МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Кафедра «Прикладная информатика в экономике»

# РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине «Криптографические методы защиты информации»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Криптографические методы защиты информации» включена в основную профессиональную образовательную программу направления подготовки _10.03.01 «Информационная безопасность» направленности (профиля) «Организация и технология защиты информации» решением Президиума Ученого совета.

Протокол № 4 от 28.06.2018 г.

Начальник учебно-методического отдела_____ Н.М.Шемендюк

28.06.2018 г.

Рабочая учебная программа по дисциплине «Криптографические методы защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки РФ от 1 декабря 2016 г. N 1515.

Составила: Губанова С.Е., Раченко Т.А.

Согласовано Директор научной библиотеки _____ В.Н. Еремина

Согласовано Начальник управления информатизации _____ В.В. Обухов

Рабочая программа утверждена на заседании кафедры «Прикладная информатика в экономике»
Протокол № _12__ от «_22_» ____06_____ 2018__г.

И.о. заведующего кафедрой _____ _д.э.н., Бердников В.А._____
(подпись) (ученая степень, звание, Ф.И.О.)

Согласовано начальник учебно-методического отдела _____ Н.М.Шемендюк

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цели освоения дисциплины

Целями освоения дисциплины являются:

– изучение изложение основополагающих принципов защиты информации с помощью криптографических методов;

– формирование практических навыков применения криптографических методов на практике для решения профессиональных задач.

1.2. В соответствии с видами профессиональной деятельности, на которые ориентирована образовательная программа указанного направления подготовки, содержание дисциплины позволит обучающимся решать следующие профессиональные задачи:

**эксплуатационная деятельность:**

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

системы обеспечения информационной безопасности с учетом установленных требований.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

| Код компетенции | Наименование компетенции |
|---|---|
| ПК-1 | Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. |
| ОПК-7 | Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты. |
| ОК-4 | Способность использовать основы правовых знаний в различных сферах деятельности. |

1.4. Перечень планируемых результатов обучения по дисциплине

| Результаты освоения дисциплины | Технологии формирования компетенции по указанным результатам | Средства и технологии оценки по указанным результатам |
|---|---|---|
| ***Знает*:**<br>основы термины и понятия методов криптографической защиты информации (ПК-1);<br>методы криптозащиты компьютерных систем и сетей (ОПК-7);<br>нормативные требования по административно-правовому | Лекции | Собеседование |

| Результаты освоения дисциплины | Технологии формирования компетенции по указанным результатам | Средства и технологии оценки по указанным результатам |
|---|---|---|
| регулированию в области криптографической защиты информации (ОК-4). | | |
| ***Умеет*:**<br>применять основные методы криптографии для организации и обеспечения защиты информации (ПК-1);<br>анализировать возможность практической реализации типовых криптографических алгоритмов в профессиональной деятельности (ОПК-7);<br>применять требования государственных стандартов в области криптографии при организации защиты информации (ОК-4). | Лабораторные работы | Защита лабораторных работ |
| ***Имеет практический опыт*:**<br>использования программ для шифрования и формирования/ проверки электронной подписи (ПК-1);<br>анализа типовых криптографических алгоритмов для практической реализации (ОПК-7);<br>в оценке соответствия технологии информационного обмена нормативно-правовым требованиям (ОК-4). | Решение разноуровневых и проблемных задач | Защита лабораторных работ |

## 2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части. Её освоение осуществляется: в 5, 8 семестрах.

| № п/п | Наименование дисциплин, определяющих междисциплинарные связи | Код компетенций |
|---|---|---|
| | *Предшествующие дисциплины* | |
| 1. | Информатика | ОПК-4 |
| 2. | Основы информационной безопасности | ОК-5, ОПК-7 |
| 3. | Математика | ОПК-2 |
| | *Последующие дисциплины* | |
| 1. | Организационное и правовое обеспечение информационной безопасности | ОК-4, ОПК-5 |
| 2. | Основы управления информационной безопасностью | ОПК-5, ОПК-7 |
| 3. | Программно-аппаратные средства защиты информации | ОПК-7, ПК-6 |
| 4. | Теория информации | ПК-7, ПК-8, ПК-13 |
| 5. | Защита информационных процессов в компьютерных системах и телекоммуникационных сетях | ОПК-7 |

**3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу**

*Распределение фонда времени по семестрам и видам занятий*

| Виды занятий | очная форма обучения | очно-заочная форма обучения |
|---|---|---|
| Итого часов<br>Зачетных единиц | 108 ч.<br>3 з.е. | 108 ч.<br>3 з.е. |
| Лекции (час) | 32 ч. | 4 ч. |
| Практические (семинарские) занятия (час) | - | - |
| Лабораторные работы (час) | 52 ч. | 8 ч. |
| Самостоятельная работа (час) | 24 ч. | 92 ч. |
| Курсовой проект (работа) (+,-) | - | - |
| Контрольная работа (+,-) | - | - |
| Экзамен, семестр/час. | - | - |
| Зачет (дифференцированный зачет), семестр | 5 семестр | 8 семестр/4 ч. |
| Контрольная работа, семестр | - | - |

