Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Астраханский государственный технический университет»
Система менеджмента качества в области образования, воспитания, науки и инноваций сертифицирована DQS по международному стандарту ISO 9001:2015

Институт информационных технологий и коммуникаций

Кафедра «Информационная безопасность»

ЗАЩИТА ИНФОРМАЦИИ

Методические указания
для самостоятельной работы студентов

направления подготовки
09.03.01 «Информатика и вычислительная техника»

Профиль подготовки
«Автоматизированные системы обработки информации и управления»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная, заочная

АСТРАХАНЬ – 2018

Автор(ы): к.т.н., доцент Давидюк Н.В.

Рецензент: д.т.н., проф., зав. кафедрой ИБ Попов Г.А.

Методические указания по выполнению самостоятельной работы по дисциплины «Защита информации» утверждены на заседании кафедры «Информационная безопасность» «14» июня 2018 г., протокол №14.

© Астраханский государственный технический университет

Цель методических указаний: оказание помощи обучающимся в выполнении самостоятельной работы по дисциплине «Защита информации».

Настоящие методические указания содержат работы, которые позволят обучающимся самостоятельно овладеть фундаментальными знаниями, профессиональными умениями и навыками деятельности по данной дисциплине, и направлены на формирование следующих компетенций:

Код	**Определение**
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате выполнения самостоятельных работ по дисциплине «Защита информации» обучающиеся должны:

Знать	**Уметь**	**Владеть навыками и (или) иметь опыт**
основные нормативно-правовые акты в области информационной безопасности	применять на практике нормативные и правовые документы, регламентирующие деятельность в сфере информационной безопасности, классифицировать защищаемую информацию по видам тайн в соответствии с законодательством РФ и определять меры по ее защите	использования положений нормативно-правовых актов для обеспечения защиты информации ограниченного доступа
основы государственной информационной политики, стратегию развития информационного общества в России; понятие государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну, и сведений конфиденциального характера; организационно-правовые основы режима секретности; цели и задачи обеспечения информационной безопасности; основные термины по проблематике информационной безопасности; методы обеспечения защиты информации;	пользоваться законодательными и нормативными документами в профессиональной деятельности; пользоваться современными источниками информации по исследуемым проблемам и задачам; осуществлять сбор, обработку, анализ и систематизацию информации по обеспечению информационной безопасности; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; пользоваться нормативно-правовой, организационно-распорядительной и методической документацией по вопросам обеспечения информационной безопасности; составлять перечень конфиденциальных	анализа организаций и защищенности их информационных ресурсов с точки зрения информационной безопасности, состава комплекса мер для обеспечения защиты информации

классификацию угроз; классификацию каналов утечки информации; модель потенциального злоумышленника	информационных ресурсов; определять состав угроз безопасности информации и возможные каналы утечки информации; составить представление о потенциальном злоумышленнике	

1. Перечень видов самостоятельной работы по дисциплине «Защита информации» Для очной формы обучения

№ п/п	Тема (*в соответствии с РП*)	Вид самостоятельной работы	Форма контроля	СРС		Требования к выполнению заданий (*знание и/или умение и/или владение навыками*)
				Аудиторная СРС	Внеаудиторная СРС	
1	Основные термины и определения в области информационной безопасности. Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №1 «Расчет вероятности проникновения злоумышленника на объект хранения информации»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу	использования положений нормативно-правовых актов для обеспечения защиты информации ограниченного доступа; анализа организаций и защищенности их информационных ресурсов с точки зрения информационной безопасности, состава комплекса мер для обеспечения защиты информации
2	Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений. Определение требований к защищаемой информации.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №2 «Преобразование аналоговых телефонных сообщений (скремблеры)»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу	

	Особенности автоматизированной системы обработки информации как объекта защиты.					
3	Понятие угрозы безопасности информации, коррелирующие с этим понятием термины. Основные виды угроз безопасности субъектов информационных отношений. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №3 «Модели дискреционного управления доступом Харрисона-Руззо-Ульмана»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу	
4	Классификация каналов проникновения в систему и технических каналов утечки информации. Модель нарушителя.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №4 «Модель доступа Белла-ЛаПадула»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу	
5	Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация. Основные механизмы защиты информации.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе,	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №5 «Шифры перестановки»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка	

	Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и аутентификация. Особенности парольных систем аутентификации. Протоколирование и аудит. Методы разграничения доступа. Понятие модели управления доступом. Типы моделей управления доступом. Системы обнаружения вторжений.	подготовка к устному опросу			к устному опросу	
6	Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №6 «Шифры простой замены»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу	
7	Построение систем защиты от угроз нарушения целостности.	Подготовка к выполнению и выполнение лабораторной работы,	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №7 «Шифры сложной замены»	Подготовка к лабораторной работе, собеседованию и отчету по	

		собеседованию и отчету по работе, подготовка к устному опросу			лабораторной работе; подготовка к устному опросу	
8	Схема системы защиты от угроз нарушения доступности.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №8 «Шифрование методом гаммирования»	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу	
9	Организационные меры защиты информации в автоматизированных системах.	Подготовка к выполнению и выполнение лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу и контрольной работе	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №9 «Одноразовая система шифрования», контрольная работа	Подготовка к лабораторной работе, собеседованию и отчету по лабораторной работе; подготовка к устному опросу; подготовка к контрольной работе	

Для заочной формы обучения

№ п/п	**Тема (*в соответствии с РП*)**	**Вид самостоятельной работы**	**Форма контроля**	**СРС**		**Требования к выполнению заданий (*знание и/или умение и/или владение навыками*)**
				Аудиторная СРС	**Внеаудиторная СРС**	
1	Основные термины и определения в области информационной	Подготовка к выполнению лабораторной работы,	Собеседование и отчет по лабораторной	Лабораторная работа №1 «Расчет вероятности проникнов	Работа №2 «Преобразование аналоговых телефонных сообщений	использования положений нормативно-правовых актов для обеспечения

	безопасности. Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера. Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений. Определение требований к защищаемой информации. Особенности автоматизированной системы обработки информации как объекта защиты. Понятие угрозы безопасности информации, коррелирующие с этим понятием термины. Основные виды угроз безопасности субъектов информационных отношений. Уязвимость основных структурно-	выполнение работы, собеседованию и отчету по работе, подготовка к устному опросу	работе, устный опрос	ения злоумышленника на объект хранения информации», устный опрос, решение задач	(скремблеры)». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	

	функциональных элементов распределенных автоматизированных систем. Классификация каналов проникновения в систему и технических каналов утечки информации. Модель нарушителя.					
2	Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация. Основные механизмы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и аутентификация. Особенности парольных систем аутентификации. Протоколирование и аудит.	Подготовка к выполнению лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №3 «Модели дискреционного управления доступом Харрисона-Руззо-Ульмана»	Лабораторная работа №4 «Модель доступа Белла-ЛаПадула». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	

	Методы разграничения доступа. Понятие модели управления доступом. Типы моделей управления доступом. Системы обнаружения вторжений.					
3	Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.	Подготовка к выполнению лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу	Собеседование и отчет по лабораторной работе, устный опрос	Лабораторная работа №5 «Шифры перестановки»	Лабораторная работа №6-7 «Шифры простой замены. Шифры сложной замены». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе	
4	Построение систем защиты от угроз нарушения целостности. Схема системы защиты от угроз нарушения доступности. Организационные меры защиты информации в автоматизированных системах.	Подготовка к выполнению лабораторной работы, собеседованию и отчету по работе, подготовка к устному опросу и контрольной работе	Собеседование и отчет по лабораторной работе, устный опрос, контрольная работа	Лабораторная работа №8 «Шифрование методом гаммирования», контрольная работа	Лабораторная работа №9 «Одноразовая система шифрования». Подготовка к лабораторной работе, опросу, собеседованию и отчету по работе. Подготовка к контрольной работе	

2. Тематика и задания самостоятельной работы

Темы самостоятельных работ совпадают с названиями разделов дисциплины «Защита информации».

