

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«04» июля 2022 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.06.3 Адаптивная Криптографические протоколы

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2022

Авторы программы:

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Кандидат технических наук, Соловьев Денис Сергеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «29» июня 2022 г. Протокол № 12

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «04» июля 2022 г. № 6.

СОДЕРЖАНИЕ

| | |
|---|----|
| 1. Цели и задачи дисциплины..... | 4 |
| 2. Место дисциплины в структуре ОП бакалавра..... | 5 |
| 3. Объем и содержание дисциплины..... | 5 |
| 4. Контроль знаний обучающихся и типовые оценочные средства..... | 9 |
| 5. Методические указания для обучающихся по освоению дисциплины (модуля)..... | 21 |
| 6. Учебно-методическое и информационное обеспечение дисциплины..... | 22 |
| 7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы..... | 23 |

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

| Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта) | Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия | Индикаторы достижения компетенций |
|---|---|--|
| | ПК-1 Способен администрировать подсистемы защиты информации в операционных системах | Администрирует криптографические протоколы в операционных системах |

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах

| № п/п | Наименование дисциплин, определяющих междисциплинарные связи | Форма обучения | | | | |
|-------|---|-----------------|---|---|---|---|
| | | Очная (семестр) | | | | |
| | | 3 | 4 | 5 | 6 | 7 |
| 1 | Безопасные информационные технологии | | | | + | + |
| 2 | Криптографические протоколы | | | | | + |
| 3 | На английском языке Cryptographic protocols | | | | | + |
| 4 | Ознакомительная практика | | | | + | |
| 5 | Основы программирования в корпоративных информационных системах | + | + | + | | |
| 6 | Программно-аппаратные средства защиты информации | | | + | + | |

| | | | | | | |
|---|------------------------|--|--|--|--|---|
| 7 | Электронная подпись | | | | | + |
|---|------------------------|--|--|--|--|---|

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Адаптивная Криптографические протоколы» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Адаптивная Криптографические протоколы» изучается в 7 семестре.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 2 з.е.

Очная: 2 з.е.

| Вид учебной работы | Очная (всего часов) |
|--------------------------------------|------------------------|
| Общая трудоёмкость дисциплины | 72 |
| Контактная работа | 32 |
| Лекции (Лекции) | 16 |
| Лабораторные (Лаб. раб.) | 16 |
| Самостоятельная работа (СР) | 40 |
| Зачет | - |

3.2.Содержание курса:

| № темы | Название раздела/темы | Вид учебной работы, час. | | | Формы текущего контроля |
|-----------|--|-----------------------------|------------------|----|--|
| | | Лек ции | Лаб · раб. | СР | |
| | | О | О | О | |
| 7 семестр | | | | | |
| 1 | Основы информационной безопасности и защиты информации | 2 | 2 | 4 | Вопросы для самоподготовки |
| 2 | История криптографии | 2 | 2 | 6 | Вопросы для самоподготовки |
| 3 | Основные термины и определения. Классификация шифров | 2 | 2 | 6 | Вопросы для самоподготовки; Тестирование |
| 4 | Шифры замены | 2 | 2 | 4 | Вопросы для самоподготовки/Ла бораторная работа |
| 5 | Шифры перестановки | 2 | 2 | 4 | Вопросы для самоподготовки/Ла бораторная работа; Тестирование |
| 6 | Шифры гаммирования | 2 | 2 | 4 | Вопросы для самоподготовки/Ла бораторная работа |

| | | | | | |
|---|------------------------------|---|---|---|--|
| 7 | Шифрование с открытым ключом | 2 | 2 | 6 | Вопросы для самоподготовки/Лабораторная работа; Тестирование |
| 8 | Криптографические протоколы | 2 | 2 | 6 | Вопросы для самоподготовки |

Тема 1. Основы информационной безопасности и защиты информации

Лекция.

Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.

Лабораторные работы.