## 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

### 4.1. Содержание дисциплины

| № п/п | Раздел дисциплины | Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах) | | | | Средства и технологии оценки |
|---|---|---|---|---|---|---|
| | | Лекции, час | Практические занятия, час | Лабораторные работы, час | Самостоятельная работа, час | |
| **5, 8 семестры** | | | | | | |
| 1. | Тема 1. История криптографии.<br>Основное содержание:<br>1. Основные этапы становления криптографии как науки.<br>2. Стеганография.<br>3. Развитие криптографии в настоящее время. | 2/0,5 | -/- | -/- | 1/4 | Устный опрос |
| 2. | Тема 2. Основные понятия криптографии. Модели шифров.<br>Основное содержание:<br>1. Открытые сообщения и их характеристики.<br>2. Виды информации, подлежащие закрытию, их модели и свойства.<br>3. Модель угроз безопасности информации.<br>4. Простейшие шифры и их свойства.<br>5. Блочные и поточные шифры.<br>6. Понятие криптосистемы.<br>7. Основные требования к шифрам. | 3/0,5 | -/- | 4/- | 2/10 | Устный опрос, защита лабораторных работ |
| 3. | Тема 3. Нормативно-правовая база криптографии.<br>Основное содержание:<br>1. Стандарты в области криптографии.<br>2. Стандарты России в области криптографии.<br>3. Стандарты криптографического преобразования данных ГОСТ Р 34.12-2015. Процессы формирования и проверки электронной цифровой подписи ГОСТ Р 34.10-2012.<br>Функция хеширования ГОСТ Р 34.11-2012. | 3/0,5 | -/- | -/- | 2/8 | Устный опрос |
| 4. | Тема 4. Шифры перестановки. Шифры замены. Блочные и поточные шифры.<br>Основное содержание:<br>1. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты.<br>2. Криптоанализ шифров перестановок.<br>3. Одноалфавитные и | 2/- | -/- | 8/2 | 2/8 | Устный опрос, защита лабораторных работ |

| № п/п | Раздел дисциплины | Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах) | | | | Средства и технологии оценки |
|---|---|---|---|---|---|---|
| | многоалфавитные замены.<br>4. Табличное и модульное гаммирование.<br>5. Сети Фейстеля. | | | | | |
| 5. | Тема 5. Надежность шифров. Имитостойкость шифров.<br>Основное содержание:<br>1. Теоретико-информационный подход к оценке криптостойкости шифров.<br>2. Криптографическая стойкость шифров. Типы криптостойких систем шифрования.<br>3. Имитация и подмена сообщения. Характеристика имитостойкости шифров.<br>4. Коды аутентификации. | 2/- | -/- | 6/- | 2/6 | Устный опрос, защита лабораторных работ |
| 6. | Тема 6. Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами.<br>Основное содержание:<br>1. Основные классы симметричных криптосистем.<br>2. Реализация криптографических алгоритмов.<br>3. Методы получения случайных и псевдослучайных последовательностей.<br>4. Методы усложнения последовательностей псевдослучайных чисел.<br>5. Программная реализация шифров. | 3/0,5 | -/- | 8/- | 2/8 | Устный опрос, защита лабораторных работ |
| 7. | Тема 7 Методы анализа криптографических алгоритмов.<br>Основное содержание:<br>1. Криптоанализ. Методы криптоанализа.<br>2. Понятие криптоатаки. Классификация криптоатак.<br>3. Классификация методов анализа криптографических алгоритмов. | 2/- | -/- | -/- | 2/7 | Устный опрос |
| 8. | Тема 8. Криптографическая система RSA.<br>Основное содержание:<br>1. Алгоритм RSA.<br>2. Программная реализация алгоритма RSA.<br>3. Преимущества и недостатки.<br>4. Криптографические хэш-функции.<br>5. Характеристики и алгоритмы выработки хэш-функций. | 3/0,5 | -/- | 4/2 | 2/9 | Устный опрос, защита лабораторных работ |

