Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра вычислительной техники

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки (специальность) 09.03.01 Информатика и вычислительная техника

Квалификация (степень) выпускника – Бакалавр

Профиль (направленность) Вычислительные машины, комплексы, системы и сети

Академический бакалавриат

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки 12.01.2016 г. №5.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

кандидат технических наук, доцент _____ М.Ю. Харитонов

ОБСУЖДЕНО:
на заседании кафедры вычислительной техники 30 августа 2017 г., протокол № 1

заведующий кафедрой _____ А.В. Щипцова

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники 30 августа 2017 г., протокол № 1

Декан факультета _____ А.В. Щипцова

Директор научной библиотеки _____ Н.Д. Никитина

Начальник управления информатизации _____ И.П. Пивоваров

Начальник учебно-методического управления _____ В.И. Маколов

Содержание

1. Цель и задачи обучения по дисциплине

Цель преподавания дисциплины – формирование у студентов знаний об основных направлениях, методах и средствах защиты компьютерной информации и умений выполнять анализ угроз информационной безопасности и выбор способов противодействия выявленным угрозам.

В процессе изучения дисциплины студент должен получить знания, умения и навыки для решения профессиональных задач, связанных с разработкой программного обеспечения средств криптографической и иной защиты информации. Указанные задачи включают в себя:

– анализ угроз информационной безопасности и потенциальных путей утечки конфиденциальной информации;

– выбор методов и средств обеспечения безопасности информации, адекватных выявленным угрозам;

– разработка нового и эффективное применение существующего программного обеспечения для обеспечения информационной безопасности, в комплексе с применением аппаратных, организационных и административно-законодательных средств защиты.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Защита информации» относится к обязательным дисциплинам вариативной части основной образовательной программы подготовки бакалавров направления 09.03.01 «Информатика и вычислительная техника».

Изучение данной дисциплины базируется на следующих курсах:

«Программирование» – знать язык программирования высокого уровня и владеть методиками использования программных средств для решения практических задач;

«Алгебра и геометрия», «Математический анализ», «Теория вероятностей, математическая статистика и случайные процессы» – знать и уметь методы алгебры комплексных чисел, основ дифференциального и интегрального исчисления, теории функций комплексной переменной, дифференциальных уравнений, теории вероятностей и случайных функций;

«Методы вычислений» – проводить сравнительный анализ различных методов вычислительной математики в приложении к решению конкретной задачи по таким параметрам как точность вычислений, объём системных ресурсов, необходимых для решения задачи, и быстродействие.

«Дискретная математика» - знать модулярную арифметику.

Дисциплина является предшествующей для прохождения преддипломной практики и выполнения выпускной квалификационной работы бакалавра.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-5);

способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования (ПК-2).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

– основные угрозы информационной безопасности и пути утечки конфиденциальной информации (З1);

– состав и назначение компонентов криптографической системы (З2);

– принципы построения симметричных и ассиметричных криптографических алгоритмов (З3);

– угрозы, службы и механизмы безопасности в информационно-вычислительных сетях (З4);

– способы противодействия компьютерным вирусам (З5);

– основные принципы обеспечения безопасности в сетевых операционных системах и СУБД (З6);

– структуру, математическую модель и методы стеганографической защиты информации (З7);

– методы защиты речевых сообщений (З8);

– организационные и правовые основы защиты информации (З9);

– организационно-технические меры и мероприятия по обеспечению безопасности информации (З10);

уметь:

– анализировать информационную инфраструктуру (У1);

– выявлять угрозы информационной безопасности и возможные пути утечки конфиденциальной информации (У2);

– принимать адекватные решения при выборе средств защиты информации на основе анализа угроз (У3);

– выбирать и анализировать показатели качества систем и отдельных методов и средств защиты информации (У4);

– разрабатывать программные реализации различных методов криптографической защиты информации (У5);

– выбирать оптимальные методы защиты конфиденциальной информации (У6);

