентификации для симметичной и несимметричной криптосистем: в режиме on-line, при участии нескольких серверов, в режиме off-line, с привлечением арбитра. Организация серверов аутентификации. Системы POS-терминалов и сети банкоматов и обеспечение их безопасности в ракурсе идентификации, аутентификации и управления ключами.<br>***Тема 9. Основные разновидности атак на шифры – криптоанализа***<br>Дифференциальный криптоанализ. Дифференциальный криптоанализ на основе отказов устройства. Линейный криптоанализ. Некоторые другие виды криптоанализа и атак.<br>***Тема 10. Древнекитайская теорема об остатках и схема разделения секрета на её основе***<br>Древнекитайская теорема об остатках. Понятия схемы разделения секрета и совершенной схемы разделения секрета. Применение теоремы об остатках для безопасного сохранения (защищённого разделения) ключа между двумя компаньонами в случае цифрового замка сейфа. Возможности использования квадратичных вычетов.<br>***Тема 11. Расчётные соотношения для контролируемой и неконтролируемой преград комплексной системы защиты*** |

| | | |
|---|---|---|
| | | ***информации***<br>Расчётные соотношения для контролируемой и неконтролируемой преград комплексной системы защиты информации в случаях однозвенной (элементарной) и многозвенной защиты. Защита штатного входа в систему и прочность защитной преграды. Случай многоуровневой защиты. |
| **2** | **Возможности дискретной оптимизации при криптографической защите и обработке информации в социотехнических системах** | ***Тема 12. Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа***<br>Задача об управлении кадрами подразделений как задача о назначениях. Венгерский метод решения задачи о назначениях. Технические приложения задачи о назначениях: распределение задач шифрования по компьютерам сети, оптимизация наборов прав пользователей при матричном принципе управления доступом. Возможности разбиения на классы для объектов и субъектов доступа. Роль бинарных отношений в попарном сравнении вариантов и выражении предпочтений экспертов по защите информации.<br>***Тема 13. Защита "ноу-хау" пороговыми схемами разделения секрета и оптимальность борьбы за рынки между двумя фирмами с учётом и без учёта страхования***<br>Особенности пороговых схем разделения секрета и возможности недобросовестной конкуренции между двумя фирмами. Игра на единичном квадрате и оптимальность борьбы за рынки при защищаемом пороговыми схемами разделения секрета "ноу-хау" с учётом и без учёта страхования. Инженерно-технические и информационные риски, возможности их страхования и страхование ответственности. |
| **3** | **Модели безопасности и контроля целостности информации и основные подходы к анализу защищённости криптографических протоколов** | ***Тема 14. Модель безопасности информационных потоков и другие модели безопасности***<br>Модель безопасности информационных потоков при использовании мандатного принципа управления доступом. Другие модели безопасности: модель Low-Water-Mark, модель "Китайской стены".<br>***Тема 15. Модели контроля целостности информации и контроль доступа, базирующийся на ролях***<br>Модели контроля целостности: модель Биба, модель Кларка-Вилсона. Контроль доступа, базирующийся на ролях и его актуальность для вычислительной системы организации.<br>***Тема 16. Основные подходы к анализу защищённости криптографических протоколов***<br>Четыре основных подхода к анализу защищённости криптографических протоколов. Моделирование и проверка работы протокола с использованием языков описания и средств проверки, не разработанных специально для анализа криптографических протоколов. Создание экспертных систем, позволяющих разработчику протокола исследовать различные сценарии. Выработка требований к семейству протоколов с использованием некой логики для анализа понятий "знание" и "доверие" (BAN-логика). Выработка формальных методов, основанных на записи свойств криптосистем в алгебраическом виде. |

## 4. Образовательные технологии

| № п/п | Наименование раздела | Виды учебных занятий | Образовательные технологии |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | **Криптография и её математические основы; идентификация и аутентификация** | Лекция 1. Некоторые традиционные одноключевые криптосистемы и вопросы классификации систем, их закономерностей и ошибок операторов сложных социотехнических систем. | Вводная лекция. |
| | | Лабораторная работа 1. Некоторые традиционные одноключевые криптосистемы и вопросы классификации систем, их закономерностей и ошибок операторов сложных социотехнических систем. | Вводное занятие. Лабораторная работа на ПК с использованием частично-поисковых методов обучения. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 2. Понятие о блочном и поточном шифровании. | Лекция с разбором конкретных ситуаций. |
| | | Лабораторная работа 2. Понятие о блочном и поточном шифровании. | Лабораторная работа на ПК с использованием частично-поисковых методов обучения. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 3. Теоретико-числовые основы криптографии и их применение. | Лекция с разбором конкретных ситуаций. |
| | | Лабораторная работа 3. Теоретико-числовые основы криптографии и их применение. | Лабораторная работа на ПК с использованием частично-поисковых методов обучения. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 4. Некоторые двухключевые асимметричные криптосистемы и их использование в режиме шифрования. | Лекция с разбором конкретных ситуаций. |
| | | Лабораторная работа 4. Некоторые двухключевые асимметричные криптосистемы и их использование в режиме шифрования. | Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией. Выступления студентов с докладами и презентациями. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 5. Использование известных двухключевых асимметричных криптосистем в режиме электронной | Лекция с использованием частично-поисковых методов обучения. |