| № п/п | Раздел дисциплины | Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах) | | | | Средства и технологии оценки |
|---|---|---|---|---|---|---|
| 9. | Тема 9. Шифры с открытыми ключами.<br>Основное содержание:<br>1. Проблемы дискретного логарифмирования.<br>2. Задача Диффи-Хеллмана.<br>3. Криптосистема Эль-Гамаля.<br>4. Преимущества асимметричных систем шифрования. | 4/0,5 | -/- | 4/- | 2/8 | Устный опрос, защита лабораторных работ |
| 10. | Тема 10. Электронная подпись.<br>Основное содержание:<br>1 Понятие электронной подписи.<br>2. Виды ЭП.<br>3. Криптографические хэш-функции.<br>4. Характеристики и алгоритмы выработки хэш-функций.<br>5. Общая схема подписывания и проверки подписи с использованием хэш-функции.<br>6. Удостоверяющие центры.<br>7. Цифровая подпись на основе RSA. | 3/0,5 | -/- | 14/2 | 3/10 | Устный опрос, защита лабораторных работ |
| 11. | Тема 11. Модели криптографических протоколов.<br>Основное содержание:<br>1. Понятие криптографического протокола. Требования к протоколам.<br>2. Основные примеры и классификация криптографических протоколов.<br>3. Взаимосвязь между протоколами аутентификации и цифровой подписи.<br>4. Инфраструктура открытых ключей PKI.<br>5. Протоколы сертификации ключей.<br>6. Протоколы распределения ключей. | 3/0,5 | -/- | 4/2 | 2/9 | Устный опрос, защита лабораторных работ |
| 12. | Тема 12. Особенности использования вычислительной техники в криптографии.<br>Основное содержание:<br>1. Программные реализации шифров.<br>2. Различие между программными и аппаратными реализациями.<br>3. Криптографические параметры узлов и блоков шифраторов.<br>4. Вопросы организации сетей засекреченной связи.<br>5. Ключевые системы. | 2/- | -/- | -/- | 2/5 | Устный опрос |
| | Промежуточная аттестация по дисциплине | 32/4 | -/- | 52/8 | 24/92 | Зачёт |

Примечание:

*-/-/-, объем часов соответственно для очной, очно-заочной, заочной форм обучения.*

**4.2. Содержание лабораторных работ**

| № | Наименование лабораторных работ | Обьем часов | Наименование темы дисциплины |
|---|---|---|---|
| **5 семестр** | | | |
| 1. | Лабораторная работа 1. «Построение модели угроз безопасности информации». | 4/- | Основные понятия криптографии |
| 2. | Лабораторная работа 2. «Шифрование сообщений с помощью шифров замены криптографическими функциями Excel». | 4/- | Шифры перестановки. Шифры замены. Блочные и поточные шифры. |
| 3. | Лабораторная работа 3. «Криптоаналитический частотный анализ одноалфавитных шифров средствами Excel». | 4/- | Шифры перестановки. Шифры замены. Блочные и поточные шифры. |
| 4. | Лабораторная работа 4. «Оценка криптостойкости шифра». | 6/- | Надежность шифров. Имитостойкость шифров. |
| 5. | Лабораторная работа 5. «Варианты получения случайных и псевдослучайных последовательностей и их оценка». | 4/- | Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. |
| 6. | Лабораторная работа 6. «Программная реализация шифра DES». | 6/- | Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. |
| 7. | Лабораторная работа 7. «Исследование алгоритма шифрования RSA». | 4/- | Криптографическая система RSA. |
| 8. | Лабораторная работа 8. «Реализация обмена ключей по Диффи-Хеллману». | 8/- | Шифры с открытыми ключами. |
| 9. | Лабораторная работа 9. «Исследование | 6/- | Электронная |

| № | Наименование лабораторных работ | Обьем часов | Наименование темы дисциплины |
|---|---|---|---|
| | процесса формирования ЭП на основе RSA». | | подпись. |
| 10. | Лабораторная работа 10. «Построение схемы жизненного цикла ключей на основе криптографических протоколов». | 6/- | Модели криптографических протоколов. |
| | **Итого за 5 семестр** | 52/- | |
| **8 семестр** | | | |
| 1. | Лабораторная работа 2. «Шифрование сообщений с помощью шифров замены криптографическими функциями Excel». | -/2 | Шифры перестановки. Шифры замены. Блочные и поточные шифры. |
| 2. | Лабораторная работа 6. «Программная реализация шифра DES». | -/2 | Принципы построения криптографических алгоритмов с симметричными и несимметричным ключами. |
| 3. | Лабораторная работа 7. «Исследование алгоритма шифрования RSA». | -/2 | Криптографическая система RSA. |
| 4. | Лабораторная работа 9. «Исследование процесса формирования ЭП на основе RSA». | -/2 | Электронная подпись. |
| | **Итого за 8 семестр** | -/8 | |

Примечание:
*-/-/-, объем часов соответственно для очной, очно-заочной, заочной форм обучения.*

## 5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

*Технологическая карта самостоятельной работы студента*

| Код реализуемой компетенции | Вид деятельности студентов (задания на самостоятельную работу) | Итоговый продукт самостоятельной работы | Средства и технологии оценки | Обьем часов |
|---|---|---|---|---|
| ОК-4 | Работа с литературой | Конспект | Собеседование | 9/-/- |
| ПК-1 | Ответы на контрольные вопросы | Конспект | Тест | 3/-/- |
| ОПК-7 | Подготовка доклада на конференцию | Доклад | Опубликование тезисов доклада | 12/-/- |
| | | | **Итого за 5 семестр** | 24/-/- |
| ОК-4 | Работа с литературой | Конспект | Собеседование | -/-/48 |

| | | | | |
|---|---|---|---|---|
| ПК-1 | Ответы на контрольные вопросы | Конспект | Тест | -/-/8 |
| ОПК-7 | Подготовка доклада на конференцию | Доклад | Опубликование тезисов доклада | -/-/36 |
| | | | **Итого за 8 семестр** | -/-/92 |