ЗАДАНИЯ ДЛЯ СРС

1. Лабораторные работы

Задание – подготовка к выполнению лабораторной работы и отчета по результатам выполнения работы (частично аудиторно).

Требования к выполнению и последовательность выполнения задания:

Необходимо заранее изучить методические рекомендации по проведению лабораторной работы. Обратить внимание на цель занятия, на основные вопросы для подготовки к занятию, на контрольные вопросы самопроверки после каждой лабораторной работы, на содержание темы занятия.

Порядок выполнения задания:

Подготовиться к выполнению лабораторной работы, изучить теоретические материалы по изучаемой теме, по результатам выполненной согласно задания в методических указаниях работы подготовить отчет. Подготовиться к собеседованию по тематике работы.

Форма контроля – собеседование и отчет по лабораторным работам.

Требования к оформлению отчета:

Подготовить отчет по работе и оформить в соответствии с типовой структурой:

1. Тема лабораторной работы
2. Цель и задачи лабораторной работы
3. Ход и пошаговое описание выполнения заданий лабораторной работы
4. Вывод по работе

Тематика лабораторных работ представлена в Приложении 1.

Рекомендуемые источники указаны в рабочей программе дисциплины.

2. Устный опрос

Задание – подготовка к устному опросу по изучаемым темам

Требования к выполнению и последовательность выполнения задания:

Подготовиться к устному опросу, изучив предоставленные материалы по изучаемой теме.

Порядок выполнения задания:

Необходимо заранее изучить вопросы по изучаемым темам, представленные в Приложении 1, подготовить на них развернутые ответы.

Форма контроля – качество ответов обучающихся на вопросы по темам.

Рекомендуемые источники указаны в рабочей программе дисциплины.

3. Контрольная работа

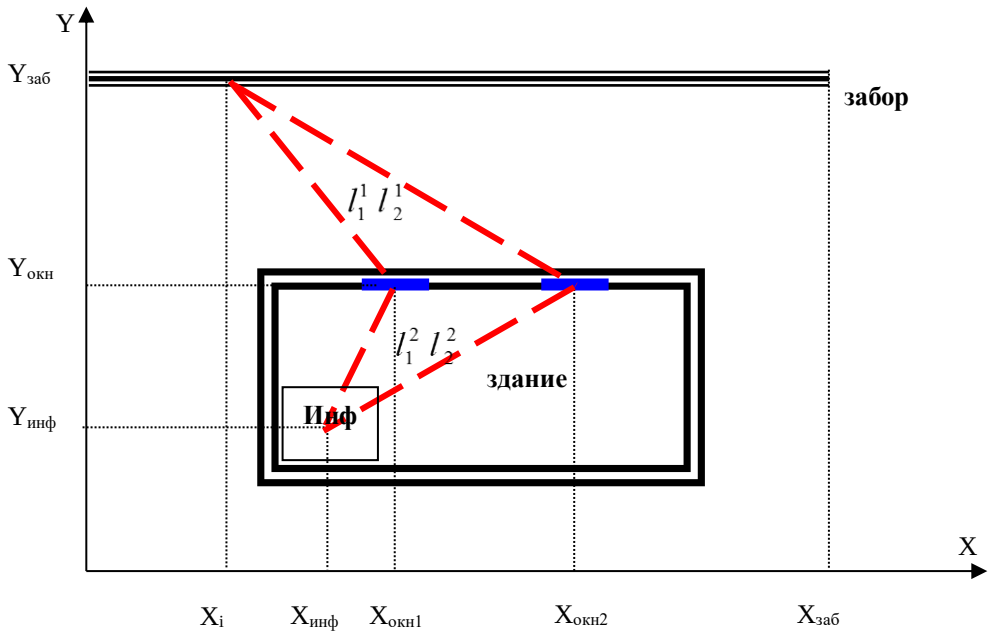
Задание –подготовка к контрольной работе.

Требования к выполнению и последовательность выполнения задания:

В качестве теоретического вопроса – вопросы из списка вопросов к зачету.