| | | | |
|---|---|---|---|
| | | цифровой подписи.<br><br>Лабораторная работа 5. Использование известных двухключевых асимметричных криптосистем в режиме электронной цифровой подписи.<br><br>Самостоятельная работа.<br><br>Лекция 6. Отечественный Стандарт шифрования данных.<br><br>Лабораторная работа 6. Отечественный Стандарт шифрования данных.<br><br>Самостоятельная работа.<br><br>Лекция 7. Некоторые современные подходы к шифрованию информации.<br><br>Лабораторная работа 7. Некоторые современные подходы к шифрованию информации.<br><br>Самостоятельная работа.<br><br>Лекция 8. Идентификация и аутентификация и управление ключами.<br><br>Лабораторная работа 8. Идентификация и аутентификация и управление ключами.<br>Самостоятельная работа.<br><br>Лекция 9. Основные разновидности атак на шифры – криптоанализа.<br><br>Лабораторная работа 9. Основные разновидности атак на шифры – криптоанализа.<br><br>Самостоятельная работа.<br><br>Лекция 10. Древнекитайская теорема об остатках и схема разделения секрета на её основе. | Лабораторная работа на ПК с использованием частично-поисковых методов обучения.<br>Выступления студентов с докладами и презентациями.<br><br>Консультирование посредством электронной почты.<br><br>Теоретическая справка с кратким изложением основных понятий.<br><br>Лабораторная работа на ПК с использованием частично-поисковых методов обучения.<br><br>Консультирование посредством электронной почты.<br><br>Лекция с использованием частично-поисковых методов обучения.<br><br>Лабораторная работа на ПК с использованием частично-поисковых методов обучения.<br>Выступления студентов с докладами и презентациями.<br><br>Консультирование посредством электронной почты.<br><br>Лекция с разбором конкретных ситуаций.<br><br>Лабораторная работа на ПК с использованием частично-поисковых методов обучения.<br>Выступления студентов с докладами и презентациями.<br><br>Теоретическая справка с кратким изложением основных понятий.<br><br>Лабораторная работа на ПК с использованием частично-поисковых методов обучения.<br><br>Консультирование посредством электронной почты.<br><br>Теоретическая справка с кратким изложением основных понятий.<br><br>Лабораторная работа на ПК с |

| | | | |
|---|---|---|---|
| | | Лабораторная работа 10. Древнекитайская теорема об остатках и схема разделения секрета на её основе. | использованием частично-поисковых методов обучения и с разбором конкретных ситуаций. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 11. Расчётные соотношения для контролируемой и неконтролируемой преград комплексной системы защиты информации. | Теоретическая справка с кратким изложением основных понятий. |
| | | Лабораторная работа 11. Расчётные соотношения для контролируемой и неконтролируемой преград комплексной системы защиты информации. | Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| **2** | **Возможности дискретной оптимизации при криптографической защите и обработке информации в социотехнических системах** | Лекция 12. Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа. | Теоретическая справка с кратким изложением основных понятий. |
| | | Лабораторная работа 12. Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа. | Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 13. Защита “ноу-хау” пороговыми схемами разделения секрета и оптимальность борьбы за рынки между двумя фирмами с учётом и без учёта страхования. | Теоретическая справка с кратким изложением основных понятий. |
| | | Лабораторная работа 13. Защита “ноу-хау” пороговыми схемами разделения секрета и оптимальность борьбы за рынки между двумя фирмами с учётом и без учёта страхования. | Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| **3** | **Модели безопасности и контроля целостности информации и основные подходы к анализу защищённости криптографических протоколов** | Лекция 14. Модель безопасности информационных потоков и другие модели безопасности. | Теоретическая справка с кратким изложением основных понятий. |
| | | Лабораторная работа 14. Модель безопасности информационных потоков и другие модели безопасности. | Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |

| | | | |
|---|---|---|---|
| | | Лекция 15. Модели контроля целостности информации и контроль доступа, базирующийся на ролях. | Теоретическая справка с кратким изложением основных понятий. |
| | | Лабораторная работа 15. Модели контроля целостности информации и контроль доступа, базирующийся на ролях. | Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |
| | | Лекция 16. Основные подходы к анализу защищённости криптографических протоколов. | Теоретическая справка с кратким изложением основных понятий. |
| | | Лабораторная работа 16. Основные подходы к анализу защищённости криптографических протоколов. | Лабораторная работа на ПК с использованием частично-поисковых методов обучения. Дискуссия. |
| | | Самостоятельная работа. | Консультирование посредством электронной почты. |

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

## 5. Оценка планируемых результатов обучения

### 5.1 Система оценивания

| **Форма контроля** | **Макс. количество баллов** | |
|---|---|---|
| | **За одну работу** | **Всего** |
| *Текущий контроль:* | | |
| - тесты №№ 1,2 | 11 баллов | 22 балла |
| - аудиторная (домашняя) контрольная (самостоятельная) работа | 21 балл | 21 балл |
| - посещаемость теоретических и лабораторных занятий | 3 балла (за каждую половину семестра) | 6 баллов |
| - устный опрос | 3 балла (за каждую половину семестра) | 6 баллов |
| - занятие призовых мест на олимпиадах и конкурсах, наличие публикаций (тезисов конференций, статей, в том числе, в соавторстве) по математическому либо смежному профилю | 5 баллов | 5 баллов |
| Промежуточная аттестация - зачёт с оценкой | | 40 баллов |

| | | |
|---|---|---|
| (зачёт по билетам) | | |
| **Итого за семестр** | | 100 баллов |

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

| 100-балльная шкала | Традиционная шкала | | Шкала ECTS |
|---|---|---|---|
| 95 – 100 | отлично | зачтено | A |
| 83 – 94 | | | B |
| 68 – 82 | хорошо | | C |
| 56 – 67 | удовлетворительно | | D |
| 50 – 55 | | | E |
| 20 – 49 | неудовлетворительно | не зачтено | FX |
| 0 – 19 | | | F |