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
- 1 5. Дайте характеристику средствам защиты информации.

Задания для самостоятельной работы.

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
5. Дайте характеристику средствам защиты информации.

Тема 2. История криптографии

Лекция.

Наивная криптография, формальная криптография, математическая криптография.

Лабораторные работы.

1. Перечислите способы тайной передачи информации на расстоянии.
2. Назовите основные этапы развития криптографии.
3. Назовите основные этапы развития криптоанализа.
4. Современная обстановка в сфере криптоанализа.
5. Надежные средства криптографии.
1. Перечислите способы тайной передачи информации на расстоянии.
2. Назовите основные этапы развития криптографии.
3. Назовите основные этапы развития криптоанализа.
4. Современная обстановка в сфере криптоанализа.
5. Надежные средства криптографии.

Задания для самостоятельной работы.

1. Перечислите способы тайной передачи информации на расстоянии.
2. Назовите основные этапы развития криптографии.

Тема 3. Основные термины и определения. Классификация шифров

Лекция.

Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.

Лабораторные работы.

1. Что является целью криптоанализа?
 - A. Определение стойкости алгоритма
 - B. Увеличение количества функций замещения в криптографическом алгоритме
 - C. Уменьшение количества функций подстановок в криптографическом алгоритме
 - D. Определение использованных перестановок

2. Частота применения брутфорс-атак возросла, поскольку:
 - A. Возросло используемое в алгоритмах количество перестановок и замещений
 - B. Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
 - C. Мощность и скорость работы процессоров возросла
 - D. Длина ключа со временем уменьшилась

3. Что из перечисленного ниже не является свойством или характеристикой односторонней функции хэширования?
 - A. Она преобразует сообщение произвольной длины в значение фиксированной длины
 - B. Имея значение дайджеста сообщения, невозможно получить само сообщение
 - C. Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
 - D. Она преобразует сообщение фиксированной длины в значение переменной длины

4. Что может указывать на изменение сообщения?
 - A. Изменился открытый ключ
 - B. Изменился закрытый ключ
 - C. Изменился дайджест сообщения
 - D. Сообщение было правильно зашифровано

5. Какой из перечисленных ниже алгоритмов является алгоритмом американского правительства, предназначенным для создания безопасных дайджестов сообщений?
 - A. Data Encryption Algorithm
 - B. Digital Signature Standard
 - C. Secure Hash Algorithm
 - D. Data Signature Algorithm

Задания для самостоятельной работы.

1. Дайте определение понятиям «шифр», «ключ», «дешифрование».
2. Перечислите основные требования, предъявляемые к криптосистемам.
3. Дайте классификацию криптосистем по алгоритму шифрования.
4. Дайте классификацию криптосистем по стойкости шифра.

Тема 4. Шифры замены

Лекция.

Основы шифрования. Шифры однозначной замены. Полиграммные шифры. Омофонические шифры. Полеалфавитные шифры. Нерегулярные шифры.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- шифра Цезаря;
- лозунгового шифра;

- полибианского квадрата;
- шифрующей системы Трисемуса;
- шифра Playfair;
- системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
- шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.

Задания для самостоятельной работы.

1. В чем заключается основная идея криптографических преобразований шифров замены?
2. Перечислите основные разновидности шифров замены.
3. Дайте характеристику разновидностям шифров замены.
4. Назовите основной недостаток шифра однозначной замены.

Тема 5. Шифры перестановки

Лекция.

Основы шифрования, шифры одинарной и множественной перестановки.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию (для первых двух шифров) или фамилию и имя (для остальных) с помощью следующих шифров:

- простой одинарной перестановки;
- блочной одинарной перестановки;
- табличной маршрутной перестановки;
- вертикальной перестановки;
- поворотной решетки;
- магический квадрат (размер квадрата - 4x4);
- двойной перестановки.