– использовать современные средства обеспечения безопасности информации (У7);

– выполнять анализ информации на предмет наличия в ней скрытых данных (У8);

– разрабатывать программные реализации различных методов стеганографической защиты информации (У9);

– выбирать оптимальные методы защиты речевых сообщений (У10);

владеть навыками:

– анализа информационной инфраструктуры и определения угроз информационной безопасности (Н1);

– выбора средств защиты информации, адекватных выявленным угрозам (Н2);

– разработки средств криптографической защиты информации (Н3);

– разработки средств стеганографической защиты информации (Н4);

– оценки качества применяемых средств защиты информации (Н5).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (лабораторные работы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения и сокращения:

Л – лекции, л/р – лабораторные работы, КСР – контроль самостоятельной работы,

СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль, ЗИ – защита информации.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Основные вопросы обеспечения безопасности информации	ОПК-5	З1, З2, У1, У2, Н1
1.1. Эволюция технологии обеспечения безопасности связи		
1.2. Основные определения и классификация методов и средств ЗИ		
1.3. Основные пути утечки информации и несанкционированного доступа		
1.4. Основные концепции криптографии		
1.5. Управление ключевой системой		
1.6. Теоретическая и практическая стойкость криптоалгоритмов		
Раздел 2. Методы криптографической защиты информации	ОПК-5, ПК-2	З3, У1, У4, У5, Н3, Н5
2.1. Простейшие классические криптоалгоритмы		
2.2. Криптосистема DES		
2.3. Криптоалгоритмы с открытым ключом		
2.4. Критерии оценки качества защиты информации		
Раздел 3. Методы ЗИ в информационно-вычислительных сетях	ОПК-5, ПК-2	З4, З5, З6, У1, У2, У6, У7, Н2
3.1. Угрозы, службы и механизмы безопасности		
3.2. Компьютерные вирусы и вопросы их нейтрализации		
3.3. Защита операционных систем		
3.4. Защита СУБД		
Раздел 4. Стеганографические методы защиты информации	ОПК-5, ПК-2	З7, У1, У6, У8, У9, Н1, Н4
4.1. Основные задачи стеганографии		
4.2. Структура и математическая модель стеганографической системы		
4.3. Классификация стеганографических методов ЗИ		
4.4. Методы, использующие текстовые контейнеры		
4.5. Методы, использующие графические контейнеры		
Раздел 5. Обеспечение безопасности при передачи речевых сообщений	ОПК-5, ПК-2	З8, У1, У7, У10, Н1, Н2
5.1. Аналоговые методы защиты речевых сообщений		
5.2. Цифровые методы защиты речевых сообщений		
Раздел 6. Организационные и правовые вопросы защиты информации	ОПК-5	З9, У1, У2, Н1
6.1. Организационные основы защиты информации		
6.2. Правовые основы защиты информации		
Раздел 7. Рекомендации по обеспечению безопасности информации	ОПК-5	З10, У1, У2, У3, У6, У7, Н1, Н2, Н5
7.1. Практические рекомендации по обеспечению безопасности информации		
7.2. Организационные и организационно-технические мероприятия по обеспечению безопасности информации		
Зачет	ОПК-5, ПК-2	З1, З2, З3, З4, З5, З6, З7, З8, З9, З10, У1, У2, У3, У4, У5, У6, У7, У8, У9, У10, Н1, Н2, Н3, Н4, Н5
Экзамен	ОПК-5, ПК-2	З1, З2, З3, З4, З5, З6, З7, З8, З9, З10, У1, У2, У3, У4, У5, У6, У7, У8, У9, У10, Н1, Н2, Н3, Н4, Н5