### 5.2 Критерии выставления оценки по дисциплине

| **Баллы/ Шкала ECTS** | **Оценка по дисциплине** | **Критерии оценки результатов обучения по дисциплине** |
|---|---|---|
| 100-83/ A,B | отлично/ зачтено | Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.<br>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.<br>Свободно ориентируется в учебной и профессиональной литературе.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий». |
| 82-68/ C | хорошо/ зачтено | Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.<br>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.<br>Достаточно хорошо ориентируется в учебной и профессиональной литературе.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший». |
| 67-50/ D,E | удовлетво-рительно/ зачтено | Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.<br>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.<br>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный». |

| Баллы/ Шкала ECTS | Оценка по дисциплине | Критерии оценки результатов обучения по дисциплине |
|---|---|---|
| 49-0/ F,FX | неудовлет-ворительно/ не зачтено | Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.<br>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.<br>Демонстрирует фрагментарные знания учебной литературы по дисциплине.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы. |

### 5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

**Текущий контроль**

**Тест №0 1** (примерный вариант)

1. Существует ли понятие “тени” защищаемого схемой разделения секрета ключа:
A) да;
B) нет;
C) постановка вопроса некорректна;
D) существует синоним это понятия?
2. Равнозначными (синонимами) являются следующие понятия:
A) симметричное шифрование и шифрование с открытым ключом;
B) несимметричное шифрование и асимметричное шифрование;
C) двухключевое шифрование с открытым ключом и асимметричное шифрование;
D) несимметричное шифрование и шифрование с секретным ключом.
3. Возможны схемы разделения секрета:
A) основанные только на древнекитайской теореме об остатках, ибо другие так и не созданы;
B) основанные на любых теоремах;
C) геометрической природы;
D) с количеством участников как менее 10, так и более 10.
4. Всегда ли в схемах разделения секрета у каждого из участников одинаковые доли секрета:
A) да;
B) нет;
C) зависит только от значения числового ключа;
D) постановка вопроса некорректна?
5. В используемых в основанной на древнекитайской теореме об остатках схеме разделения секрета выражениях $(N_1 \cdot M_1)(\mathrm{mod}\, m_1) \equiv 1$ и $(N_2 \cdot M_2)(\mathrm{mod}\, m_2) \equiv 1$ числа $N_1$ и $N_2$:
A) могут совпасть;
B) не могут и не должны совпадать;
C) обычно никак не используются;
D) всегда одинаковы.
6. При совместном восстановлении ключа:
A) всем участникам схемы разделения секрета необходимо собраться в одном помещении;
B) всем участникам схемы разделения секрета необходимо собраться в одном здании;
C) части участников схемы разделения секрета необходимо собраться в одном помещении;

D) ничего из перечисленного.
7. Шифрование с помощью таблиц Трисемуса является:
A) монограммным; B) биграммным; C) зависит только от размеров таблицы;
D) ничего из перечисленного.
8. В аналитическом (матричном) методе шифрования:
A) один ключ; B) несколько ключей, каждый из которых – элемент матрицы-ключа;
C) нет ни одного ключа;
D) два ключа.
9. Центр распределения ключей:
A) всегда нежелательно использовать при разделении секрета;
B) никогда не используют при разделении секрета;
C) используют исключительно тогда, когда разделение секрета происходит на основе древнекитайской теоремы об остатках; D) ничего из перечисленного.
10. В шифре "двойной квадрат" Уитстона обе таблицы:
A) могут быть только прямоугольными;
B) могут быть только квадратными;
C) могут иметь различающееся между 1-й и 2-й таблицами количество строк;
D) ничего из перечисленного.

**Тест №2** (примерный вариант)

1. Классом вычетов по модулю m для данного модуля:
A) являются все целые числа, сравнимые по mod m;
B) являются не все целые числа, сравнимые по mod m;
C) является лишь меньшая часть целых чисел, сравнимых по mod m;
D) ничего из перечисленного.
2. Верно следующее:
A) числа p и q взаимно просты тогда и только тогда, когда выполнено соотношение up+vq=1 для некоторых целых чисел u, v;
B) числа p и q взаимно просты тогда и только тогда, когда выполнено соотношение up+vq=1 для всех целых чисел u, v;
C) требуется дополнительное исследование;
D) всё вышесказанное имеет отношение только к простым, а не к взаимно простым, числам.
3. В пороговых схемах разделения секрета:
A) обязательно все участники должны объединить свои усилия для совместного получения доступа к объекту защиты;
B) обязательно большинство участников должны объединить свои усилия для совместного получения доступа к объекту защиты;
C) обязательно меньшинство участников должны объединить свои усилия для совместного получения доступа к объекту защиты;
D) ничего из перечисленного.
4. Древнекитайскую теорему об остатках:
A) нельзя использовать в схеме разделения секрета, если количество участников более 2-х;
B) можно использовать в схеме разделения секрета, если количество участников более 2-х;
C) можно использовать исключительно для разделения секрета; D) ничего из перечисленного.
5. Допустимо ли для краткости, когда вместо указания всего класса вычетов приводится только один его представитель:
A) да; B) нет; C) требуется дополнительное исследование;
D) постановка вопроса некорректна?
6. Метод шифрования маршрутами Гамильтона:
A) характеризуется тем, что в нём длина каждого блока обязательно равна 4;
B) не относится к методам шифрования перестановкой;
C) характеризуется тем, что в нём используется неорграф-таблица и два либо более орграфа;