При оформлении отчета необходимо привести исходное сообщение (фамилию или фамилию и имя), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, повороты решетки и зашифрованное сообщение

Задания для самостоятельной работы.

1. В чем заключается основная идея криптографических преобразований шифров перестановки?
2. Перечислите основные разновидности шифров перестановки.
3. Дайте характеристику разновидностям шифров перестановки.

Тема 6. Шифры гаммирования

Лекция.

Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию с помощью шифров гаммирования по модулю N и модулю 2.

При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы зашифрования/дешифрования.

Задания для самостоятельной работы.

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?
2. Назовите основные характеристики гаммы.
3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.
4. Дайте характеристику программным способам генерации гаммы (алгоритм RANDU и BBS).
5. Что такое паритетный бит?

6. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.

Тема 7. Шифрование с открытым ключом

Лекция.

Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамала, алгоритм на основе эллиптических кривых.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;
- алгоритма на основе задачи об укладке ранца;
- алгоритма шифрования Эль-Гамала.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251.

Задания для самостоятельной работы.

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асимметричном шифровании.
4. Дайте краткую характеристику алгоритма RSA.
5. В чем отличие сверхвозрастающей последовательности от обыкновенной?
6. Что означает обратное число по модулю?
7. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
8. В чем суть задачи дискретного логарифмирования?
9. Приведите уравнение эллиптической кривой в короткой форме Вейерштрасса.

Тема 8. Криптографические протоколы

Лекция.

Основные сведения о криптографических протоколах, протоколы обмена ключами.

Лабораторные работы.

1. Перечислите основные задачи, для решения которых используется криптография.
2. Перечислите основные отличия криптопротоколов от традиционных криптосистем.
3. Дайте определение понятию «протокол».
4. Дайте классификацию криптопротоколов в зависимости от наличия третьей стороны.
5. Перечислите основные криптопротоколы.

Задания для самостоятельной работы.

1. Перечислите основные задачи, для решения которых используется криптография.
2. Перечислите основные отличия криптопротоколов от традиционных криптосистем.
3. Дайте определение понятию «протокол».
4. Дайте классификацию криптопротоколов в зависимости от наличия третьей стороны.
5. Перечислите основные криптопротоколы.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

7 семестр

- посещаемость – 10 баллов

- текущий контроль – 64 балла
- контрольные срезы – 3 среза: 10 баллов, 8 баллов, 8 баллов
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

| № те мы | Название темы / вид учебной работы | Формы текущего контроля / срезы | Мах. кол-во баллов | Методика проведения занятия и оценки |
|---------|--|---------------------------------|--------------------|--|
| 1. | Основы информационной безопасности и защиты информации | Вопросы для самоподготовки | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>8 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>5 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>2 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. |

| | | | | |
|----|--|--------------------------------|----|--|
| 2. | История криптографии | Вопросы для самоподготовки | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>8 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>5 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>2 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. |
| 3. | Основные термины и определения. Классификация шифров | Вопросы для самоподготовки | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>8 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>5 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>2 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. |
| | | Тестирование(контрольный срез) | 10 | <p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> - 90 % - 10 баллов; - 65 % - 5 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется. |

| | | | | |
|----|--------------|--|---|---|
| 4. | Шифры замены | Вопросы для самоподготовки/Лабораторная работа | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>3 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>1 балл ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>0,5 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> 1. Степень соответствия выполненного задания поставленным требованиям; 2. Структурирование и комментирование лабораторной работы; 3. Уникальность выполнение работы (отличие от работ коллег); 4. Успешные ответы на контрольные вопросы. <p>«5 баллов» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«3 балла» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p> |
|----|--------------|--|---|---|