Типовые задачи:

1. Дан объект хранения информации, состоящий из заграждения и здания с двумя окнами. Необходимо определить траекторию, по которой вероятность проникновения злоумышленника на объект будет минимальной.



Исходные данные:
План расположения объекта:
Yзаб= 50,
Xзаб= 50,
Yок = 30,
Xокн1 = 20,
Xокн2 = 30,
Yин = 15,
Xин = 25,
Xi= 45
Вероятность проникновения через окна:
Рок1 = 0,2,
Рок2 = 0,4
3. Коэффициенты защищенности:
k1 = 1,
k2 = 0,5

2. Методом вертикальной перестановки зашифруйте словосочетание КОНТРОЛЬНАЯ_РАБОТА. Ключ: 531462.

3. С помощью магического квадрата 4х4 зашифруйте словосочетание ЗАЩИТАИНФОРМАЦИИ-НАША_ДИСЦИПЛИНА.

4. Методом двойной перестановки зашифруйте словосочетание ЖИЗНЬ_ПРЕКРАСНА!. Ключи (столбцы, строки): 3142, 1432.

5. К заданной шифрограмме слова ПЕРЕСТАНОВКА подберите все возможные ключи и объясните полученный результат. ЕАВПРОТАЕНКС.

6. Самостоятельно составьте шифрующую таблицу Трисемуса (размерность 8х4; й=и, ё=е, +_; ключевое слово: ОТЛИЧНО) и зашифруйте с ее помощью слово КОНФИДЕНЦИАЛЬНОСТЬ.

7. Методом аффинной подстановки Цезаря зашифруйте слово ИМПЕРАТОР. При этом учтите следующее: m=32 (й=и, ё=е, +_), константыА и В выбрать самостоятельно согласно существующим требованиям.

8. Методом аффинной подстановки Цезаря зашифруйте слово ПОДСТАНОВКА. При этом учтите следующее: m=32 (й=и, ё=е, +_), константыА и В выбрать самостоятельно согласно существующим требованиям.

9. Зашифруйте слово КРИПТОГРАФИЯ, используя для генерации гаммы шифра линейный конгруэнтный генератор. При этом считайте b=7, a=5, Y0=2, m=4 (почему выбраны такие константы?) или выберите константы самостоятельно, длина алфавита – 31 (и=й, е=ё).

Для подготовки к контрольной работе необходимо повторить весь пройденный на момент проведения работы теоретический материал согласно тематическому плану лекций.

Форма контроля – оценка выполнения заданий контрольной работы.

Рекомендуемые источники указаны в рабочей программе дисциплины.

Приложение 1

Темы лабораторных работ:

Лабораторная работа №1 «Расчет вероятности проникновения злоумышленника на объект хранения информации»
Лабораторная работа №2 «Преобразование аналоговых телефонных сообщений (скремблеры)»
Лабораторная работа №3 «Модели дискреционного управления доступом Харрисона-Руззо-Ульмана»
Лабораторная работа №4 «Модель доступа Белла-ЛаПадула»
Лабораторная работа №5 «Шифры перестановки»
Лабораторная работа №6 «Шифры простой замены»
Лабораторная работа №7 «Шифры сложной замены»
Лабораторная работа №8 «Шифрование методом гаммирования»
Лабораторная работа №9 «Одноразовая система шифрования»

Типовые вопросы для подготовки к опросу и собеседованию:

1. Что такое система физической защиты объекта?
2. Какие требования предъявляются к комплексной системе безопасности объекта?
3. Аналоговый, дискретный сигнал.

4. Спектр. Спектр аналогового и дискретного сигнала.
5. Скремблер. Принцип действия скремблера.
6. Условие для выбора n (число мелких интервалов в пределах T).
7. Виды скремблирования. Достоинства и недостатки.
8. Полосовой фильтр. Как он используется при скремблировании, в каком из видов скремблирования.
9. Инверсия частотного спектра сообщения. Для чего применяется?
10. Какие модели доступа Вам известны? Раскройте их сущность.
11. К каким криптосистемам относится данный шифр?
12. Алгоритм шифрования по данному методу.
13. Достоинства и недостатки указанного шифра.
14. Криптостойкость указанного шифра.

