МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета информационных технологий и компьютерной безопасности
_____ / П.Ю. Гусев /
подпись *И.О. Фамилия*
«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Защита информации»

наименование дисциплины (модуля) в соответствии с учебным планом)

Направление подготовки (специальность) 09.03.01 Информатика и вычислительная техника
код и наименование направления подготовки/специальности

Профиль (специализация) Вычислительные машины, комплексы, системы и сети
название профиля/программы

Квалификация выпускника **бакалавр**

Нормативный период обучения **4 года / 4 года и 11 мес.**
Очная/очно-заочная/заочная (при наличии)

Форма обучения Очная / Заочная

Год начала подготовки 2019 г.

Автор(ы) программы _____ Т.И. Сергеева
подпись

Заведующий кафедрой автоматизированных и вычислительных систем _____ В.Ф. Барабанов
подпись

Руководитель ОПОП _____ С.Л. Подвальный
подпись

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Изучение и практическое освоение основных методов и средств защиты компьютерной информации.

1.2. Задачи освоения дисциплины

К теоретическим задачам относятся ознакомление с основными угрозами компьютерной безопасности, стандартами безопасности, особенностями реализации политики безопасности, криптографическими моделями и алгоритмами шифрования; ознакомление с технологиями защиты информации в сетях, с требованиями к системам защиты информации.

Прикладные задачи состоят в приобретении навыков организации защиты компьютерной информации, в практическом освоении алгоритмов и программ шифрования данных, технологий защиты информации в сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Защита информации» направлен на формирование следующих компетенций:

ПК-2 - Способен проектировать и разрабатывать компоненты программных комплексов и информационных систем, используя современные технологии программирования и инструментальные средства разработки

ПК-8 - Способен администрировать программное обеспечение инфокоммуникационных систем

Компетенция	**Результаты обучения, характеризующие сформированность компетенции** (в РП)
ПК-2	Знать: - криптографические методы защиты информации; - основные алгоритмы реализации симметричных и асимметричных систем шифрования; - алгоритмы формирования электронной подписи.
	Уметь: - проектировать и разрабатывать программы шифрования сообщений, используя алгоритмы замены и перестановки.
	Владеть: - методами и средствами проектирования и разработки программного обеспечения симметричных и асимметричных криптосистем.

ПК-8	Знать: - основные угрозы компьютерной безопасности; - методы защиты информации; - стандарты информационной безопасности; - программные средства защиты информации; - принципы установки и настройки программного обеспечения для защиты информации.
	Уметь: - устанавливать программно-аппаратные средства инфокоммуникационной системы и/или ее составляющих, обеспечивающие защиту информации.
	Владеть: - методиками управления программным обеспечением инфокоммуникационной системы с целью защиты информации.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	18	18
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	54	54
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	16	16
В том числе:		
Лекции	4	4
Лабораторные работы (ЛР)	12	12
Самостоятельная работа	88	88
Контрольная работа	+	+
Часы на контроль	4	4
Виды промежуточной аттестации - зачет	+	+

Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение в защиту информации	**Введение в основы защиты информации** Основные направления защиты информации. Информация как предмет защиты. Основные понятия и определения. **Угрозы и нарушители компьютерной безопасности** Основные угрозы компьютерной безопасности. Модель потенциального нарушителя. **Классификация методов и средств защиты данных** Основные определения. Методы защиты данных. Классификация средств защиты данных. Организационные средства защиты данных. Законодательные средства защиты данных. Физические средства защиты данных. Аппаратные и программные средства защиты данных. **Стандарты информационной безопасности** Требования к комплексным системам защиты информации. Стандарты безопасности компьютерных систем. Государственные стандарты РФ по защите информации.	6	4	18	28
2	Криптографическая защита информации	**Криптографические методы защиты информации** Основные определения. Принципы криптографической обработки данных. Принципы построения симметричных криптосистем. Классические разновидности шифров. Шифры замены, шифры перестановки. **Криптографическая система DES** Схема шифрования DES. Режимы реализации алгоритма DES: «Элек-	10	16	30	56

		тронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру», «Обратная связь по выходу». **Отечественный стандарт шифрования данных** Режимы реализации симметричного отечественного стандарта. **Асимметричные криптосистемы** Принцип построения асимметричных криптосистем шифрования. Открытый и секретный ключи. Однонаправленные функции. Криптоконцепция Диффи-Хеллмана. Криптозащита Меркля-Хеллмана. Криптосистема шифрования данных RSA. **Алгоритмы формирования электронной цифровой подписи** Однонаправленные хэш-функции. Практические методы построения хэш-функций. Современные алгоритмы хеширования. Отечественные стандарты формирования электронной цифровой подписи.				
3	Защита информации в локальных сетях	**Организация защиты информации в локальных сетях**. Методы и средства программного и аппаратного обеспечения защиты информации.	2	16	6	24
		Итого	**18**	**36**	**54**	**108**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение в защиту информации	**Введение в основы защиты информации** Основные направления защиты информации. Информация как предмет защиты. Основные понятия и определения. **Угрозы и нарушители компьютерной безопасности** Основные угрозы компьютерной безопасности. Модель потенциального нарушителя. **Классификация методов и средств защиты данных** Основные определения. Методы защиты данных. Классификация средств защиты	2	4	30	36

		данных. Организационные средства защиты данных. Законодательные средства защиты данных. Физические средства защиты данных. Аппаратные и программные средства защиты данных. **Стандарты информационной безопасности** Требования к комплексным системам защиты информации. Стандарты безопасности компьютерных систем. Государственные стандарты РФ по защите информации.				
2	Криптографическая защита информации	**Криптографические методы защиты информации** Основные определения. Принципы криптографической обработки данных. Принципы построения симметричных криптосистем. Классические разновидности шифров. Шифры замены, шифры перестановки. **Криптографическая система DES** Схема шифрования DES. Режимы реализации алгоритма DES: «Электронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру», «Обратная связь по выходу». **Отечественный стандарт шифрования данных** Режимы реализации симметричного отечественного стандарта. **Асимметричные криптосистемы** Принцип построения асимметричных криптосистем шифрования. Открытый и секретный ключи. Однонаправленные функции. Криптоконцепция Диффи-Хеллмана. Криптозащита Меркля-Хеллмана. Криптосистема шифрования данных RSA. **Алгоритмы формирования электронной цифровой подписи** Однонаправленные хэш-функции. Практические методы построения хэш-функций. Современные алгоритмы хеширования. Отечественные стандарты формирования электронной цифровой подписи.	2	4	30	36
3	Защита информации в локальных	**Организация защиты информации в локальных сетях**.	-	4	28	32

	сетях	Методы и средства программного и аппаратного обеспечения защиты информации.				
		Итого	**4**	**12**	**88**	**104**

5.2 Перечень лабораторных работ

Перечень лабораторных работ для очного обучения

Лабораторная работа № 1. Реализация программных генераторов паролей

Лабораторная работа № 2. Программная реализация алгоритмов шифрования, основанных на методах замены

Лабораторная работа № 3. Программная реализация алгоритмов шифрования, основанных на методах перестановки

Лабораторная работа № 4. Изучение стандартных программ шифрования с применением алгоритма DES

Лабораторная работа № 5. Изучение существующих программ шифрования электронных сообщений и формирования электронных цифровых подписей

Лабораторная работа № 6. Программные средства обеспечения информационной безопасности

Лабораторная работа № 7. Настройка и администрирование операционных систем для обеспечения информационной безопасности компьютерных систем

Лабораторная работа № 8. Настройка и конфигурирование FireWall на примере бесплатно распространяемой версии

Лабораторная работа № 9. Настройка сетевых элементов инфокоммуникационной системы для обеспечения защиты информации

Перечень лабораторных работ для заочного обучения

Лабораторная работа № 1. Реализация программных генераторов паролей

Лабораторная работа № 2. Программная реализация алгоритмов шифрования, основанных на методах замены

Лабораторная работа № 3. Настройка и конфигурирование FireWall на примере бесплатно распространяемой версии

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы).