D) характеризуется тем, что в нём в любом случае бессмысленно использовать неорграф-таблицу, а применяются только орграфы.
7. Верно ли, что два целых числа n и k являются сравнимыми по модулю m, если разность n-k делится на m:
A) да; B) нет; C) для ответа на этот вопрос требуется дополнительное исследование;
D) нет, поскольку правильно так – два целых числа n и k называются сравнимыми по модулю m, если сумма n+k делится на m?
8. Если при рассмотрении модуля m=3 имеется три класса сравнимых по этому чисел, а именно – 1) все целые числа, делящиеся на 3 {…,-6, -3, 0, 3, 6, …}; 2) все целые числа, дающие при делении на 3 остаток 1 {…, -5, -2, 1, 4, 7,…}; 3) все целые числа, дающие при делении на 3 остаток 2 {…, -4, -1, 2, 5, 8, …}, то эти классы: A) пересекаются: B) не пересекаются:
C) постановка вопроса некорректна;
D) для ответа на этот вопрос нужно знать ещё один, четвёртый класс чисел.
9. Сравнения, как и обычные целые числа:
A) можно только складывать; B) можно только умножать; C) можно складывать и умножать;
D) ничего из перечисленного, поскольку постановка вопроса некорректна.
10. Корректна ли запись $m_1 m_2 \equiv m \equiv 0 (\mathrm{mod}\, m)$:
A) да; B) нет; C) да, только если бы в ней отсутствовал 0;
D) да, только если бы в ней вместо 0 была 1?

***Вариант аудиторной (домашней) контрольной (самостоятельной) работы***
(вариант выбирается по последней цифре студенческого билета – зачётной книжки)

Вариант 0

1. Найти наибольший общий делитель НОД ($a$, $b$), применяя алгоритм Евклида.

| Вариант | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 21 | 144 | 136 | 1938 | 481 | 11781 | 217 | 1176 | 2277 | 3751 |
| $b$ | 13 | 89 | 51 | 1394 | 325 | 3619 | 413 | 4214 | 924 | 1024 |

2. Используя схему разделения секрета, основанную на (древне)китайской теореме об остатках, защитить общий для двух компаньонов ключ $K$. (При отыскании $N$ из выражений вида $(N \cdot M) (\mathrm{mod}\, m) = 1$ рекомендуется применить любые два из трёх изучавшихся способов – поочерёдная проверка значений, вычисление на основе функции Эйлера (с использованием алгоритма (способа) быстрого возведения в степень) при использовании алгоритма быстрого возведения в степень, расширенный алгоритм Евклида).

| Вариант | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| Ключ $K$ | 20 | 21 | 22 | 23 | 24 | 25 | 16 | 17 | 18 | 19 |

3. Применяя расширенный алгоритм Евклида, найти обратный элемент $a^{-1}$ по модулю $m$ (при условии его существования) и проверить, что найденные числа $u$, $v$ удовлетворяют равенству $au + mv = 1$.

| Вариант | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 19 | 4 | 10 | 10 | 9 | 31 | 181 | 10 | 17 | 35 |
| $m$ | 93 | 7 | 13 | 7 | 11 | 73 | 19 | 11 | 13 | 82 |

4. **Теоретический вопрос.** Классификация ошибок операторов сложных социотехнических систем.

**Промежуточная аттестация**

***Примерный перечень контрольных вопросов к зачёту с оценкой:***

1. Понятие ключа шифрования, принцип (правило) Кёркхоффа и его применение к одноключевым криптосистемам.
2. Алгоритм Евклида и его применение.
3. Обратимость как важное свойство, используемое в криптографии. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение.
4. Основы одноключевых криптосистем.
5. Шифр Трисемуса и шифр Гронсфельда, примеры.
6. Шифр Гронсфельда и алгоритм RSA.
7. Шифр "двойной квадрат" Уитстона и шифр Гронсфельда, примеры.
8. Шифр Вижинера и шифр Гронсфельда.
9. Матричный (аналитический) метод шифрования-дешифрования.
10. Асимметричные криптосистемы.
11. Криптосистема (алгоритм) RSA.
12. Функция Эйлера и её применение в криптосистеме (алгоритме) RSA.
13. Задача факторизации и криптосистема (алгоритм) RSA.
14. (Древне)китайская теорема об остатках и возможности её использования в целях защиты информации.
15. Операция mod и её использование в криптографии.
16. Вычисление обратных величин.
17. Отличие между криптосистемой и схемой разделения секрета, примеры.
18. Односторонняя функция, заложенная в основу криптосистемы RSA.
19. Схема разделения секрета на основе (древне)китайской теоремы об остатках.
20. Возможности представления компьютерных программ графами: управляющий и информационный графы программы, примеры.
21. Возможности представления компьютерных программ графами: области отладки программы и их сравнительная характеристика.
22. Понятия кольца, вычета, поля Галуа.
23. Модель “Китайской стены” (Брюэра и Нэша).
24. Шифрование маршрутами Гамильтона.
25. Решение систем сравнений.
26. Прочность защитной преграды. Основные расчётные соотношения для однозвенной защиты (при атаках одним злоумышленником и организованной группой злоумышленников). Понятие о многоуровневой защите и понятие многозвенной защиты.
27. Некоторые вопросы классификации систем и их закономерности. Компоненты и подсистемы. Надсистемы.
28. Система и среда. Связи. Разделение алгоритма процесса на подсистемы.
29. Классификация ошибок операторов сложных социотехнических систем.