**Рекомендуемая литература:** 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.

**Содержание заданий для самостоятельной работы**

*Вопросы для самоконтроля*

1. Основные этапы становления криптографии как науки.
2. Виды информации, подлежащие закрытию, их модели и свойства
3. Модели шифров.
4. Блочные и поточные шифры.
5. Понятие криптосистемы.
6. Ручные и машинные шифры.
7. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты.
8. Криптоанализ шифров перестановок.
9. Одноалфавитные и многоалфавитные замены.
10. Вопросы криптоанализа простейших шифров замены.
11. Стандартные алгоритмы криптографической защиты данных.
12. Табличное и модульное гаммирование.
13. Случайные и псевдослучайные гаммы.
14. Криптограммы, полученные при повторном использовании ключа..
15. Теоретико-информационный подход к оценке криптостойкости шифров.
16. Криптографическая стойкость шифров.
17. Имитация и подмена сообщения.
18. Характеристика имитостойкости шифров.
19. Коды аутентификации.
20. Характеристики помехоустойчивости.
21. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.
22. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним.
23. Методы получения случайных и псевдослучайных последовательностей.
24. Методы усложнения последовательностей псевдослучайных чисел.
25. Понятие криптоатаки.
26. Классификация криптоатак.
27. Классификация методов анализа криптографических алгоритмов.
28. Криптосистемы RSA и Эль-Гамаля.
29. Преимущества асимметричных систем шифрования.
30. Криптографические хэш-функции.
31. Характеристики и алгоритмы выработки хэш-функций.
32. Понятие криптографического протокола.
33. Основные примеры.
34. Классификация криптографических протоколов.
35. Понятие электронной цифровой подписи.
36. Стандарты ЭЦП.
37. Протоколы установления подлинности.
38. Взаимосвязь между протоколами аутентификации и цифровой подписи.

39. Протоколы управления ключами.
40. Протоколы сертификации ключей.
41. Протоколы распределения ключей.
42. Вопросы организации сетей засекреченной связи.
43. Ключевые системы.
44. Нормативный базис криптографии.
45. Удостоверяющие центры. Функциональные обязанности.

## 6. Методические указания для обучающихся по освоению дисциплины

*Инновационные образовательные технологии*

| Вид образовательных технологий, средств передачи знаний, формирования умений и практического опыта | № темы / тема лекции | № практического (семинарского) занятия/наименование темы | № лабораторной работы / цель |
|---|---|---|---|
| Слайд-лекция | Тема 10. Модели криптографических протоколов. | | |

В начале семестра студентам необходимо ознакомиться с технологической картой дисциплины, выяснить, какие результаты освоения дисциплины заявлены (знания, умения, практический опыт). Для успешного освоения дисциплины студентам необходимо выполнить задания, предусмотренные рабочей учебной программой дисциплины и пройти контрольные точки в сроки, указанные в технологической карте (раздел 11). От качества и полноты их выполнения будет зависеть уровень сформированности компетенций и оценка текущей успеваемости по дисциплине. По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы лабораторных работ, вопросы к экзамену и другие необходимые материалы указаны в разработанном для данной дисциплины учебно-методическом пособии.

Основной формой освоения дисциплины является контактная работа с преподавателем – лекции, лабораторные работы, консультации, в том числе проводимые с применением дистанционных технологий.

По дисциплине часть тем изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий, подготовку к промежуточной аттестации (зачету, экзамену).

На лекционных и практических занятиях вырабатываются навыки и умения обучающихся по применению полученных знаний в конкретных ситуациях, связанных с будущей профессиональной деятельностью. По окончании изучения дисциплины проводится промежуточная аттестация (экзамен).

Регулярное посещение аудиторных занятий не только способствует успешному овладению знаниями, но и помогает организовать время, т.к. все виды учебных занятий распределены в семестре планомерно, с учетом необходимых временных затрат.

### 6.1. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

*Лабораторные работы*

| № | Наименование лабораторной работы | Задания по лабораторной работе |
|---|---|---|
| 3 семестр | | |
| 1. | Лабораторная работа 1. «Построение модели угроз безопасности». | Берётся конкретная предметная область (банк, учебное заведение, госучреждение, больница, лаборатория, промышленное предприятие – по выбору). Строится модель виртуальной инфраструктуры, набор данных, степень конфиденциальности данных, количество пользователей, точки выхода в Сеть и пр. Для этой структуры необходимо создать модель актуальных угроз и соответствующий инструментарий криптозащиты с обоснованием. |
| 2. | Лабораторная работа 2. «Шифрование сообщений с помощью шифров замены криптографическими функциями Excel». | Зашифровывание определённой фразы с использованием метода Цезаря и среды Microsoft Excel.<br>Расшифровывание данной фразы с использованием метода Цезаря и среды Microsoft Excel. |
| 3. | Лабораторная работа 3. «Криптоаналитический частотный анализ одноалфавитных шифров средствами Excel». | Открыть книгу MS Excel «Простая замена.xlsm», в строке предупреждения включить выполнение макросов.<br>Скопировать текст криптограммы, загрузить, подсчитать частоты появления символов криптограммы, упорядочить, сравнить со стандартными частотами символов русского языка, предложить варианты соответствия, проверить. |
| 4. | Лабораторная работа 4. «Оценка криптостойкости шифра». | Все современные криптосистемы построены по принципу Кирхгофа, т.е. секретность зашифрованных сообщений определяется секретностью ключа.<br>Моноалфавитная подстановка является наименее стойким шифром, так как при ее использовании сохраняются все статистические закономерности исходного текста.<br>Стойкость простой полиалфавитной подстановки оценивается значением 20 n , где n — число различных алфавитов, используемых для замены.<br>Стойкость простой перестановки однозначно определяется размерами используемой матрицы.<br>Стойкость гаммирования однозначно определяется длиной периода гаммы.<br>При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов. |
| 5. | Лабораторная работа 5. «Варианты получения случайных и псевдослучайных | Предложить методы получения случайных (псевдослучайных) последовательностей.<br>Учесть необходимость равномерного |

