МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
декан факультета _____С.А.Баркалов
«31» августа 2021 года

РАБОЧАЯ ПРОГРАММА
дисциплины

«Информационная безопасность и защита информации»

Направление подготовки 38.03.05 БИЗНЕС-ИНФОРМАТИКА

Профиль Информационные системы в бизнесе

Квалификация выпускника бакалавр

Нормативный период обучения 4 года/4 года 11 м

Форма обучения очная/заочная

Год начала подготовки 2019

Автор программы _____/Сергеева Т.И./

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

Руководитель ОПОП _____/ Наролина Т.С./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

освоение методов и средств, обеспечивающих информационную безопасность и защиту информации предприятия на основе имеющихся стандартов информационной безопасности.

1.2. Задачи освоения дисциплины

– ознакомление с методами защиты информации, в том числе в сфере электронного бизнеса;

– ознакомление с имеющимися средствами защиты информации, в том числе в сфере электронного бизнеса;

– приобретение практических навыков применения стандартных программ для защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ОПК-1 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	**Знать:** – основные угрозы информационной безопасности; – методы защиты информации; – средства обеспечения информационной безопасности компьютерных систем; – стандарты информационной безопасности; – криптографические методы защиты информации.
	Уметь: – применять стандартные программные средства для защиты информации в бизнес системах.
	Владеть:

	– методами построения системы комплексной защиты информационных систем в бизнесе.
ПК-9	**Знать**: – задачи управления информационной безопасностью ИТ-инфраструктуры предприятия.
	Уметь: – настраивать конфигурации операционных систем для обеспечения информационной безопасности ИТ-инфраструктуры предприятия; – инсталлировать, тестировать и использовать программно-аппаратные средства для обеспечения информационной безопасности компьютерных систем.
	Владеть: – навыками применения стандартных пакетов программ для обеспечения информационной безопасности компьютерных систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	72	72
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	12	12
В том числе:		
Лекции	4	4
Лабораторные работы (ЛР)	8	8

Самостоятельная работа	159	159
Контрольная работа		
Часы на контроль	9	9
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

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 основы защиты информации**		**6**	**8**	**12**	**26**
		Информация как предмет защиты Определение информации и защищаемой информации, уровень важности информации, уровень секретности. Безопасность информации, конфиденциальность, целостность и доступность информации, угроза безопасности информации, несанкционированный доступ, политика безопасности, защита информации, информационная безопасность.	2		4	6
		Основные угрозы информационной безопасности. Модель нарушителя Классификация угроз информационной безопасности. Воздействия и каналы утечки. Модель потенциального нарушителя.	2	8	4	14
		Стандарты информационной безопасности Требования к комплексным системам защиты информации. Стандарты безопасности компьютерных систем. Государственные стандарты РФ по защите информации.	2		4	6
2	**Методы и средства защиты информации**		**14**	**12**	**28**	**54**
		Классификация методов и средств защиты данных Понятие метода защиты, средства защиты, механизма защиты. Классификация методов защиты. Классификация средств защиты.	2		4	6
		Средства защиты данных	2	4	4	10

		Законодательные средства защиты данных. Организационные средства защиты данных. Физические средства защиты данных.				
		Аппаратные и программные средства защиты данных Основные и вспомогательные средства защиты данных и их функциональное назначение.	2		4	6
		Криптографические методы защиты информации Основные определения (криптография, открытое сообщение, шифротекст, шифрование, шифр, ключ, криптоанализ, криптология). Симметричные и асимметричные системы шифрования. Классификация криптографических методов.	2	8	4	14
		Криптографическая система DES Схема шифрования DES. Режимы реализации алгоритма DES: «Электронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру», «Обратная связь по выходу».	2		4	6
		Отечественный стандарт шифрования данных Режимы реализации отечественного стандарта.	2		4	6
		Асимметричные криптосистемы Криптосистема шифрования данных RSA.	2		4	6
3	Организация безопасности информационных систем в бизнесе		**16**	**16**	**32**	**64**
		Методы и средства обеспечения безопасности информационных систем в бизнесе.	2		4	6
		Защита компьютерных систем от вредоносных программ. Защита программных средств от несанкционированного использования и копирования.	2	4	4	10
		Основные угрозы и принципы организации безопасности электронной коммерции Принципы организации безопасности. Методика построения системы безопасности. Основные угрозы безопасности и специфические риски электронной коммерции.	2	4	4	10
		Организация безопасности плате-				