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Основные вопросы обеспечения безопасности информации								
1.1. Эволюция технологии обеспечения безопасности связи	3	2				1		
1.2. Основные определения и классификация методов и средств ЗИ	3	2				1		
1.3. Основные концепции криптографии	3	2				1		
1.4. Управление ключевой системой	3	2				1		
1.5. Теоретическая и практическая стойкость криптоалгоритмов	2	1				1		
1.6. Основные пути утечки информации и несанкционированного доступа	2	1				1		
Раздел 2. Методы криптографической защиты информации								
2.1. Простейшие классические криптоалгоритмы	15	2	12			1	12	
2.2. Криптосистема DES	25	4	20			1	20	
2.3. Криптоалгоритмы с открытым ключом	3	2				1		
2.4. Критерии оценки качества защиты информации	3	2				1		
Раздел 3. Методы ЗИ в информационно-вычислительных сетях								
3.1. Угрозы, службы и механизмы безопасности	5	4				1		
3.2. Компьютерные вирусы и вопросы их нейтрализации	3	2				1		
3.3. Защита операционных систем	4	2				2		
3.4. Защита СУБД	4	2				2		
Раздел 4. Стеганографические методы защиты информации								
4.1. Основные задачи стеганографии	4	2				2		
4.2. Структура и математическая модель стеганографической системы	6	2				4		
4.3. Классификация стеганографических методов ЗИ	6	2				4		
4.4. Методы, использующие текстовые контейнеры	15	2	8			5	8	
4.5. Методы, использующие графические контейнеры	6	2				4		
Раздел 5. Обеспечение безопасности при передачи речевых сообщений								
5.1. Аналоговые методы защиты речевых сообщений	5	1				4		
5.2. Цифровые методы защиты речевых сообщений	5	1				4		
Раздел 6. Организационные и правовые вопросы защиты информации								
6.1. Организационные основы защиты информации	6	2				4		
6.2. Правовые основы защиты информации	4	2				2		
Раздел 7. Рекомендации по обеспечению безопасности информации								
7.1. Практические рекомендации по обеспечению безопасности информации	3	1				2		

7.2. Организационные и организационно-технические мероприятия по обеспечению безопасности информации	3	1				2		
Зачет (7 семестр)	6					6		
Зачет (8 семестр)	6				2	4		
Экзамен	27							27
Итого	180, 5 з.е.	48	40		2	63	40	27

5. Содержание разделов дисциплины

5.1. Лекции

Тема 1. Основные вопросы обеспечения безопасности информации.

Лекция 1. Введение. Предмет дисциплины, ее структура и содержание. Связь дисциплины с другими дисциплинами. Эволюция технологии обеспечения безопасности связи (ТОБС). Три фазы развития ТОБС. Проблемы защиты информации в условиях развития сетей. Понятие защищенной системы обработки информации.

Тема 2. Основные определения и классификация методов и средств ЗИ.

Лекция 2. Классификация методов ЗИ. Классификация средств ЗИ. Соотношение методов и средств ЗИ.

Тема 3. Основные концепции криптографии.

Лекция 3. Криптология и её составные части. Криптография и криптоанализ. Задачи криптографии. Задачи криптоанализа. Пассивный электронный перехват. Активный электронный перехват. Шифрование и кодирование. Понятие аутентификации. Виды аутентификации в сетях. Понятие криптосистемы.

Тема 4. Управление ключевой системой

Лекция 4. Задачи центра управления ключевой системой. Вопросы создания, хранения, передачи, смены, уничтожения ключвой информации. Плановая и внеплановая смена ключей. Компрометация ключей.

Тема 5. Вопросы стойкости криптоалгоритмов. Основные пути утечки информации и несанкционированного доступа.

Лекция 5. Теоретическая и практическая стойкость криптоалгоритмов. Основные пути утечки информации и несанкционированного доступа. Активные и пассивные утечки. Умышленный и неумышленный несанкционированный доступ.

Тема 6. Методы криптографической защиты информации. Простейшие классические криптоалгоритмы.