***Демонстрационный вариант билета для зачёта с оценкой***

Российский Государственный Гуманитарный университет
Направление подготовки – 01.04.04 Прикладная математика
Профиль – Математические методы и модели обработки и защиты информации в социотехнических системах
Дисциплина “Криптография в социотехнических системах”

**Билет** для зачёта (с оценкой) **№0**

1. Равнозначными (синонимами) являются следующие понятия:
A) симметричное шифрование и шифрование с открытым ключом;
B) несимметричное шифрование и асимметричное шифрование;
C) двухключевое шифрование с открытым ключом и асимметричное шифрование;
D) несимметричное шифрование и шифрование с секретным ключом. (до 4 баллов)
2. В общем случае криптоалгоритм RSA:
A) работает быстрее одноключевых криптоалгоритмов;
B) работает медленнее одноключевых криптоалгоритмов;
C) работает с той же скоростью, что и одноключевые криптоалгоритмы;
D) ничего из перечисленного. (до 4 баллов)
3. Верно ли, что два целых числа n и k являются сравнимыми по модулю m, если разность n-k делится на m?
A) да;
B) нет;
C) для ответа на этот вопрос требуется дополнительное исследование;
D) нет, поскольку правильно так – два целых числа n и k называются сравнимыми по модулю m, если сумма n+k делится на m. (до 4 баллов)
4. Если при рассмотрении модуля m=3 имеется три класса сравнимых по этому чисел, а именно
1) все целые числа, делящиеся на 3 {…,-6, -3, 0, 3, 6, …};
2) все целые числа, дающие при делении на 3 остаток 1 {…, -5, -2, 1, 4, 7,…};
3) все целые числа, дающие при делении на 3 остаток 2 {…, -4, -1, 2, 5, 8, …}, то эти классы:
A) пересекаются:
B) не пересекаются:
C) постановка вопроса некорректна;
D) для ответа на этот вопрос нужно знать ещё один, четвёртый класс чисел. (до 4 баллов)

5. Понятие ключа шифрования, принцип (правило) Кёркхоффа (Кирхгофса) и его применение к одноключевым криптосистемам. (до 5 баллов)
6. Расширенный алгоритм Евклида и его применение. (до 5 баллов)

7. Используя схему разделения секрета, основанную на (древне)китайской теореме об остатках, защитить общий для двух компаньонов ключ *K=19*. (При отыскании *N* из выражений вида $(N \cdot M) \pmod{m} = 1$ рекомендуется применить любые два из трёх изучавшихся способов – поочерёдная проверка значений, вычисление на основе функции Эйлера при использовании алгоритма быстрого возведения в степень, расширенный алгоритм Евклида). (до 7 баллов)
8. Применяя алгоритм RSA, зашифровать и расшифровать сообщение ИМЯ при заданном *p* либо *q*: 13. (до 7 баллов)

*Примечание (к билету).* В билете для зачёта могут встречаться любые вопросы, тестовые задания и практические задачи, имевшие место в период текущей аттестации.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Список источников и литературы

Литература
*Основная*
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 .

2. Применко Э.А. Алгебраические основы криптографии : учебное пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информ. технологии" / Э. А. Применко. - Москва : URSS : Либроком, 2013. - 283 с. ; 22 см. - (Основы защиты информации). - Библиогр.: с. 282-283. - ISBN 978-5-397-03871-3
3. Рябко, Б. Я. Криптографические методы защиты информации: Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - 2-е изд., стереотип. - Москва : Гор. линия-Телеком, 2012. - 229 с.: ил.; . - (Специальность). ISBN 978-5-9912-0286-2, 500 экз. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/370317 (дата обращения: 24.08.2019).

*Дополнительная*

1. Коблиц Нил. Курс теории чисел и криптографии / Н. Коблиц ; [пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова]. - М. : ТВП, 2001. - X, 260 с.
2. Нечаев В. И. Элементы криптографии : Основы теории защиты информации: Учеб. пособие для ун-тов и пед. вузов. - М. : Высш. шк., 1999. - 108 с.

### 6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Журнал “Прикладная дискретная математика”:
http://journals.tsu.ru/pdm/&journal_page=archive;
2. Журнал “Математические вопросы криптографии”:
http://www.mathnet.ru/php/archive.phtml?jrnid=mvk&wshow=contents&option_lang=rus

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

### 6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

## 7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимы:

*- для лекций:*
- учебная аудитория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук,
- программное обеспечение (ПО).

*- для лабораторных занятий:*

- лаборатория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук для преподавателя,
- компьютеры для обучающихся,
- программное обеспечение (ПО).

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

## 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

## 9. Методические материалы

### 9.1 Планы практических занятий

***Тема 1. Некоторые традиционные одноключевые криптосистемы***

Цель занятия: приобретение практических навыков использования и анализа некоторых традиционных одноключевых криптосистем

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Обобщённая модель симметричной криптосистемы и её реализация средствами MS Excel.

2) Модель нарушителя информационной системы и её реализация средствами MS Excel.

3) Принцип (правило) Кёркхоффа и его реализация средствами MS Excel.

4) Шифры простой замены, шифрующие таблицы Трисемуса и их реализация средствами MS Excel.

5) Шифры сложной замены; шифр Гронсфельда, система шифрования Вижинера и их реализация средствами MS Excel.

6) Шифр “двойной квадрат” Уитстона и его реализация средствами MS Excel.

7) Шифрование перестановкой; использование маршрутов Гамильтона и их реализация средствами MS Excel.

***Тема 2. Понятие о блочном и поточном шифровании***

Цель занятия: приобретение навыков анализа практической применимости блочного и поточного шифрования

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Понятия блочного и поточного шифрования и их основные особенности, реализация средствами MS Excel.