В соответствии с учебным планом освоения дисциплины на заочном обучении предусматривается выполнение контрольной работы в 9-ом семестре.

Контрольная работа состоит из двух частей: теоретическая часть и

практическая часть.

Теоретическая часть включает по одному теоретическому вопросу из трех разделов учебной дисциплины.

Практическая часть включает реализацию двух программ по шифрованию сообщений с применением методов замены и перестановки.

Методические рекомендации по выполнению контрольной работы имеются в электронном виде и выложены на сетевом диске кафедры. Выбор вариантов контрольных заданий осуществляется по таблице, указанной в методических рекомендациях, и по номеру зачетной книжки.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	Знать: - криптографические методы защиты информации; - основные алгоритмы реализации симметричных и асимметричных систем шифрования; - алгоритмы формирования электронной подписи.	Тест	Выполнение теста на 60-100 %	Выполнение теста менее 60 %
	Уметь: - проектировать и разрабатывать программы шифрования сообщений, используя алгоритмы замены и перестановки.	Решение стандартных практических задач	Выполнение лабораторных работ № 1-5 (контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - методами и средствами проектирования и разработки программного обеспечения симметричных и асимметричных криптосистем.	Решение стандартных практических задач	Выполнение лабораторных работ № 1-5 (контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-8	Знать: - основные угрозы ком-	Тест	Выполнение теста на 60-100 %	Выполнение теста менее 60 %

	пьютерной безопасности; - методы защиты информации; - стандарты информационной безопасности; - программные средства защиты информации; - принципы установки и настройки программного обеспечения для защиты информации.			
	Уметь: устанавливать программно-аппаратные средства инфокоммуникационной системы и/или ее составляющих, обеспечивающие защиту информации.	Решение стандартных практических задач	Выполнение лабораторных работ № 6-9 (№ 1-2 для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ в срок, предусмотренный в рабочих программах
	Владеть: методиками управления программным обеспечением инфокоммуникационной системы с целью защиты информации.	Решение стандартных практических задач	Выполнение лабораторных работ № 6-9 (№ 1-2 для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7 семестре для очной формы обучения, 9 семестре для заочной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Зачтено**	**Не зачтено**
ПК-2	Знать: - криптографические методы защиты информации; - основные алгоритмы реализации симметричных и асимметричных систем шифрования; - алгоритмы формирования электронной подписи.	Тест	Выполнение теста на 60 – 100 %	Выполнение теста менее 60 %
	Уметь: - проектировать и разрабатывать программы шифрования сообщений, используя алгоритмы замены и перестановки	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - методами и средствами	Решение прикладных задач в конкретной предметной	Продемонстрирован верный ход решения	Задачи не решены

	проектирования и разработки программного обеспечения симметричных и асимметричных криптосистем.	области	в большинстве задач	
ПК-8	Знать: - основные угрозы компьютерной безопасности; - методы защиты информации; - стандарты информационной безопасности; - программные средства защиты информации; - принципы установки и настройки программного обеспечения для защиты информации.	Тест	Выполнение теста на 60 – 100 %	Выполнение теста менее 60 %
	Уметь: устанавливать программно-аппаратные средства инфокоммуникационной системы и/или ее составляющих, обеспечивающие защиту информации.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: методиками управления программным обеспечением инфокоммуникационной системы с целью защиты информации.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Укажите правильный ответ

… является предметом собственности и подлежит защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации.

а) Правовая информация
б) Конфиденциальная информация
в) Защищаемая информация

Ответ в

2. Укажите правильный ответ

… - это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации.

а) Уровень секретности
б) Политика безопасности
в) Законодательные средства защиты

Ответ а

3. Укажите правильный ответ

… - это деятельность по предотвращению утечки информации, несанкциониро-

ванных и непреднамеренных воздействий на защищаемую информацию.