Лекция 6. Классические (симметричные) и новые (асимметричные) криптографические алгоритмы. Понятие открытого и закрытого ключа. Требования к криптоалгоритмам, предназначенным для применения в информационно-вычислительных сетях. Простейшие (базовые) классические криптоалгоритмы: подстановка, перестановка, гаммирование.

Тема 7. Криптосистема DES.

Лекция 7. Понятие о криптосистеме DES. Режимы работы DES. Структура алгоритма шифрования. Функция Фейстеля. S-блоки. Порядок формирования сеансовых ключей. Алгоритм дешифрования. Достоинства и недостатки базового режима DES ECB. Слабые и частично-слабые ключи.

Лекция 8. Альтернативные режимы DES: сцепление блоков шифра DES CBC, режимы с обратной связью по шифртексту DES CFB и по выходу DES OFB. Двойной DES, тройной DES и его варианты. Усиленный вариант DESX. Достоинства и недостатки режимов, сравнительный анализ.

Тема 8. Криптоалгоритмы с открытым ключом.

Лекция 9. Концепции асимметричной криптографии. Взаимосвязь открытого и закрытого ключа. Односторонние (необратимые) функции. Метод Диффи-Хеллмана для

формирования симметричного ключа при использовании незащищенных каналов связи. Криптоалгоритм RSA.

Тема 9. Критерии оценки качества защиты информации.

Лекция 10. Проблемы объективной оценки качества защиты. Критерии оценки. Методика оценки на примере сравнительной оценки симметричной (DES) и асимметричной (RSA) криптосистем.

Тема 10. Методы защиты информации в информационно-вычислительных сетях (ИВС).

Лекция 11. Общая характеристика угроз, служб и механизмов безопасности. Архитектура безопасности МККТТ X.800. Угрозы безопасности, их классификация и характеристика основных угроз.

Лекция 12. Понятие виртуальных и дейтаграммных сетей. Службы безопасности ИВС. Механизмы безопасности ИВС. Взаимосвязь служб и механизмов безопасности. Различия служб и механизмов безопасности для виртуальных и дейтаграммных сетей.

Тема 11. Компьютерные вирусы и вопросы их нейтрализации.

Лекция 13. Общая характеристика и классификация компьютерных вирусов. Различие понятий «вирус» и «троянская программа». Жизненный цикл вируса. Классификация и характеристика антивирусных средств.

Тема 12. Защита операционных систем.

Лекция 14. Защита операционных систем как один из аспектов проблемы защиты ИВС. Активные субъекты и пассивные объекты защиты. Права и возможности доступа. Матрица доступа и способы её свёртки – списки возможностей, списки управления доступом, механизм «замок-ключ». Механизм колец безопасности. Механизмы мандатного и дискреционного управления.

Тема 13. Защита баз данных в ИВС.

Лекция 15. Особенности защиты СУБД как прикладного компонента ОС ИВС. Факторы, определяющие разрешение вопроса о доступе к СУБД. Механизм представлений. Механизм модификации запросов.

Тема 14. Основные задачи стеганографии.

Лекция 16. Введение. Понятие стеганографии. История развития стеганографии и взаимосвязь с критографией. Стеганография в современном мире. Основные задачи компьютерной стеганографии.

Тема 15. Структура и математическая модель стеганографической системы.

Лекция 17. Основные термины и определения стеганографии. Структура обобщенной стеганографической системы. Понятие контейнера. Виды контейнеров. Математическая модель стеганографической системы.

Тема 16. Классификация стеганографических методов ЗИ.

Лекция 18. Классификация стеганографических методов по способу выбора контейнера, по способу доступа к скрываемой информации, по способу организации контейнера, по принципу скрытия информации, по назначению, по форматам контейнеров.

Тема 17. Методы, использующие текстовые контейнеры.

Лекция 19. Использование информационной избыточности. Синтаксические и семантические методы. Метод изменения интервала между предложениями. Метод изменения количества пробелов в конце строк. Использование особенностей форматов.