| № | Наименование лабораторной работы | Задания по лабораторной работе |
|---|---|---|
| | последовательностей и их оценка». | распределения. Оценить результаты.<br>Линейный конгуэнтный генератор псевдослучайных чисел (ЛКГ ПСЧ)<br>$x_{k+1} = (ax_k + b) \bmod m$,<br>где $x_0$ - начальное значение (инициализирующий вектор)<br>a - множитель<br>b - приращение<br>m - модуль<br>У такого генератора максимальный период равен m. Он достигается, например, при выборе констант Парка-Милера:<br>$x_{k+1} = 75x_k \bmod (231 – 1)$<br>Нелинейные конгуэнтные генераторы псевдослучайных чисел (НКГ ПСЧ)<br>Квадратный конгуэнтный генератор выглядит следующим образом:<br>$x_{k+1} = (ax_k^2 + bx_k + c) \bmod m$ |
| 6. | Лабораторная работа 6. «Программная реализация шифра DES». | В программной реализации должен быть разработан<br>интерфейс, удобный для эксплуатации программы, в интерфейсе следует предусмотреть:<br>• два режима формирования ключа – ключ задан, ключ формируется по умолчанию;<br>• ввод начальной информации из сформированного заранее файла и из файла, который создается в оболочке программы;<br>• режимы шифрования, которые предусмотрены в DES;<br>• режимы шифрования и дешифрования информации. |
| 7. | Лабораторная работа 7. «Исследование алгоритма шифрования RSA». | Наиболее важной частью алгоритма RSA является процесс создания пары открытый/секретный ключи. В RSA он состоит из следующих шагов.<br><br>1. Согласно номеру компьютера выберите значения двух секретных простых чисел, p и q, $p^1q$. Допустим, что p=17, q=31.<br>2. Вычислите n=p*q=29*7=203.<br><br>3. Согласно заданной формуле, рассчитайте функцию Эйлера.F(p,q)=(p-1)(q-1)=(29-1)(7-1)=168<br>4. Пользуясь методом подбора, который должен отвечать условию , рассчитайте значения e, k и d. Открытый (e) и секретный (d) ключи должны быть взаимно простыми. В нашем случае e=11, k=7, d=107. |

| № | Наименование лабораторной работы | Задания по лабораторной работе |
|---|---|---|
| | | e•d=k•f(p,q)+1 11•107= k•168+1 |
| 8. | Лабораторная работа 8. «Реализация обмена ключей по Диффи-Хеллману». | Расписать пошаговую схему обмена ключами между А и Б.<br>А и Б выбирают два числа g и p.<br>А и Б выбирают секретные числа (a и b соответственно)<br>А и Б вычисляют g ^ x mod p, где x – секретное число.<br>А и Б обмениваются полученными данными (числа Г и В соответственно).<br>А и Б используют полученное число и секретное число для вычисления общего ключа.<br>В шаге 5 имеем следующее:<br>У А: B^a mod p = (g^b mod p) ^ a mod p = g^ab mod p.<br>У Боба: Г^b mod p = (g^a mod p) ^ b mod p = g^ab mod p.<br>Получили одинаковый ключ. |
| 9. | Лабораторная работа 9. «Реализация процесса формирования ЭП на основе RSA». | Для осуществления подписи сообщения $m=m_1m_2m_3..m_n$ необходимо вычислить хеш-функцию $y=h(m_1m_2m_3..m_n)$, которая ставит в соответствие сообщению m число y. На следующем шаге достаточно снабдить подписью только число y, и эта подпись будет относиться ко всему сообщению m.<br>Далее по алгоритму RSA вычисляются ключи (e,n) и (d,n).<br>Затем вычисляется $s = y^d \bmod n$ (d на этот раз секретная степень).<br>Число s это и есть цифровая подпись. Она просто добавляется к сообщению и получается подписанное сообщение <m,s>.<br>Теперь каждый, кто знает параметры подписавшего сообщение (т.е. числа e и n), может проверить подлинность подписи.<br>Для этого необходимо проверить выполнение равенства $h(m) = s^e \bmod n$ |
| 10. | Лабораторная работа 10. «Построение схемы жизненного цикла ключей на основе криптографических протоколов». | Расписать подробные шаги по реализации ключей и протоколы, участвующие в их взаимодействиях.<br>1.Регистрация пользователя.<br>2.Инициализация пользователя.<br>3.Генерация ключа.<br>4.Инсталляция ключа. |

| № | Наименование лабораторной работы | Задания по лабораторной работе |
|---|---|---|
| | | 5.Регистрация ключа.<br>6.Штатное использование ключа.<br>И т.д.<br>Протокол обмена ключей.<br>Протокол распределения ключей.<br>Блокировочный протокол. |