		жей в интернете Российские платежные системы. Направления обеспечения безопасности информации при организации платежей. Стандарты безопасности платежных систем.	4		8	12
		Электронная цифровая подпись Основные определения (ЭЦП, электронный документ, открытый и закрытый ключи, регистрационное свидетельство, удостоверяющий центр). Алгоритмы формирования ЭЦП. Стандарт цифровой подписи ГОСТ Р34.10-94. Новые отечественные стандарты ЭЦП.	4	4	8	16
		Организация защиты информации в локальной сети Методы и средства защиты информации в сетях. Нарушение защиты информации через службы Интернет. Политика сетевой безопасности. Основные компоненты межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сетевого уровня. Шлюзы прикладного уровня.	2	4	4	10
Итого			**36**	**36**	**72**	**144**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение в основы защиты информации		**2**		**48**	**50**
		Информация как предмет защиты Определение информации и защищаемой информации, уровень важности информации, уровень секретности. Безопасность информации, конфиденциальность, целостность и доступность информации, угроза безопасности информации, несанкционированный доступ, политика безопасности, защита информации, информационная безопасность.	1		16	17
		Основные угрозы информационной безопасности. Модель нарушителя Классификация угроз информационной безопасности. Воздействия и каналы утечки. Модель потенциального нарушителя.	1		16	17
		Стандарты информационной безопасности Требования к комплексным системам			16	16

		защиты информации. Стандарты безопасности компьютерных систем. Государственные стандарты РФ по защите информации.				
2	Методы и средства защиты информации				**48**	**48**
		Классификация методов и средств защиты данных Понятие метода защиты, средства защиты, механизма защиты. Классификация методов защиты. Классификация средств защиты.			6	6
		Средства защиты данных Законодательные средства защиты данных. Организационные средства защиты данных. Физические средства защиты данных.			6	6
		Аппаратные и программные средства защиты данных Основные и вспомогательные средства защиты данных и их функциональное назначение.			6	6
		Криптографические методы защиты информации Основные определения (криптография, открытое сообщение, шифротекст, шифрование, шифр, ключ, криптоанализ, криптология). Симметричные и асимметричные системы шифрования. Классификация криптографических методов.			6	6
		Криптографическая система DES Схема шифрования DES. Режимы реализации алгоритма DES: «Электронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру», «Обратная связь по выходу».			6	6
		Отечественный стандарт шифрования данных Режимы реализации отечественного стандарта.			12	12
		Асимметричные криптосистемы Криптосистема шифрования данных RSA.			6	6
3	Организация безопасности информационных систем в бизнесе		**2**	**8**	**63**	**73**
		Методы и средства обеспечения безопасности информационных систем в бизнесе.	2		10	12
		Защита компьютерных систем от		2	10	12

		вредоносных программ. Защита программных средств от несанкционированного использования и копирования.				
		Основные угрозы и принципы организации безопасности электронной коммерции Принципы организации безопасности. Методика построения системы безопасности. Основные угрозы безопасности и специфические риски электронной коммерции.		2	10	12
		Организация безопасности платежей в интернете Российские платежные системы. Направления обеспечения безопасности информации при организации платежей. Стандарты безопасности платежных систем.			11	11
		Электронная цифровая подпись Основные определения (ЭЦП, электронный документ, открытый и закрытый ключи, регистрационное свидетельство, удостоверяющий центр). Алгоритмы формирования ЭЦП. Стандарт цифровой подписи ГОСТ Р34.10-94. Новые отечественные стандарты ЭЦП.		2	11	13
		Организация защиты информации в локальной сети Методы и средства защиты информации в сетях. Нарушение защиты информации через службы Интернет. Политика сетевой безопасности. Основные компоненты межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сетевого уровня. Шлюзы прикладного уровня.		2	11	13
Итого			**4**	**8**	**159**	**171**

5.2 Перечень лабораторных работ

Неделя семестра	Наименование лабораторной работы	Объем часов	Виды контроля
7 семестр – очная форма обучения		**36**	
Введение в основы защиты информации		**4**	
1	Лабораторная работа № 1. Реализация программных генераторов паролей	4	Отчет, демонстрация работы на компьютере