Список вопросов к зачету:

1. Основные термины и определения: информация, информационные отношения, субъекты информационных отношений, автоматизированная система обработки информации, информационная безопасность автоматизированной системы.
2. Базовые свойства защищаемой информации и систем ее обработки. Свойства информации как предмета защиты. Способы нанесения ущерба субъектам информационных отношений.
3. Определение требований к защищаемой информации. Информационные пакеты.
4. Особенности автоматизированной системы (АС) как объекта защиты. Уязвимость основных структурно-функциональных элементов распределенных АС. Понятие угрозы безопасности. Основные виды угроз безопасности субъектов информационных отношений.
5. Классификация угроз безопасности информации, автоматизированных систем и субъектов информационных отношений по различным признакам. Методы перечисления угроз.
6. Основные искусственные угрозы информационной безопасности: преднамеренные и случайные.
7. Классификация каналов проникновения в систему и утечки информации.
8. Неформальная модель нарушителя в автоматизированных системах обработки информации.
9. Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация.
10. Взаимосвязь различных методов обеспечения информационной безопасности, их достоинства и недостатки. Задачи системы информационной безопасности.
11. Основные принципы обеспечения безопасности автоматизированных систем обработки информации.
12. Основные механизмы защиты автоматизированных систем. Термины и определения, касающиеся данного вопроса.
13. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Идентификация и аутентификация.
14. Особенности парольных систем аутентификации.
15. Рекомендации по практической реализации парольных систем аутентификации.
16. Оценка стойкости парольных систем аутентификации. Методы хранения паролей. Передача паролей по сети.
17. Два основных метода разграничения доступа. Понятие модели управления доступом.
18. Типы моделей управления доступом.
19. Криптографические методы обеспечения конфиденциальности информации. Симметричные и ассиметричные криптосистемы. Примеры.
20. Методы обеспечения сетевой безопасности. Межсетевое экранирование. Классы межсетевых экранов.
21. Шифры перестановки: маршрутной перестановки, «Сцитала», «Поворотная решетка».
22. Шифры перестановки: вертикальной перестановки, применение магических квадратов, перестановка бит. Криптостойкость шифров перестановки.
23. Шифры замены. Определение. Шифры простой замены: система шифрования Цезаря, афинная система подстановок, лозунговый шифр.
24. Шифры простой замены: полибианский квадрат, шифрующая таблица Трисемуса, биграммный шифр Плейфера.

25. Шифры сложной замены: система омофонов, шифр Гронсфельда, система шифрования Вижинера, «двойной квадрат» Уитстона.
26. Шифрование методом гаммирования. Достоинства и недостатки метода. Методы генерации псевдослучайных последовательностей чисел. Система шифрования «Одноразовый блокнот».
27. Методы обеспечения сетевой безопасности. Системы обнаружения вторжений.
28. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Протоколирование и аудит.
29. Построение систем защиты от угроз нарушения целостности. Принципы обеспечения целостности (Кларка-Вилсона).
30. Криптографические методы обеспечения целостности информации. Цифровые подписи и порядок их использования.
31. Криптографические методы обеспечения целостности информации. Криптографические хэш-функции. Коды проверки подлинности.
32. Схема системы защиты от угроз нарушения доступности. Дублирование каналов передачи, шлюзов, межсетевых экранов. Методы резервного копирования информации.
33. Схема системы защиты от угроз нарушения доступности. Применение RAID-массивов. Дублирование и зеркалирование серверов. Использование кластеров, избыточной маршрутизации.
34. Механизмы защиты информации в операционных системах.
35. Организационные меры защиты информации в автоматизированных системах. Перечень основных нормативных и организационно-распорядительных документов, необходимых для организации комплексной системы безопасности информации.
36. Основные организационные и организационно-технические мероприятия по созданию и эксплуатации комплексной системы защиты: разовые, периодически проводимые, проводимые по необходимости, постоянные.