Лабораторные работы обеспечивают: демонстрацию применения теоретических знаний на практике, закрепление и углубление теоретических знаний, контроль знаний и умений в формулировании выводов, развитие интереса к изучаемой дисциплине.

Применение лабораторных работ позволяет вовлечь в активную работу всех обучающихся группы и сформировать интерес к изучению дисциплины.

Самостоятельный поиск ответов на поставленные вопросы и задачи в ходе лабораторной работы приобретают особую значимость в восприятии, понимании содержания дисциплины.

Изученный на лекциях материал лучше усваивается, лабораторные работы демонстрируют практическое их применение.

### 6.2. Методические указания для выполнения контрольных работ

Контрольная работа **по дисциплине учебным планом не предусмотрена.**

### 6.3. Методические указания для выполнения курсовых работ

Курсовая работа рассматривается как вид учебной работы по дисциплине и выполняется в пределах часов, отводимых на её изучение. Выполнение курсовых работ по дисциплине осуществляется в соответствии с тематикой, сформированной в соответствии с содержанием дисциплины, сопряженным с направленностью (профилем) образовательной программы. Подготовка курсовой работы содействует лучшему усвоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся навыков поиска и критического анализа научной литературы, готовит их к самостоятельной профессиональной деятельности, повышает уровень профессиональной подготовки, является подготовительным этапом к написанию выпускником выпускной квалификационной работы.

Выполнение курсовых работ предусматривается по дисциплинам, формирующим последовательно профессиональные компетенции выпускника, и служит основой для выполнения выпускной квалификационной работы.

**Примерная тематика курсовой работы**

1. Программная реализация шифров замены.
2. Программная реализация шифров перестановки.
3. Средство шифрования информации на основе ГОСТ Р 34.12–2015.
4. Сравнительный анализ алгоритмов формирования хэш-функций.
5. Сравнительный анализ криптографических протоколов распределения ключей.
6. Синтез шифров.
7. Управление криптографическими ключами в асимметрической криптосистеме.
8. Криптографическая стойкость шифров.
9. Модели открытых текстов на основе частотных характеристик языка. Энтропия и избыточность языка.
10. Способы повышения имитостойкости, помехоустойчивости шифров.

## 7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (зачет, экзамен)

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций и результаты освоения дисциплины, представлены следующими компонентами:

| Код оцениваемой компетенции | Тип контроля | Вид контроля | Количество элементов, шт. |
|---|---|---|---|
| ПК-1 | *текущий* | *Тест / устный опрос* | *5/4* |
| ОПК-7 | *текущий* | *Тест / устный опрос* | *2/5* |
| ОК-4 | *текущий* | *Тест / устный опрос* | *3/3* |
| ПК-1, ОПК-7, ОК-4 | *промежуточный* | *компьютерный тест* | *80* |

**7.1. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины**

| Результаты освоения дисциплины | Оценочные средства |
|---|---|
| ***Знает*:**<br>основы термины и понятия методов криптографической защиты информации (ПК-1);<br>методы криптозащиты компьютерных систем и сетей (ОПК-7);<br>нормативные требования по административно-правовому регулированию в области криптографической защиты информации (ОК-4). | **ПК-1**<br>1.Шифр Цезаря относится к шифрам<br>1) перестановки<br>2) замены<br>3) гаммирования<br>2. Выберите криптографические хэш-функции<br>1) DES<br>2) RSA<br>3) MD-5<br>4) AES<br>3. Сеть Фейстеля используется<br>1) в симметричном шифровании<br>2) в асимметричном шифровании<br>4. Какие из следующих утверждений верные?<br>1) открытый ключ ЭП и сертификат ЭП – синонимы<br>2) открытый ключ ЭП содержит сертификат ЭП<br>3) сертификат ЭП содержит открытый ключ ЭП<br>5. Алгоритм RSA используется<br>1) в режиме шифрования<br>2) в режиме электронной подписи<br>3) то и другое<br>**ОПК-7**<br>6. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма RSA<br>1) задача факторизации больших чисел<br>2) задача дискретного логарифмирования<br>7. В каких шифрах используется один и тот же ключ для шифрования и дешифрирования?<br>1) симметричных<br>2) асимметричных<br>8. Опишите суть односторонней функции<br>**ОК-4**<br>9. Какие задачи решает ЭП<br>1) конфиденциальность |