| | | | | |
|----|--------------------|--|---|---|
| 5. | Шифры перестановки | Вопросы для самоподготовки/Лабораторная работа | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>3 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>1 балл ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>0,5 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> 1. Степень соответствия выполненного задания поставленным требованиям; 2. Структурирование и комментирование лабораторной работы; 3. Уникальность выполнения работы (отличие от работ коллег); 4. Успешные ответы на контрольные вопросы. <p>«5 баллов» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«3 балла» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p> |
| | | Тестирование(контрольный срез) | 8 | <p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> - 90 % - 8 баллов; - 65 % - 4 балла; - 30 % - 2 балла; - менее 30 % - балл не начисляется. |

| | | | | |
|----|-----------------------|--|---|---|
| 6. | Шифры гаммирования | Вопросы для самоподг отовки/Ла бораторна я работа | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>3 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>1 балл ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>0,5 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> 1. Степень соответствия выполненного задания поставленным требованиям; 2. Структурирование и комментирование лабораторной работы; 3. Уникальность выполнение работы (отличие от работ коллег); 4. Успешные ответы на контрольные вопросы. <p>«5 баллов» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«3 балла» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p> |
|----|-----------------------|--|---|---|

| | | | | |
|----|------------------------------|--|---|---|
| 7. | Шифрование с открытым ключом | Вопросы для самоподготовки/Лабораторная работа | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>3 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>1 балл ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>0,5 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> 1. Степень соответствия выполненного задания поставленным требованиям; 2. Структурирование и комментирование лабораторной работы; 3. Уникальность выполнения работы (отличие от работ коллег); 4. Успешные ответы на контрольные вопросы. <p>«5 баллов» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«3 балла» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p> |
| | | Тестирование(контрольный срез) | 8 | <p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> - 90 % - 8 баллов; - 65 % - 4 балла; - 30 % - 2 балла; - менее 30 % - балл не начисляется. |

| | | | | |
|-----|-----------------------------|----------------------------|-----|--|
| 8. | Криптографические протоколы | Вопросы для самоподготовки | 8 | <p>Методика оценки самоподготовки студентов.</p> <p>8 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>5 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>2 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена. |
| 9. | Посещаемость | | 10 | <p>10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.</p> |
| 10. | Премияльные баллы | | 20 | <p>Дополнительные премияльные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции</p> |
| 11. | Итого за семестр | | 100 | |

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

| 100-балльная система | Традиционная система |
|----------------------|----------------------|
| 50 - 100 баллов | Зачтено |
| 0 - 49 баллов | Не зачтено |

4.2 Типовые оценочные средства текущего контроля

Вопросы для самоподготовки

Тема 1. Основы информационной безопасности и защиты информации

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
- 1 5. Дайте характеристику средствам защиты информации.

Тема 2. История криптографии

1. Перечислите способы тайной передачи информации на расстоянии.
2. Назовите основные этапы развития криптографии.
3. Назовите основные этапы развития криптоанализа.
4. Современная обстановка в сфере криптоанализа.
5. Надежные средства криптографии.

Тема 3. Основные термины и определения. Классификация шифров

1. Дайте определение понятиям «шифр», «ключ», «дешифрование».
2. Перечислите основные требования, предъявляемые к криптосистемам.
3. Дайте классификацию криптосистем по алгоритму шифрования.
4. Дайте классификацию криптосистем по стойкости шифра.

Тема 8. Криптографические протоколы

1. Перечислите основные задачи, для решения которых используется криптография.
2. Перечислите основные отличия криптопротоколов от традиционных криптосистем.
3. Дайте определение понятию «протокол».
4. Дайте классификацию криптопротоколов в зависимости от наличия третьей стороны.
5. Перечислите основные криптопротоколы.

Вопросы для самоподготовки/Лабораторная работа

Тема 4. Шифры замены

1. В чем заключается основная идея криптографических преобразований шифров замены?
2. Перечислите основные разновидности шифров замены.
3. Дайте характеристику разновидностям шифров замены.
4. Назовите основной недостаток шифра однозначной замены.
5. Возможно ли усилить шифр замены?