2) Шифрование методом гаммирования и его реализация средствами MS Excel.

3) Возможности использования сдвиговых регистров для генерации псевдослучайных последовательностей. Абонентское шифрование. Их реализация средствами MS Excel.

***Тема 3. Теоретико-числовые основы криптографии и их применение***

Цель занятия: приобретение и закрепление теоретико-практических навыков по основам криптографии

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Обратимость как важное свойство, используемое в криптографии, реализация средствами MS Excel.

2) Алгоритм Евклида для отыскания наибольшего общего делителя и его реализация средствами MS Excel.

3) Вычисление обратных величин. Расширенный алгоритм Евклида и его применение. Конечные поля. Поле Галуа. Вычеты, кольца вычетов. Их реализация средствами MS Excel.

4) Решение сравнений и систем сравнений. Функция Эйлера, теорема Эйлера. Понятие дискретного логарифма. Их реализация средствами MS Excel.

5) Основы двухключевых криптосистем. Обобщённая модель асимметричной криптосистемы. Реализация средствами MS Excel.

***Тема 4. Некоторые двухключевые асимметричные криптосистемы и их использование в режиме шифрования***

Цель занятия: приобретение навыков практического использования двухключевых асимметричных криптосистем в режиме шифрования

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Криптосистема RSA и её использование в режиме шифрования, реализация средствами MS Excel.

2) Криптосистема Эль-Гамаля и её использование в режиме шифрования. Реализация средствами MS Excel.

3) Понятия односторонней (однонаправленной) функции и односторонней (однонаправленной) функции с потайным ходом (лазейкой). Реализация средствами MS Excel.

4) Атака на криптосистему RSA методом факторизации. Реализация средствами MS Excel.

***Тема 5. Использование известных двухключевых асимметричных криптосистем в режиме электронной цифровой подписи***

Цель занятия: приобретение навыков практического использования двухключевых асимметричных криптосистем в режиме цифровой подписи

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Понятия односторонней (однонаправленной) хеш-функции и электронной цифровой подписи и основные требования к ним. Реализация средствами MS Excel.

2) Использование криптосистемы RSA в режиме электронной цифровой подписи и её реализация средствами MS Excel.

***Тема 6. Отечественный Стандарт шифрования данных***

Цель занятия: приобретение практических навыков использования Отечественного Стандарта шифрования данных

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Отечественный Стандарт шифрования данных и его реализация средствами MS Excel.

2) Режимы: простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки. Реализация средствами MS Excel.

***Тема 7. Некоторые современные подходы к шифрованию информации***

Цель занятия: приобретение практических навыков в применении современных подходов к шифрованию информации

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Возможности шифрования на основе метода укладки рюкзака (упаковки ранца). Реализация средствами MS Excel.

2) Криптосхема с перестановкой фиксированных процедур. Реализация средствами MS Excel.

3) Шифры на основе процедур и операций преобразования, зависящих от преобразуемых данных. Реализация средствами MS Excel.

4) Шифры: с управляемыми операциями, на основе управляемых перестановок, с управляемыми подстановками, на основе модифицирования подключей. Реализация средствами MS Excel.

5) Многоуровневая криптография. Шарады с временны*ы*м замком, их построение и решение. Реализация средствами MS Excel.

***Тема 8. Идентификация и аутентификация и управление ключами***

Цель занятия: приобретение практических навыков при анализе и построении систем идентификации и аутентификации и управлении ключами

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Реализация средствами MS Excel.

2) Генерация и хранение ключей. Распределение ключей с участием центра. Реализация средствами MS Excel.

3) Распределения ключей и прямой обмен ключами между пользователями. Криптографические методы аутентификации для симметичной и несимметричной криптосистем: в режиме on-line, при участии нескольких серверов, в режиме off-line, с привлечением арбитра. Реализация средствами MS Excel.

***Тема 9. Основные разновидности атак на шифры – криптоанализа***

Цель занятия: получение основных представлений и “азов” криптоанализа.

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Дифференциальный криптоанализ и его реализация средствами MS Excel.

2) Дифференциальный криптоанализ на основе отказов устройства и его реализация средствами MS Excel.

3) Линейный криптоанализ. Некоторые другие виды криптоанализа и атак. Реализация средствами MS Excel.

***Тема 10. Древнекитайская теорема об остатках и схема разделения секрета на её основе***

Цель занятия: приобретение практических навыков в использовании древнекитайской теоремы об остатках и схем разделения секрета

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения с разбором конкретных ситуаций.

Вопросы для обсуждения и реализации на ПК:

1) Древнекитайская теорема об остатках и её применение. Реализация средствами MS Excel.

2) Понятия схемы разделения секрета и совершенной схемы разделения секрета. Применение теоремы об остатках для безопасного сохранения (защищённого разделения) ключа между двумя компаньонами в случае цифрового замка сейфа. Реализация средствами MS Excel.

***Тема 11. Расчётные соотношения для контролируемой и неконтролируемой преград комплексной системы защиты информации***

Цель занятия: приобретение навыков расчёта и анализа прочности защиты контролируемой и неконтролируемой преград комплексной системы защиты информации

Форма проведения – Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией.

Вопросы для обсуждения и реализации на ПК:

1) Расчётные соотношения для контролируемой и неконтролируемой преград комплексной системы защиты информации в случаях однозвенной (элементарной) и многозвенной защиты. Их реализация средствами MS Excel.

2) Защита штатного входа в систему и прочность защитной преграды. Реализация расчётных соотношений средствами MS Excel.