Тема 18. Методы, использующие графические контейнеры.

Лекция 20. Метод замены наименее значащего бита. Метод псведослучайного интервала. Метод псевдослучайной перестановки. Скрытие данных в частотной области изображения.

Тема 19. Обеспечение безопасности при передаче речевых сообщений.

Лекция 21. Основные принципы связи. Аналоговое скремблирование и дискретизация речи с последующим шифрованием. Тактический и стратегический

уровень закрытия речевых сообщений. Виды аналоговых скремблеров. Классификация цифровых систем закрытия речи. Информационная эффективность цифровой передачи речи.

Тема 20. Организационные основы защиты информации.

Лекция 22. Понятие обеспечения информационной безопасности. Объекты информационной безопасности. Основные задачи, направления и принципы организационной защиты. Основные подходы и требования к организации системы ЗИ. Основные силы и средства, применяемые для организации системы ЗИ.

Тема 21. Правовые основы защиты информации.

Лекция 23. Виды конфиденциальной информации. Правовая защита информации, составляющей коммерческую, налоговую или банковскую тайну. Правовая защита в области компьютерной информации. Правовая защита сведений, составляющих государственную тайну.

Тема 22. Рекомендации по обеспечению безопасности информации.

Лекция 24. Практические рекомендации по обеспечению безопасности информации. Организационные меры защиты общего характера. Организационно-технические мероприятия защиты. Блокирование несанкционированного доступа к информации при помощи технических средств.

5.2. Лабораторные работы

№	Тема	Количество ауд. часов
1	Шифрование данных методом подстановки.	4
2	Шифрование данных методом перестановки.	4
3	Линейное шифрование данных (гаммирование).	4
4	Классический криптоалгоритм DES в режиме ECB.	4
5	Работа алгоритма DES в режиме CBC.	6
6	Работа алгоритма DES в режиме CFB.	4
7	Работа алгоритма DES в режиме OFB.	4
8	Метод изменения интервала между предложениями.	4
9	Метод изменения количества пробелов в конце текстовых строк.	6
	Всего	40

5.3. Вопросы для самостоятельной работы студента в соответствии с содержанием разделов дисциплины

1. Актуальность проблемы защиты хранимой и передаваемой информации.
2. Эволюция технологии обеспечения безопасности передачи информации; три фазы развития ТОБС.
3. Основные определения и классификация методов и средств обеспечения безопасности передачи информации.
4. Основные пути утечки информации и несанкционированного доступа.
5. Два раздела криптологии - криптография и криптоанализ. Основные концепции криптографии.
6. Шифрование данных и проблема аутентификации информации.
7. Управление ключевой системой.
8. Теоретическая и практическая стойкость криптографических алгоритмов. Требования к надежной системе шифрования.
9. Классические криптоалгоритмы и криптоалгоритмы с открытым ключом: общие понятия. Понятие криптографической системы.
10. Основные требования к алгоритмам шифрования, ориентированным на применение в информационно-вычислительных сетях.