Тема 5. Шифры перестановки

1. В чем заключается основная идея криптографических преобразований шифров перестановки?
2. Перечислите основные разновидности шифров перестановки.
3. Дайте характеристику разновидностям шифров перестановки.
4. Проведите анализ устойчивости шифра перестановки.
5. Возможно ли усилить шифр перестановки?

Тема 6. Шифры гаммирования

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?
2. Назовите основные характеристики гаммы.

3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.
4. Дайте характеристику программным способам генерации гаммы (алгоритм RANDU и BBS).
5. Что такое паритетный бит?
6. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.

Тема 7. Шифрование с открытым ключом

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асимметричном шифровании.
4. Дайте краткую характеристику алгоритма RSA.
5. В чем отличие сверхвозрастающей последовательности от обыкновенной?
6. Что означает обратное число по модулю?
7. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
8. В чем суть задачи дискретного логарифмирования?
9. Приведите уравнение эллиптической кривой в короткой форме Вейерштрасса.

Тестирование

Тема 3. Основные термины и определения. Классификация шифров

1. Что является целью криптоанализа?
 - A. Определение стойкости алгоритма
 - B. Увеличение количества функций замещения в криптографическом алгоритме
 - C. Уменьшение количества функций подстановок в криптографическом алгоритме
 - D. Определение использованных перестановок
2. Частота применения брутфорс-атак возросла, поскольку:
 - A. Возросло используемое в алгоритмах количество перестановок и замещений
 - B. Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
 - C. Мощность и скорость работы процессоров возросла
 - D. Длина ключа со временем уменьшилась
3. Что из перечисленного ниже не является свойством или характеристикой односторонней функции хэширования?
 - A. Она преобразует сообщение произвольной длины в значение фиксированной длины
 - B. Имея значение дайджеста сообщения, невозможно получить само сообщение
 - C. Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
 - D. Она преобразует сообщение фиксированной длины в значение переменной длины
4. Что может указывать на изменение сообщения?
 - A. Изменился открытый ключ
 - B. Изменился закрытый ключ
 - C. Изменился дайджест сообщения
 - D. Сообщение было правильно зашифровано

5. Какой из перечисленных ниже алгоритмов является алгоритмом американского правительства, предназначенным для создания безопасных дайджестов сообщений?

- A. Data Encryption Algorithm
- B. Digital Signature Standard
- C. Secure Hash Algorithm
- D. Data Signature Algorithm

Тема 5. Шифры перестановки

1. Что из перечисленного ниже лучше всего описывает отличия между HMAC и CBC-MAC?

- A. HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
- B. HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
- C. HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC
- D. HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

2. В чем преимущество RSA над DSA?

- A. Он может обеспечить функциональность цифровой подписи и шифрования
- B. Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
- C. Это блочный шифр и он лучше поточного
- D. Он использует одноразовые шифровальные блокноты

3. Многие страны ограничивают использование и экспорт криптографических систем. Зачем они это делают?

- A. Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
- B. Эти системы могут использоваться некоторыми странами против их местного населения
- C. Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования
- D. Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

4. Что используется для создания цифровой подписи?

- A. Закрытый ключ получателя
- B. Открытый ключ отправителя
- C. Закрытый ключ отправителя
- D. Открытый ключ получателя

5. Что из перечисленного ниже лучше всего описывает цифровую подпись?

- A. Это метод переноса собственноручной подписи на электронный документ
- B. Это метод шифрования конфиденциальной информации
- C. Это метод, обеспечивающий электронную подпись и шифрование
- D. Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

Тема 7. Шифрование с открытым ключом

1. Какова эффективная длина ключа в DES?

- A. 56
- B. 64
- C. 32
- D. 16

2. По какой причине удостоверяющий центр отзывает сертификат?

- A. Если открытый ключ пользователя скомпрометирован
- B. Если пользователь переходит на использование модели РЕМ, которая использует сеть доверия
- C. Если закрытый ключ пользователя скомпрометирован
- D. Если пользователь переходит работать в другой офис

3. Что из перечисленного ниже лучше всего описывает удостоверяющий центр?