3) Случай многоуровневой защиты. Реализация расчётных соотношений средствами MS Excel.

***Тема 12. Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа***

Цель занятия: анализ практических возможностей задачи о назначениях

Форма проведения – Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией.

Вопросы для обсуждения и реализации на ПК:

1) Задача об управлении кадрами подразделений как задача о назначениях. Реализация средствами MS Excel.

2) Венгерский метод решения задачи о назначениях. Реализация средствами MS Excel.

3) Технические приложения задачи о назначениях: распределение задач шифрования по компьютерам сети, оптимизация наборов прав пользователей при матричном принципе управления доступом. Реализация расчётных соотношений средствами MS Excel.

4) Возможности разбиения на классы для объектов и субъектов доступа. Роль бинарных отношений в попарном сравнении вариантов и выражении предпочтений экспертов по защите информации. Реализация средствами MS Excel.

***Тема 13. Защита "ноу-хау" пороговыми схемами разделения секрета и оптимальность борьбы за рынки между двумя фирмами с учётом и без учёта страхования***

Цель занятия: приобретение теоретико-практических навыков защиты "ноу-хау" пороговыми схемами разделения секрета и оптимальность борьбы за рынки между двумя фирмами с учётом и без учёта страхования и анализа такой защиты

Форма проведения – Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией.

Вопросы для обсуждения и реализации на ПК:

1) Особенности пороговых схем разделения секрета и возможности недобросовестной конкуренции между двумя фирмами. Реализация расчётных соотношений средствами MS Excel.

2) Игра на единичном квадрате и оптимальность борьбы за рынки при защищаемом пороговыми схемами разделения секрета "ноу-хау" с учётом и без учёта страхования. Реализация расчётных соотношений средствами MS Excel.

3) Инженерно-технические и информационные риски, возможности их страхования и страхование ответственности. Реализация расчётных соотношений средствами MS Excel.

***Тема 14. Модель безопасности информационных потоков и другие модели безопасности***

Цель занятия: получение основных теоретико-практических представлений о модели безопасности информационных потоков и других моделях безопасности

Форма проведения – Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией.

Вопросы для обсуждения и реализации на ПК:

1) Модель безопасности информационных потоков при использовании мандатного принципа управления доступом. Реализация расчётных соотношений средствами MS Excel.

2) Модель Low-Water-Mark. Реализация средствами MS Excel.

3) Модель "Китайской стены". Реализация средствами MS Excel.

***Тема 15. Модели контроля целостности информации и контроль доступа, базирующийся на ролях***

Цель занятия: получение основных теоретико-практических представлений о модели контроля целостности информации и контроль доступа, базирующийся на ролях

Форма проведения – Самостоятельное моделирование задач на ПК с последующим их обсуждением и оптимизацией.

Вопросы для обсуждения и реализации на ПК:

1) Модель Биба. Реализация средствами MS Excel.

2) Модель Кларка-Вилсона. Реализация расчётных соотношений средствами MS Excel.

3) Контроль доступа, базирующийся на ролях и его актуальность для вычислительной системы организации. Реализация средствами MS Excel.

***Тема 16. Основные подходы к анализу защищённости криптографических протоколов***

Цель занятия: приобретение навыков и практических подходов к анализу защищённости криптографических протоколов

Форма проведения – Лабораторная работа на ПК с использованием частично-поисковых методов обучения.

Вопросы для обсуждения и реализации на ПК:

1) Четыре основных подхода к анализу защищённости криптографических протоколов. Моделирование и проверка работы протокола с использованием языков описания и средств проверки, не разработанных специально для анализа криптографических протоколов. Реализация средствами MS Excel.

2) Создание экспертных систем, позволяющих разработчику протокола исследовать различные сценарии. Реализация основных расчётных и иных соотношений средствами MS Excel.

3) Выработка требований к семейству протоколов с использованием некой логики для анализа понятий “знание” и “доверие” (BAN-логика). Реализация средствами MS Excel.

4) Выработка формальных методов, основанных на записи свойств криптосистем в алгебраическом виде. Реализация расчётных соотношений средствами MS Excel.

9.2. Методические рекомендации по подготовке письменных работ

Рекомендуется выполнять письменные работы на листах А-4 от руки либо на компьютере (набор формул на компьютере не обязателен, но писать весь текст следует разборчивым почерком). Оформляется титульный лист, выполненная работа с титульным листом вкладывается в файл и в назначенный день сдается на проверку преподавателю.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Студентам следует:

- руководствоваться графиком самостоятельной работы, определенным РПД;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на практических занятиях и консультациях неясные вопросы;
- при подготовке к зачёту параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на плановой консультации.

*Методические рекомендации по подготовке научного доклада.* Одной из форм самостоятельной работы студента является подготовка научного доклада, для обсуждения его на практическом занятии.

Цель научного доклада – развитие у студентов навыков аналитической работы с научной литературой, анализа дискуссионных научных позиций, аргументации собственных взглядов. Подготовка научных докладов также развивает творческий потенциал студентов.

Научный доклад готовится под руководством преподавателя, который ведет практические занятия.

Рекомендации студенту:

- перед началом работы по написанию научного доклада согласовать с преподавателем тему, структуру, литературу, а также обсудить ключевые вопросы, которые следует раскрыть в докладе;

- представить доклад научному руководителю в письменной форме;

- выступить на практическом занятии с 10-минутной презентацией своего научного доклада, ответить на вопросы студентов группы.