а) Политика безопасности
б) Защита информации
в) Организационные средства защиты

Ответ б

4. Укажите правильный ответ

… - это неконтролируемое распространение защищаемой информации.

а) Разглашение
б) Несанкционированный доступ
в) Утечка

Ответ в

5. Укажите правильный ответ

… - это ситуация, когда защищаемая информация становится известной лицу, которое не должно иметь к ней доступ.

а) Угроза нарушения конфиденциальности
б) Угроза нарушения целостности
в) Угроза нарушения работоспособности

Ответ а

6. Укажите правильный ответ

… - это ситуация, когда происходит изменение или искажение защищаемой информации, приводящее к нарушению ее качества или полному уничтожению.

а) Угроза нарушения конфиденциальности
б) Угроза нарушения целостности
в) Угроза нарушения работоспособности

Ответ б

7. Укажите правильный ответ

… - это ситуация, когда происходит снижение скорости работы вычислительной системы, либо ее ресурсы становятся недоступными.

а) Угроза нарушения конфиденциальности
б) Угроза нарушения целостности
в) Угроза нарушения работоспособности

Ответ в

8. Укажите правильный ответ

Угрозы нарушения конфиденциальности, целостности и работоспособности – это …

а) Угрозы по предмету направленности
б) Угрозы по источнику возникновения
в) Каналы утечки
г) Воздействия

Ответ а

9. Укажите правильный ответ

Воздействия и каналы утечки – это ..

а) Угрозы по предмету направленности
б) Угрозы по источнику возникновения
в) Угрозы нарушения целостности информации

Ответ б

10. Укажите правильный ответ

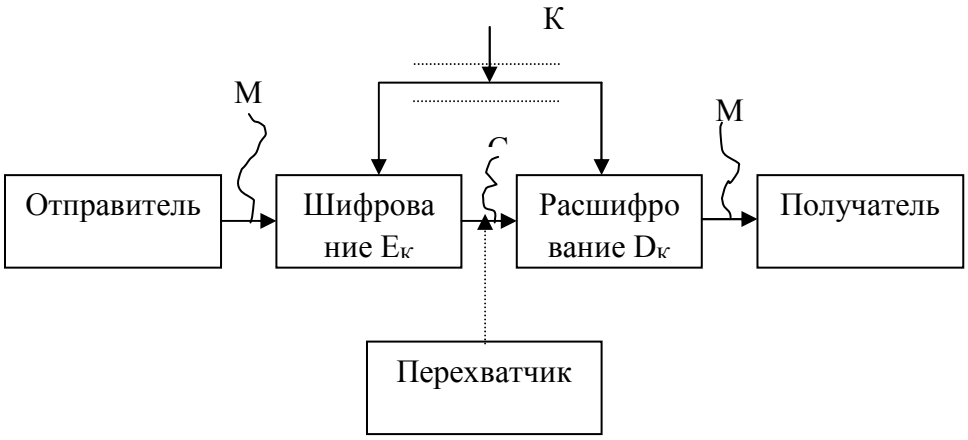
… - воздействия природной среды (ураган, землетрясение, пожар, наводнение и т.п.).

а) Случайные воздействия
б) Природные воздействия
в) Целенаправленные воздействия
г) Внутрисистемные воздействия

Ответ а

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Представлена схема криптосистемы

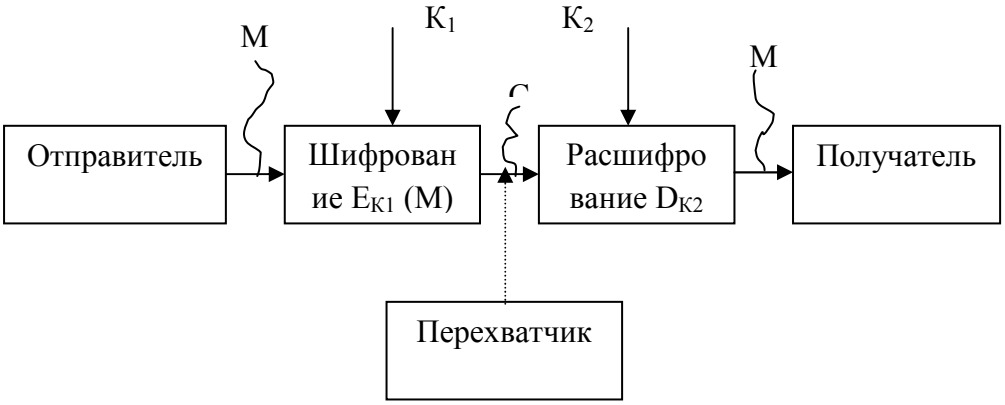


Данная схема является:

а) обобщенной схемой симметричной криптосистемы с одним ключом;
б) обобщенной схемой асимметричной криптосистемы с двумя ключами;
в) обобщенной схемой любой криптосистемы.

Ответ а

2. Представлена схема криптосистемы



Данная схема является:

а) обобщенной схемой симметричной криптосистемы с закрытым ключом;
б) обобщенной схемой асимметричной криптосистемы;
в) обобщенной схемой любой криптосистемы.

Ответ б

3. Дана формула замены

$$Yi=k1*Xi+k2(mod\ N)$$

где Yi - i-й символ алфавита шифротекста (номер буквы в алфавите);
k1 и k2 - константы;
Xi - i-й символ открытого текста (номер буквы в алфавите);
N - длина используемого алфавита.

Данная формула реализует:

а) Гомофоническую замену;

б) Моноалфавитную замену;
в) Полиалфавитную замену;
г) Полиграммную замену.
Ответ б

4. Шифр, задаваемый формулой:
yi=xi+ki(mod N),
где ki - i-ая буква ключа, в качестве которого используются слово или фраза, называется
а) шифром Вижинера;
б) шифром Бофора;
в) шифром Плейфера.
Ответ а

5. Шифр, задаваемый формулой:
yi=ki-xi(mod n) и
yi=xi-ki(mod n).
называется
а) шифром Вижинера;
б) шифром Бофора;
в) шифром Плейфера.
Ответ б

6. … означает, что одному символу открытого текста ставит в соответствие несколько символов шифротекста. Этот метод применяется для искажения статистических свойств шифротекста.
а) Моноалфавитная замена;
б) Гомофоническая замена;
в) Полиалфавитная замена.
Ответ б

7. … использует несколько алфавитов шифртекста.
Пусть используется k алфавитов. Тогда открытый текст: $X=X_1X_2...X_k \quad X_{k+1}...X_{2k} \quad X_{2k+1}...$ заменяется шифртекстом:
$Y=F1(X1)F2(X2)...Fk(Xk) \quad F1(Xk+1)...Fk(X2k) \quad F1(X2k+1)...$
где Fi(Xj) означает символ шифртекста алфавита i для символа открытого текста Xj.
а) Гомофоническая замена;
б) Полиалфавитная замена;
в) Моноалфавитная замена.
Ответ б

8. … формируется из одного алфавита с помощью специальных правил.
В качестве примера рассмотрим шифр Плэйфера.
В этом шифре алфавит располагается в матрице. Открытый текст разбивается на пары символов X_iX_{i+1}. Каждая пара символов открытого текста заменяется на пару символов из матрицы следующим образом:
1) если символы находятся в одной строке, то каждый из символов пары заменяется на стоящий правее его (за последним символом в строке следует первый);

2) если символы находятся в одном столбце, то каждый символ пары заменяется на символ, расположенный ниже его в столбце (за последним нижним символом следует верхний);

3) если символы пары находятся в разных строках и столбцах, то они считаются противоположными углами прямоугольника. Символ, находящийся в левом углу, заменяется на символ, стоящий в другом левом углу; замена символа, находящегося в правом углу, осуществляется аналогично;

4) если в открытом тексте встречаются два одинаковых символа подряд, то перед шифрованием между шали вставляется специальный символ (например, тире).

а) Полиалфавитная замена;
б) Полиграммная замена;
в) Гомофоническая замена.