| Результаты освоения дисциплины | Оценочные средства |
|---|---|
| | 2) целостность<br>3) авторство<br>4) неотказуемость<br>10. Каким ключом шифруется сообщение для партнёра в асимметричных системах<br>1) своим закрытым<br>2) своим открытым<br>3) открытым ключом партнёра<br>4) закрытым ключом партнера<br>11. Каким ключом проверяется подлинность ЭП?<br>1) открытым<br>2) закрытым |
| ***Умеет*:**<br>применять основные методы криптографии для организации и обеспечения защиты информации (ПК-1);<br>анализировать возможность практической реализации типовых криптографических алгоритмов в профессиональной деятельности (ОПК-7);<br>применять требования государственных стандартов в области криптографии при организации защиты информации (ОК-4). | **ПК-1**<br>1. Приведите схему формирования электронной подписи и поясните ее основные этапы<br>2. Опишите процедуру проверки подлинности ЭП<br>**ОПК-7**<br>1. Как длина ключа влияет на безопасность информационного обмена?<br>2. Опишите различие между симметричными и асимметричными криптосистемами.<br>**ОК-4**<br>1. В каких случаях используются зарубежные и отечественные криптоалгоритмы.<br>2. Укажите основные этапы жизненного цикла ключей шифрования и электронной подписи. |
| ***Имеет практический опыт*:**<br>использования программ для шифрования и формирования/ проверки электронной подписи (ПК-1);<br>анализа типовых криптографических алгоритмов для практической реализации (ОПК-7);<br>в оценке соответствия технологии информационного обмена нормативно-правовым требованиям (ОК-4). | **ПК-1**<br>1. Использование простых шифров перестановки, замены, одноразового блокнота.<br>2. Разработка практической реализации криптоалгоритма RSA.<br>**ОПК-7**<br>1. Шифрование сообщений электронной почты, постановка электронной подписи средствами почтового клиента.<br>2. Шифрование файлов, постановка электронной подписи на файлах средствами специального ПО.<br>**ОК-4**<br>1. Как установить, удалить, найти, проверить, просмотреть, экспортировать, импортировать сертификат электронной подписи на компьютере. |

### 7.2. Методические рекомендации к определению процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Рабочая учебная программа дисциплины содержит следующие структурные элементы:

- перечень компетенций, формируемых в результате изучения дисциплины в процессе освоения образовательной программы;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе освоения образовательной программы (далее–задания). Задания по каждой компетенции, как правило, не должны повторяться.

Требования по формированию задания на оценку ЗНАНИЙ:

- обучающийся должен воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;

- применяются средства оценивания компетенций: тестирование, вопросы по основным понятиям дисциплины и т.п.

Требования по формированию задания на оценку УМЕНИЙ:

- обучающийся должен решать типовые задачи (выполнять задания) на основе воспроизведения стандартных алгоритмов решения;

- применяются следующие средства оценивания компетенций: простые ситуационные задачи (задания) с коротким ответом или простым действием, упражнения, задания на соответствие или на установление правильной последовательности, эссе и другое.

Требования по формированию задания на оценку навыков и (или) ОПЫТА ДЕЯТЕЛЬНОСТИ:

- обучающийся должен решать усложненные задачи (выполнять задания) на основе приобретенных знаний, умений и навыков, с их применением в определенных ситуациях;

- применяются средства оценивания компетенций: задания требующие многошаговых решений как в известной, так и в нестандартной ситуациях, задания, требующие поэтапного решения и развернутого ответа, ситуационные задачи, проектная деятельность, задания расчетно-графического типа. Средства оценивания компетенций выбираются в соответствии с заявленными результатами обучения по дисциплине.

Процедура выставления оценки доводится до сведения обучающихся в течение месяца с начала изучения дисциплины путем ознакомления их с технологической картой дисциплины, которая является неотъемлемой частью рабочей учебной программы по дисциплине.

В результате оценивания компетенций по дисциплине студенту начисляются баллы по шкале, указанной в рабочей учебной программе по дисциплине.

### 7.3. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Успешность усвоения дисциплины характеризуется качественной оценкой на основе листа оценки сформированности компетенций, который является приложением к зачетно-экзаменационной ведомости при проведении промежуточной аттестации по дисциплине.

**Критерии оценивания компетенций**

*Компетенция считается сформированной*, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует *повышенному уровню* сформированности компетенции.

*Компетенция считается сформированной*, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и

другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует *пороговому уровню* сформированности компетенции.

*Компетенция считается несформированной*, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет практические работы, не демонстрирует необходимых умений, доля невыполненных заданий, предусмотренных рабочей учебной программой составляет 55 %, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует *допороговому уровню*.

**Шкала оценки уровня освоения дисциплины**

Качественная оценка может быть выражена: в процентном отношении качества усвоения дисциплины, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2, «зачтено», «не зачтено». Преподаватель ведет письменный учет текущей успеваемости студента в соответствии с технологической картой по дисциплине.