Требования:

- к оформлению научного доклада: шрифт – Times New Roman, размер шрифта – 14, межстрочный интервал 1,5, размер полей – 2,5 см, отступ в начале абзаца – 1,25 см, форматирование по ширине); листы скреплены скоросшивателем. На титульном листе указывается наименование учебного заведения, название кафедры, наименование дисциплины, тема доклада, ФИО студента;

- к структуре доклада – оглавление, введение (указывается актуальность, цель и задачи), основная часть, выводы автора, список литературы (не менее 5 позиций). Объем согласовывается с преподавателем. В конце работы ставится дата ее выполнения и подпись студента, выполнившего работу.

Общая оценка за доклад учитывает содержание доклада, его презентацию, а также ответы на вопросы преподавателя и других слушателей.

### 9.2 Методические рекомендации по изучению дисциплины

Студентам необходимо прежде всего ознакомиться с содержанием рабочей программы дисциплины (далее – РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимися на образовательном портале и сайте кафедры, с графиком консультаций преподавателей данной кафедры.

- *“Сценарий” изучения дисциплины* студентом подразумевает выполнение им следующих действий:

1. Ознакомление с целями и задачами дисциплины.
2. Ознакомление с требованиями к знаниям и навыкам студента.
3. Первичное ознакомление с разделами и темами дисциплины.
4. Ознакомление с распределением времени на изучение дисциплины.
5. Ознакомление со списками рекомендуемой основной и дополнительной литературы по дисциплине.
6. Углублённое ознакомление с разделами и темами дисциплины.
7. Предварительный охват на основе рекомендуемой литературы круга вопросов, актуальных для конкретного занятия.
8. Самостоятельная проработка основного круга вопросов как каждого последующего, так и каждого предыдущего занятия в свободное время между занятиями по дисциплине.
9. Присутствие и творческое участие на лекционных и практических занятиях.
10. Выполнение требований текущего и итогового контроля.
11. Уточнение возникающих вопросов на консультации по дисциплине.
12. Непосредственная подготовка к зачёту по дисциплине.

*Рекомендации по работе с литературой.* Целесообразно пользоваться литературой, изданной не более 7 лет назад, предшествовавших году начала изучения курса. В вопросах дискретной математики, непосредственно касающихся программной реализации решаемых в курсе задач на ЭВМ, используемая литература должна быть по возможности ещё более новой – как правило, 5–6 летней давности издания.

*Рекомендации по подготовке к занятиям.* Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных

тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры.

Студентам необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;

- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;

- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам, если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях. Не следует оставлять «белых пятен» в освоении материала.

Студентам также следует:

- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал соответствующей темы занятия;

- при подготовке к практическим занятиям следует обязательно использовать не только лекции, но и учебную литературу,

- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

- в ходе практического занятия давать конкретные, четкие ответы по существу вопросов;

- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

*Методические рекомендации по работе с литературой.* Любая форма самостоятельной работы студента (подготовка к практическому занятию, написание эссе, курсовой работы, доклада и т.п.) начинается с изучения соответствующей литературы как в библиотеке, так и дома.

Рекомендации студенту:

- выбранную монографию или статью целесообразно внимательно просмотреть. В книгах следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие – прочитать быстро;

- в книге или журнале, принадлежащие самому студенту, ключевые позиции можно выделять маркером или делать пометки на полях. При работе с Интернет-источником целесообразно также выделять важную информацию;

- если книга или журнал являются собственностью студента, то целесообразно записывать номера страниц, которые привлекли внимание. Позже следует возвратиться к ним, перечитать или переписать нужную информацию. Физическое действие по записыванию помогает прочно заложить данную информацию в «банк памяти».

Записи в той или иной форме не только способствуют пониманию и усвоению изучаемого материала, но и помогают вырабатывать навыки явного изложения в письменной форме тех или иных теоретических вопросов.

Приложение 1. Аннотация
рабочей программы дисциплины

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Криптография в социотехнических системах» реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.
Цель дисциплины: развитие способностей к логическому и алгоритмическому мышлению; получение студентами знаний в сфере криптографии, по её вопросам системного характера, необходимым для решения теоретико-практических задач социотехнической направленности.
Задачи:

- научиться определять основные требования к криптографической защите информации в их взаимосвязи применительно к социотехническим системам;
- научиться формировать множество целевых ориентиров при криптографической защите информации с учётом структурных особенностей среды;
- научиться определять и учитывать качественные и количественные особенности составляющих криптографической защиты;
- получить навыки оценки эффективности тех или иных криптографических преобразований;
- получить представление о механизмах смены параметров криптографической защиты для социотехнических систем;
- научиться решать основополагающие теоретико-практические задачи социотехнической направленности с применением необходимого математического аппарата.

Дисциплина направлена на формирование следующих компетенций:

- ПК-2. Способен осуществлять поиск, изучение и разработку новых теоретических или практических проблем, сведений, относящихся к решению текущих научных исследований, производственных задач; в информационных средах находить, создавать основные элементы будущих математических структур или конструктивных математических моделей.

В результате освоения дисциплины обучающийся должен:

Знать: понятия, методы и подходы криптографии в социотехнических системах; основные модели, методы и средства криптографии.

Уметь: применять методы и модели криптографии и основ теории информации с необходимыми формулами для решения математических прикладных задач; применять существующие криптографические системы в области социотехнических систем.

Владеть: изложенными подходами к постановке и решению задач, навыками математического описания прикладных задач методами криптографии и основ теории информации;

методами обоснования оптимальности принятых криптографических решений с учётом различных требований регуляторов в этой области;

методами проведения экспериментов в области синтеза и анализа криптографических систем и оценки их результатов.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.