Ответ б

9. … использует преобразование вида:

Y=CX.

где $Y=||y_1,y_2, ...,y_n||^T$.

$C=||C_{ij}||$

$X=||x_1,x_2, ...,x_n||$

а) Решение задачи об укладке ранца;
б) Вычисление значения полинома по модулю;
в) Метод умножения матриц.

Ответ в

10. … формулируется следующим образом.

Задан вектор $C=|c_1,c_2,...,c_n|$, который используется для шифрования сообщения, каждый символ s_i которого представлен последовательностью из n бит $s_i=|x_1,x_2,...,x_n|$, $x_k \in \{0,1\}$. Шифротекст получается как скалярное произведение $C \cdot s_i$.

а) Задача об укладке ранца;
б) Задача умножения матриц;
в) Задача вычисления значения полинома по модулю.

Ответ а

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Написать и отладить программу генерации пароля в соответствии с вариантом задания:
   - количество символов в пароле 6;
   - b1,Ь2 - случайные цифры;
   - b3 = N2 mod 10 (где mod 10 - остаток от деления числа на 10);
   - b4 - случайный символ из идентификатора пользователя;
   - b5 - случайный символ из множества {!,",#,$,%,&,',(,),*};
   - b6 - случайная малая буква английского алфавита.

2. Написать и отладить программу генерации пароля в соответствии с вариантом задания:
   - количество символов в пароле 6;
   - b1 – случайный символ из идентификатора пользователя;
   - b2– случайная малая буква английского алфавита;

- b3, b4 – случайные цифры;
- b5, b6 - случайный символ из множества {!,",#,$,%,&,',(,),*}.

3. Написать и отладить программу генерации пароля в соответствии с вариантом задания:
   - количество символов в пароле 7;
   - b1, b2 - случайные малые буквы английского алфавита;
   - b3, b4 – случайные символы из идентификатора пользователя;
   - b5, b6 - случайные заглавные буквы английского алфавита;
   - b7 - число, равное N^4 mod 10.

4. Написать и отладить программу расшифрования открытого сообщения в соответствии с вариантом задания: реализовать шифрование и расшифровку методом перестановки. Ключ 5 4 2 1 3.

5. Написать и отладить программу расшифрования открытого сообщения в соответствии с вариантом задания: реализовать шифрование и расшифровку методом перестановки. Ключ 3 4 2 1 5.

6. Написать и отладить программу расшифрования открытого сообщения в соответствии с вариантом задания: реализовать шифрование и расшифровку методом перестановки. Ключ 3 7 2 5 4 1 6.

7. Написать и отладить программу шифрования и расшифровки сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 5 символов вправо.

8. Написать и отладить программу шифрования и расшифровки сообщения методом полиалфавитной подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Первый символ шифруют из первого алфавита шифротекста, второй символ – из второго алфавита шифротекста, третий символ – снова из первого алфавита шифротекста и т.д.

9. Написать и отладить программу шифрования и расшифровки сообщения методом полиалфавитной подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен четырем, то для замены выбирать символ из первого алфавита шифротекста, в противном случае – для замены выбирать символ из второго алфавита шифротекста.