11. Блочное и поточное шифрование. Простейшие классические криптоалгоритмы и их недостатки.
12. Криптосистема DES: общие сведения; основные режимы работы, области применения отдельных режимов.
13. Криптоалгоритм DES: работа в режиме ECB. Достоинства и недостатки.
14. Криптоалгоритм DES: работа в режиме CBC. Достоинства и недостатки.
15. Криптоалгоритм DES: работа в режимах CFB и OFB; сравнительный анализ.
16. Развитие криптоалгоритмов семейства DES: двойной и тройной DES, усиленный DES.
17. Криптографические алгоритмы с открытым ключом: общие понятия.
18. Криптосистема Диффи-Хеллмана.
19. Криптосистема RSA.
20. Критерии оценки качества защиты передаваемой информации. Сравнительный анализ DES и RSA.
21. Перспективы развития криптосистем. Гибридные криптосистемы.
22. Классификация угроз безопасности. Основные угрозы безопасности.
23. Службы безопасности виртуальных и дейтаграммных сетей.
24. Механизмы безопасности.
25. Общая характеристика и классификация компьютерных вирусов.
26. Средства нейтрализации компьютерных вирусов.
27. Общие вопросы защиты операционных систем. Пассивные объекты защиты и активные субъекты ОС.
28. Защита операционной системы с помощью матрицы доступа. Средства сокращения объема матрицы доступа.
29. Общие вопросы обеспечения безопасности баз данных в ИВС.
30. Механизмы обеспечения безопасности баз данных в ИВС.
31. Обеспечение безопасности при передаче речевых сообщений: основные принципы связи; полосы и каналы.
32. Основные методы закрытия речевых сигналов в телефонных каналах.
33. Тактический и стратегический уровень закрытия речевых сигналов. Сравнительный анализ методов закрытия речи.
34. Принципы аналогового скремблирования.
35. Частотное скремблирование.
36. Временное и комбинированное скремблирование.
37. Структура обобщенной системы цифрового закрытия речи. Информационная эффективность цифровой передачи.
38. Классификация систем цифрового закрытия речи по способу описания речевого сообщения.
39. Полосный вокодер. Недостатки вокодерных систем.
40. Организационные мероприятия ТОБС.
41. Организационно-технические мероприятия ТОБС.
42. Понятие стеганографии; её роль и место в общей системе защиты информации.
43. Основные задачи стеганографии.
44. Структура обобщенной стеганографической системы. Основные термины и понятия.
45. Математическая модель стеганографической системы. Надежная стеганосистема.
46. Классификация стеганографических методов.
47. Стеганографические методы, использующие текстовые контейнеры: Семантические и синтаксические методы.
48. Стеганографические методы, использующие текстовые контейнеры: Методы произвольного интервала.

49. Стеганографические методы, использующие текстовые контейнеры: Методы, основанные на использовании особенностей формата текста.
50. Стеганографические методы, использующие контейнеры-изображения: общие сведения.
51. Стеганографические методы, использующие контейнеры-изображения: Метод замены наименее значащего бита.
52. Стеганографические методы, использующие контейнеры-изображения: Метод псевдослучайного интервала.
53. Стеганографические методы, использующие контейнеры-изображения: Метод псевдослучайной перестановки.
54. Стеганографические методы, использующие контейнеры-изображения: Методы скрытия в частотной области.
55. Понятие информационной безопасности. Обеспечение информационной безопасности.
56. Основные задачи, направления и принципы организационной защиты информации.
57. Основные подходы и требования к организации системы защиты информации.
58. Силы и средства для организации защиты информации.
59. Правовые основы защиты информации: основные понятия. Виды конфиденциальной информации.
60. Правовая защита информации, составляющей государственную тайну.
61. Правовая защита информации, составляющей коммерческую тайну.
62. Правовая защита в области компьютерной информации.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- диагностики;
- целеполагания;
- управления процессом освоения учебной информации;
- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.);
- контроля качества и оценивания результатов образовательной деятельности.

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (проектор, экран) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его

непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ, аннотирование и конспектирование литературы по теме, подготовка к лабораторным работам, подготовка реферативных сообщений, и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на экзамене и зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета (7 семестр) и экзамена и зачета (8 семестр). Принимаются экзамен и зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся:

7.1. Вопросы к зачету (7 семестр)

1. Теоретическая и практическая стойкость криптографических алгоритмов.
2. Классические криптоалгоритмы и криптоалгоритмы с открытым ключом: общие понятия. Понятие криптографической системы.
3. Основные требования к алгоритмам шифрования, ориентированным на применение в информационно-вычислительных сетях.
4. Блочное и поточное шифрование. Простейшие классические криптоалгоритмы и их недостатки.
5. Криптосистема DES: общие сведения; основные режимы работы, области применения отдельных режимов.
6. Криптоалгоритм DES: работа в режиме ECB. Достоинства и недостатки.