- A. Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
- B. Организация, которая проверяет процессы шифрования
- C. Организация, которая проверяет ключи шифрования
- D. Организация, которая выпускает сертификаты

4. Как расшифровывается аббревиатура DEA?

- A. Data Encoding Algorithm
- B. Data Encoding Application
- C. Data Encryption Algorithm
- D. Digital Encryption Algorithm

5. Кто участвовал в разработке первого алгоритма с открытыми ключами?

- A. Ади Шамир
- B. Росс Андерсон
- C. Брюс Шнайер
- D. Мартин Хеллман

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ПК-1)

1. Протоколы обмена ключами.
2. Протоколы аутентификации. Разновидности и краткая характеристика.
3. Парольная идентификация/аутентификация.
4. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
5. Сервер аутентификации Kerberos.
6. Идентификация/аутентификация с помощью биометрических данных.
7. Идентификационные карты (ID-cards) и электронные ключи.
8. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
9. ЭЦП на базе алгоритма RSA.
10. Алгоритм цифровой подписи ГОСТ 34.10-94.
11. Алгоритм цифровой подписи ГОСТ 34.10-2001.

Типовые задания для зачета (ПК-1)

Зашифровать свою фамилию с помощью шифров:

- шифра масонов;

- биграмного шифра Порты;
- шифра Хилла;
- вариантного шифра;
- шифра Тени;
- совмещенного шифра.

4.4. Шкала оценивания промежуточной аттестации

| Оценка | Компетенции | Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата) |
|---------------------------------|-------------|--|
| «зачтено» (50 - 100 баллов) | ПК-1 | |
| «не зачтено» (0 - 49 баллов) | ПК-1 | |

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Тамб. гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Лопатин Д. В. Программно-аппаратная защита информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
4. Лопатин Д. В. Технология информационной безопасности и методология защиты информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
5. Лопатин Д. В. Защита от вредоносных программ : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
6. Лопатин Д.В., Чиркин Е.С. Защита электронного документооборота в компьютерной системе : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
7. Лопатин Д.В., Чиркин Е.С. Защита информационных процессов в автоматизированных системах : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Бехроуз, А. Криптография и безопасность сетей : учебное пособие. - 2020-11-14; Криптография и безопасность сетей. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/72337.html>
2. Аграновский, А. В., Хади, Р. А. Практическая криптография: алгоритмы и их программирование. - 2021-05-25; Практическая криптография: алгоритмы и их программирование. - Москва: СОЛОН-Пресс, 2016. - 256 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/90248.html>
3. Грибунин, В. Г., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н. Криптография и безопасность цифровых систем : учебное пособие. - Весь срок охраны авторского права; Криптография и безопасность цифровых систем. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011. - 411 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/60851.html>
4. Романьков, В. А. Алгебраическая криптография : монография. - 2023-06-30; Алгебраическая криптография. - Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. - 136 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/24868.html>

6.3 Иные источники:

1. Журнал «Математические вопросы криптографии» - http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option_lang=rus
2. Журнал «BIS Journal - Информационная безопасность банков» - <https://journal.ib-bank.ru/pub/169>
3. Журнал «Занимательная криптография» - <https://bigmir81.livejournal.com/420975.html>
4. Блог «Криптография. Шифрование и криптоанализ» - <https://habrahabr.ru/hub/crypto/page4/>
5. Журнал «Безопасность информационных технологий» - <https://bit.mephi.ru/index.php/bit>
6. Журнал «Мир ПК» - <https://www.osp.ru/pcworld>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Операционная система "Альт Образование"

LibreOffice

Microsoft Windows 10

Microsoft Office Профессиональный плюс 2007

Kaspersky Endpoint Security 10 для Windows "Лаборатория Касперского" 26.07.2018

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.