10. Написать и отладить программу шифрования и расшифровки со-

общения с применением шифра Вижинера. Ключом выбрать Ваше имя. Реализовать также расшифровку шифротекста.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Информация как предмет защиты, конфиденциальная информация, защищаемая информация, уровень секретности, защита информации.
2. Определения: безопасность информации, целостность информации, конфиденциальность информации.
3. Определения: угроза безопасности информации, несанкционированный доступ к информации, политика безопасности.
4. Основные угрозы информации по предмету направленности, по источнику возникновения.
5. Виды воздействий, реализующие угрозу безопасности данных.
6. Косвенные и прямые каналы утечки данных.
7. Модель потенциального нарушителя.
8. Определения: методы защиты, средства защиты, механизмы защиты.
9. Основные методы защиты данных.
10. Классификация средств защиты.
11. Физические средства защиты данных.
12. Законодательные средства защиты компьютерной информации.
13. Организационные средства защиты компьютерной информации.
14. Аппаратные средства защиты.
15. Программные средства защиты компьютерной информации.
16. Требования к комплексным системам защиты компьютерной информации.
17. Стандарты безопасности КС.
18. Обобщенная схема симметричной криптосистемы.
19. Обобщенная схема асимметричной криптосистемы.
20. Шифрование методом моноалфавитнойой замены.
21. Шифрование методом полиалфавитной замены.
22. Шифрование методом гомофонической замены.
23. Шифрование с использованием методов гаммирования.
24. Шифрование методом перестановки.
25. Шифрование методом полиграммной замены.
26. Шифрование данных с использованием алгоритма DES.
27. Режим работы алгоритма DES: электронная кодовая книга.
28. Режим работы алгоритма DES: сцепление блоков шифра.
29. Режим работы алгоритма DES:обратная связь по шифру.
30. Режим работы алгоритма DES: обратная связь по выходу.
31. Отечественный стандарт шифрования: шифрование данных в режиме простой замены.
32. Отечественный стандарт шифрования: шифрование данных в режиме гаммирования.
33. Отечественный стандарт шифрования: шифрование данных в режиме

гаммирования с обратной связью.

34. Отечественный стандарт шифрования: выработка имитовставки.
35. Процедуры шифрования и расшифрования в криптосистеме RSA.
36. Электронная цифровая подпись (ЭЦП). Алгоритмы формирования ЭЦП.
37. Стандарт цифровой подписи ГОСТ Р34.10-94.

7.2.5 Примерный перечень вопросов для подготовки к экзамену

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по билетам, включающим по два вопроса. Допуском к зачету является выполнение всех лабораторных работ и положительное текущее тестирование по темам лекций первого и второго разделов.

Зачет ставится, если студент выполнил все лабораторные работы, прошел тестирование по темам первого и второго разделов теоретического материала и ответил на один или два вопроса, изложив основные положения вопроса.

Зачет не ставится, если студент не ответил ни на один вопрос.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в защиту информации	ПК-2, ПК-8	Тест, контрольная работа (для заочников), защита лабораторных работ, зачет, устный опрос
2	Криптографическая защита информации	ПК-2, ПК-8	Тест, контрольная работа (для заочников), защита лабораторных работ, зачет, устный опрос
3	Защита информации в локальных сетях	ПК-2, ПК-8	Защита лабораторных работ, зачет, устный опрос

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется по теоретическому материалу, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 45 мин. Затем осуществляется проверка теста преподавателем. Тест пройден, если количество правильных ответов составляет 60 – 100 %.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на

бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач преподавателем. Тест пройден, если количество правильных ответов составляет 60 – 100 %.

Решение прикладных задач осуществляется на лабораторных работах. Разработанная программа должна отвечать заданным требованиям. Время выполнения лабораторной работы составляет 4 часа.

Зачет сдается по билетам из двух вопросов. Допуском к зачету является выполнение всех лабораторных работ и положительное текущее тестирование по темам лекций первого и второго разделов.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Мельников В.П. Информационная безопасность : учеб. пособие / под ред. С. А. Клейменова. - 8-е изд., испр. - М.: Академия, 2013.

2. Хорев В.П. Методы и средства защиты информации в компьютерных системах: учебное пособие. – М.: Издательский центр «Академия», 2005.

3. Сергеева Т.И., Сергеев М.Ю. Методы и средства защиты информации: учебное пособие. – Воронеж: ВГТУ, 2008.