7.2. Вопросы к зачету (8 семестр)

1. Криптоалгоритм DES: работа в режиме CBC. Достоинства и недостатки.
2. Криптоалгоритм DES: работа в режимах CFB и OFB; сравнительный анализ.
3. Развитие криптоалгоритмов семейства DES: двойной и тройной DES, усиленный DES.
4. Криптографические алгоритмы с открытым ключом: общие понятия.
5. Понятие стеганографии; её роль и место в общей системе защиты информации.
6. Основные задачи стеганографии.
7. Структура обобщенной стеганографической системы. Основные термины и понятия.
8. Математическая модель стеганографической системы. Надежная стеганосистема.
9. Классификация стеганографических методов.
10. Стеганографические методы, использующие текстовые контейнеры: Семантические и синтаксические методы.
11. Стеганографические методы, использующие текстовые контейнеры: Методы произвольного интервала.
12. Стеганографические методы, использующие текстовые контейнеры: Методы, основанные на использовании особенностей формата текста.

7.3. Вопросы к экзамену (8 семестр)

1. Актуальность проблемы защиты хранимой и передаваемой информации.

2. Эволюция технологии обеспечения безопасности передачи информации; три фазы развития ТОБС.
3. Основные определения и классификация методов и средств обеспечения безопасности передачи информации.
4. Основные пути утечки информации и несанкционированного доступа.
5. Два раздела криптологии - криптография и криптоанализ. Основные концепции криптографии.
6. Шифрование данных и проблема аутентификации информации.
7. Управление ключевой системой.
8. Теоретическая и практическая стойкость криптографических алгоритмов. Требования к надежной системе шифрования.
9. Классические криптоалгоритмы и криптоалгоритмы с открытым ключом: общие понятия. Понятие криптографической системы.
10. Основные требования к алгоритмам шифрования, ориентированным на применение в информационно-вычислительных сетях.
11. Блочное и поточное шифрование. Простейшие классические криптоалгоритмы и их недостатки.
12. Криптосистема DES: общие сведения; основные режимы работы, области применения отдельных режимов.
13. Криптоалгоритм DES: работа в режиме ECB. Достоинства и недостатки.
14. Криптоалгоритм DES: работа в режиме CBC. Достоинства и недостатки.
15. Криптоалгоритм DES: работа в режимах CFB и OFB; сравнительный анализ.
16. Развитие криптоалгоритмов семейства DES: двойной и тройной DES, усиленный DES.
17. Криптографические алгоритмы с открытым ключом: общие понятия.
18. Криптосистема Диффи-Хеллмана.
19. Криптосистема RSA.
20. Критерии оценки качества защиты передаваемой информации. Сравнительный анализ DES и RSA.
21. Перспективы развития криптосистем. Гибридные криптосистемы.
22. Классификация угроз безопасности. Основные угрозы безопасности.
23. Службы безопасности виртуальных и дейтаграммных сетей.
24. Механизмы безопасности.
25. Общая характеристика и классификация компьютерных вирусов.
26. Средства нейтрализации компьютерных вирусов.
27. Общие вопросы защиты операционных систем. Пассивные объекты защиты и активные субъекты ОС.
28. Защита операционной системы с помощью матрицы доступа. Средства сокращения объема матрицы доступа.
29. Общие вопросы обеспечения безопасности баз данных в ИВС.
30. Механизмы обеспечения безопасности баз данных в ИВС.
31. Обеспечение безопасности при передаче речевых сообщений: основные принципы связи; полосы и каналы.
32. Основные методы закрытия речевых сигналов в телефонных каналах.
33. Тактический и стратегический уровень закрытия речевых сигналов. Сравнительный анализ методов закрытия речи.
34. Принципы аналогового скремблирования.
35. Частотное скремблирование.
36. Временное и комбинированное скремблирование.
37. Структура обобщенной системы цифрового закрытия речи. Информационная эффективность цифровой передачи.