*Шкала оценки результатов освоения дисциплины, сформированности компетенций*

| Шкалы оценки уровня сформированности компетенции (й) | | Шкала оценки уровня освоения дисциплины | | |
|---|---|---|---|---|
| *Уровневая шкала оценки компетенций* | *100 балльная шкала, %* | *100 балльная шкала, %* | *5-балльная шкала, дифференцированная оценка/балл* | *Недифференцированная оценка* |
| допороговый | ниже 61 | ниже 61 | «неудовлетворительно» / 2 | не зачтено |
| пороговый | 61-85,9 | 70-85,9 | «хорошо» / 4 | зачтено |
| | | 61-69,9 | «удовлетворительно» / 3 | зачтено |
| повышенный | 86-100 | 86-100 | «отлично» / 5 | зачтено |

## 8. Учебно-методическое и информационное обеспечение дисциплины

### 8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

*Списки основной литературы*

1. Защита информации [Электронный ресурс] : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук [и др.]. - 2-е изд. - Документ HTML. - М. : РИОР [и др.], 2015. - 393 с. - Режим доступа: http://znanium.com/bookread.php?book=474838.
2. Криптографическая защита информации [Электронный ресурс] : учеб. пособие / С. О. Крамаров [и др.] под ред. С. О. Крамарова. - Документ Bookread2. - М. : Риор [и др.], 2018. - 324 с. - Режим доступа: http://znanium.com/bookread2.php?book=901659.

3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров. - Изд. 4-е, стереотип. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 321 с. - Режим доступа: https://e.lanbook.com/reader/book/103908/#1/
4. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 120 с. - Режим доступа: https://e.lanbook.com/reader/book/107307/#1.
5. Никифоров, С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 158 с. - Режим доступа: https://e.lanbook.com/reader/book/106734/#1.
6. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502.

*Списки дополнительной литературы*

7. Лебедько, Е. Г. Теоретические основы передачи информации [Текст] : [учеб. пособие] для вузов по направлению подгот. "Оптотехника" и специальности "Оптико-электрон. приборы и системы" / Е. Г. Лебедько. - СПб. : Лань, 2011. - 350 с. : ил..
8. Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учеб. пособие для вузов по специальностям "Многоканальн. телекоммуникац. системы", "Радиосвязь, радиовещание и телевидение", "Защищен. системы связи" / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия - Телеком, 2005. - 229 с. : ил.
9. Смарт, Н. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова под ред. С. К. Ландо. - М. : Техносфера, 2006. - 528 с. : ил.
10. Торстейнсон, П. Криптография и безопасность в технологии .NET [Текст] / П. Торстейнсон ; пер. с англ. В. Д. Хорева под ред. С. М. Молявко. - М. : БИНОМ. Лаб. знаний, 2007. - 480 с. : ил.
11. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости [Текст] : учеб. пособие для вузов по специальности "Компьютерная безопасность" / А. В. Черемушкин. - М. : Академия, 2009. - 272 с.

## 8.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет"), необходимых для освоения дисциплины

*Интернет-ресурсы*

1. ИНТУИТ. Национальный открытый университет [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/. – Загл. с экрана.

2. Российское образование [Электронный ресурс] : федер. портал. - Режим доступа: http://www.edu.ru. - Загл. с экрана.

3. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.

4. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. - Загл. с экрана.

## 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

*Краткая характеристика применяемого программного обеспечения*

| № п/п | Программный продукт | Характеристика | Назначение при освоении дисциплины |
|---|---|---|---|
| 1. | Microsoft Office | Пакет прикладных программ | Оформление отчетов по лабораторным работам |
| 2. | Microsoft Excel | Среда программирования | Выполнение лабораторных работ |

## 10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации.

Для проведения практических занятий (занятий семинарского типа), групповых и индивидуальных консультаций используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения.

Для текущего контроля и промежуточной аттестации используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью, и (или) компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

Для самостоятельной работы обучающихся используются специальные помещения - учебные аудитории для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

**11. Примерная технологическая карта дисциплины «Криптографические методы защиты информации»**

Институт экономики
кафедра «Прикладная информатика в экономике»
преподаватель _____, направление подготовки 10.03.01 «Информационная безопасность»

| № | Виды контрольных точек | Кол-во контр. точек | Кол-во баллов за 1 контр. точку | График прохождения контрольных точек | | | | | | | | | | | | | | | | Зач. неделя |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Сентябрь | | | | Октябрь | | | | Ноябрь | | | | Декабрь | | | | |
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | |
| 1. | Обязательные задания: | | | | | | | | | | | | | | | | | | | |
| 1.1. | Выполнение лабораторных работ | 7 | 10 | | + | | + | | + | | + | | + | | + | | + | | | |
| 2. | Дополнительные задания: | | | | | | | | | | | | | | | | | | | |
| 2.1. | Промежуточное тестирование | 1 | 30 | | | | | | | | | | | | | | | + | | |
| | | | | | | | | | | | | | | | | | | | | |
| | Зачет | | | | | | | | | | | | | | | | | | | |