4. Сергеева Т.И., Сергеев М.Ю. Программные средства защиты информации: методические указания к выполнению лабораторных работ по дисциплине «Методы и средства защиты компьютерной информации». – Воронеж: ВГТУ, 2008. 14-2008

5. Алексеев В.А. Методы и средства криптографической защиты информации [Электронный ресурс]: методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации»/ Алексеев В.А.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009.— 16 с.— Режим доступа: http://www.iprbookshop.ru/17710.html.— ЭБС «IPRbooks»

6. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

7. Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.: Российский государственный гидрометеорологический университет, 2010.— 95 с.— Режим доступа: http://www.iprbookshop.ru/17925.html.— ЭБС «IPRbooks»

8. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.:

Российский государственный гидрометеорологический университет, 2010.— 104 с.— Режим доступа: http://www.iprbookshop.ru/17926.html.— ЭБС «IPRbooks»

9. Методические рекомендации по выполнению контрольных работ для бакалавров направления 09.03.01 профиля «Вычислительные машины, комплексы, системы и сети», магистров профиля 09.04.01 Информатика и вы-числительная техника, программа: Распределенные автоматизированные системы очной формы обучения / ФГБОУ ВО «Воронежский государственный технический университет»; сост. А.М. Нужный, Ю.С. Акинина, Н.И. Гребен-никова. Воронеж: Изд-во ВГТУ, 2020. – 8с.

10. Организация самостоятельной работы обучающихся : методические указания для студентов, осваивающих основные образовательные программы высшего образования – бакалавриата, специалитета, магистра-туры: методические указания / сост. В.Н. Почечихина, И.Н. Крючкова, Е.И. Головина, В.Р. Демидов; ФГБОУ ВО «Воронежский государственный технический университет ». – Воронеж, 2020. – 14 с.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Лицензионное ПО:

- Windows Professional 7 Single Upgrade MVL A Each Academic
- Microsoft Office Word 2007
- Microsoft Office Power Point 2007
- AcademicEdition Networked Volume Licenses RAD Studio XE8 Professional Concurrent ELC

Свободно распространяемое ПО:

- Microsoft Visual Studio Community Edition
- Microsoft Visual Studio Code
- CrypTool
- OpenPGP Studio

Отечественное ПО:

- Яндекс.Браузер
- Архиватор 7z
- Astra Linux

Ресурс информационно-телекоммуникационной сети «Интернет»:

- Образовательный портал ВГТУ
- http://www.edu.ru/
- https://metanit.com/

Информационно-справочные системы:

- http://window.edu.ru
- https://wiki.cchgeu.ru/

Современные профессиональные базы данных:

- https://proglib.io
- https://msdn.microsoft.com/ru-ru/
- https://docs.microsoft.com/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Для проведения лекционных занятий необходима аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

Для проведения лабораторных работ необходима лаборатория с ПК, оснащенными программами для проведения лабораторного практикума и обеспечивающими возможность доступа к локальной сети кафедры и Интернет, из следующего перечня:

- 307 (Лаборатория микропроцессорной техники)
- 309 (Лаборатория телекоммуникационных систем)
- 311 (Лаборатория разработки программных систем)
- 320 (Лаборатория общего назначения)
- 322 (Лаборатория распределённых вычислений)
- 324 (Специализированная лаборатория сетевых систем управления (научно-образовательный центр «АТОС»))
- 325 (Лаборатория автоматизации проектирования вычислительных комплексов и сетей)

Лаборатории расположены по адресу: 394066, г. Воронеж, Московский проспект, 179 (учебный корпус №3).

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Защита информации» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, связанные с организацией защиты информации, освоением алгоритмов шифрования и расшифровки данных, программными средствами защиты информации в локальной сети.

Лабораторные работы выполняются в дисплейных классах в соответствии с методиками, приведенными в указаниях к выполнению работ.

Лабораторные занятия направлены на приобретение практических навыков разработки, отладки и тестирования программ шифрования и расшифровки сообщений. Лабораторные работы также позволяют освоить методики программной защиты информации в локальных сетях.

Контроль усвоения материала дисциплины производится при тестировании, при защите лабораторных работ, при устном опросе. Освоение дисциплины оценивается на зачете.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.

Лист регистрации изменений

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	Актуализирован раздел 8.1 Перечень учебной литературы, необходимой для освоения дисциплины. Актуализирован раздел 8.2 в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем.	31.08.2020	
2	Внесены изменения в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем, учебной литературы, необходимой для освоения дисциплины.	31.08.2021