38. Классификация систем цифрового закрытия речи по способу описания речевого сообщения.
39. Полосный вокодер. Недостатки вокодерных систем.
40. Организационные мероприятия ТОБС.
41. Организационно-технические мероприятия ТОБС.
42. Понятие стеганографии; её роль и место в общей системе защиты информации.
43. Основные задачи стеганографии.
44. Структура обобщенной стеганографической системы. Основные термины и понятия.
45. Математическая модель стеганографической системы. Надежная стеганосистема.
46. Классификация стеганографических методов.
47. Стеганографические методы, использующие текстовые контейнеры: Семантические и синтаксические методы.
48. Стеганографические методы, использующие текстовые контейнеры: Методы произвольного интервала.
49. Стеганографические методы, использующие текстовые контейнеры: Методы, основанные на использовании особенностей формата текста.
50. Стеганографические методы, использующие контейнеры-изображения: общие сведения.
51. Стеганографические методы, использующие контейнеры-изображения: Метод замены наименее значащего бита.
52. Стеганографические методы, использующие контейнеры-изображения: Метод псевдослучайного интервала.
53. Стеганографические методы, использующие контейнеры-изображения: Метод псевдослучайной перестановки.
54. Стеганографические методы, использующие контейнеры-изображения: Методы скрытия в частотной области.
55. Понятие информационной безопасности. Обеспечение информационной безопасности.
56. Основные задачи, направления и принципы организационной защиты информации.
57. Основные подходы и требования к организации системы защиты информации.
58. Силы и средства для организации защиты информации.
59. Правовые основы защиты информации: основные понятия. Виды конфиденциальной информации.
60. Правовая защита информации, составляющей государственную тайну.
61. Правовая защита информации, составляющей коммерческую тайну.
62. Правовая защита в области компьютерной информации.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература (ежегодное обновление перечня и условия доступа представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2017. — 473 с. Режим доступа: www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-

	28E7FA40632A.
2.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. Режим доступа: http://www.iprbookshop.ru/30928.html
3.	Торокин А. А. Инженерно-техническая защита информации: [учебное пособие для вузов по специальостям в области информационной безопасности] / Торокин А. А. - Москва: Гелиос АРВ, 2005. - 959с.. - ISBN 5-85438-140-0.

8.2. Рекомендуемая дополнительная литература (ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Шумский А. А. Системный анализ в защите информации: [учебное пособие для вузов по специальностям в области информационной безопасности] / Шумский А. А., Шелупанов А. А. - Москва: Гелиос АРВ, 2005. - 221с.. - ISBN 5-85438-128-1.
2.	Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: [учебное пособие для вузов] / Тихонов В. А., Райх В. В. - М.: Гелиос АРВ, 2006. - 527с.: ил.. - ISBN 5-85438-153-2.

8.3. Рекомендуемые методические разработки по дисциплине (ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№ п/п	Наименование	Условия доступа
1.	Защита информации: метод. указания к лабораторным работам	URL: http://moodle.chuvsu.ru/course/index.php?categoryid=157

8.4. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.4.1. Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community

8.4.2. Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.5. Рекомендуемые интернет-ресурсы и открытые он-лайн курсы

№ п/п	Наименование интернет ресурса	Режим доступа
1.	Российская Государственная Библиотека	http://www.rsl.ru
2.	Государственная публичная научно-техническая	http://www.gpntb.ru

	библиотека России	
3.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
4.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
5.	Научная электронная библиотека	http://elibrary.ru
6.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
7.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением;

– настенный экран.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. Основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Форма организации студентов на лабораторных работах: фронтально-индивидуальная. Все студенты выполняют одновременно одну и ту же работу по индивидуальному заданию в соответствии с порядковым номером студента в списке группы.

В результате выполнения лабораторной работы запланирована подготовка письменного отчета в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.