Методы и средства защиты информации		**16**	
3	Лабораторная работа № 2. Программная реализация алгоритмов шифрования, основанных на методах замены	4	Отчет, демонстрация работы на компьютере
5	Лабораторная работа № 3. Программная реализация алгоритмов шифрования, основанных на методах перестановки	4	Отчет, демонстрация работы на компьютере
7	Лабораторная работа № 4. Изучение стандартных программ шифрования с применением алгоритма DES		Отчет, демонстрация работы на компьютере
9	Лабораторная работа № 5. Изучение существующих программ шифрования электронных сообщений и формирования электронных цифровых подписей	4	Отчет, демонстрация работы на компьютере
Организация безопасности информационных систем в бизнесе		**16**	
11	Лабораторная работа № 6. Программные средства обеспечения информационной безопасности прикладного программного обеспечения	4	Отчет, демонстрация работы на компьютере
13	Лабораторная работа № 7. Настройка и администрирование операционных систем для обеспечения информационной безопасности компьютерных систем	4	Отчет, демонстрация работы на компьютере
15	Лабораторная работа № 8. Настройка и конфигурирование FireWall на примере бесплатно распространяемой версии	4	Отчет, демонстрация работы на компьютере
17	Лабораторная работа № 9. Настройка сетевых элементов инфокоммуникационной системы для обеспечения защиты информации	4	Демонстрация результата выполнения задания
Итого часов на очной форме обучения		**36**	
9 семестр – заочная форма обучения		**8**	
В сессию	Лабораторная работа № 1. Реализация программных генераторов паролей	4	Отчет, демонстрация работы на компьютере
В сессию	Лабораторная работа № 2. Настройка и конфигурирование FireWall на примере бесплатно распространяемой версии	4	Отчет, демонстрация работы на компьютере
Итого часов на заочной форме обучения		**8**	

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
ОПК-1	Знать: - основные угрозы информационной безопасности; - методы защиты информации; - средства обеспечения информационной безопасности компьютерных систем; - стандарты информационной безопасности; - криптографические методы защиты информации.	Тест Решение стандартных практических задач	Выполнение теста на 60-100 % Выполнение лабораторных работ № 1-5 (лабораторной работы № 1 и контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	Выполнение теста менее 60 % Невыполнение лабораторных работ (контрольной работы для заочников) в срок, предусмотренный в рабочих программах
	Уметь: - применять стандарт-	Решение стандартных практических задач	Выполнение лабораторных работ № 1-5 (лабо-	Невыполнение лабораторных работ

	ные программные средства для защиты информации в бизнес системах.		раторной работы № 1 и контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	(контрольной работы для заочников) в срок, предусмотренный в рабочих программах
	Владеть: - методами построения системы комплексной защиты информационных систем в бизнесе.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-9	Знать: - задачи управления информационной безопасностью ИТ-инфраструктуры предприятия.	Тест	Выполнение теста на 60-100 %	Выполнение теста менее 60 %
	Уметь: - настраивать конфигурации операционных систем для обеспечения информационной безопасности ИТ-инфраструктуры предприятия; - инсталлировать, тестировать и использовать программно-аппаратные средства для обеспечения информационной безопасности компьютерных систем.	Решение стандартных практических задач	Выполнение лабораторных работ № 6-9 (лабораторной работы № 1 и контрольной работы для заочной формы обучения) в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ (контрольной работы для заочников) в срок, предусмотренный в рабочих программах
	Владеть: - навыками применения стандартных пакетов программ для обеспечения информационной безопасности компьютерных систем.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

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 четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-1	Знать: - основные угрозы	Тест	Выполнение теста на 90-	Выполнение теста на 80-	Выполнение теста на 70-	В тесте менее 70%

	информационной безопасности; - методы защиты информации; - средства обеспечения информационной безопасности компьютерных систем; - стандарты информационной безопасности; - криптографические методы защиты информации.		100%	90%	80%	правильных ответов
	Уметь: - применять стандартные программные средства для защиты информации в бизнес системах.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - методами построения системы комплексной защиты информационных систем в бизнесе.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-9	Знать: - задачи управления информационной безопасностью ИТ-инфраструктуры предприятия.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - настраивать конфигурации операционных систем для обеспечения информационной безопасности ИТ-инфраструктуры предприятия; - инсталлировать, тестировать и использовать программно-аппаратные средства для обеспечения информационной безопасности компьютерных систем.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - навыками приме-	Решение прикладных задач в	Задачи решены в полном	Продемонстрирован вер-	Продемонстрирован верный	Задачи не решены

	нения стандартных пакетов программ для обеспечения информационной безопасности компьютерных систем.	конкретной предметной области	объеме и получены верные ответы	ный ход решения всех, но не получен верный ответ во всех задачах	ход решения в большинстве задач	

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

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

3. Укажите правильный ответ

… - это деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

4. Укажите правильный ответ

… - это неконтролируемое распространение защищаемой информации.

а) Разглашение
б) Несанкционированный доступ
в) Утечка

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

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

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

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

9. Укажите правильный ответ

Воздействия и каналы утечки – это ..

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

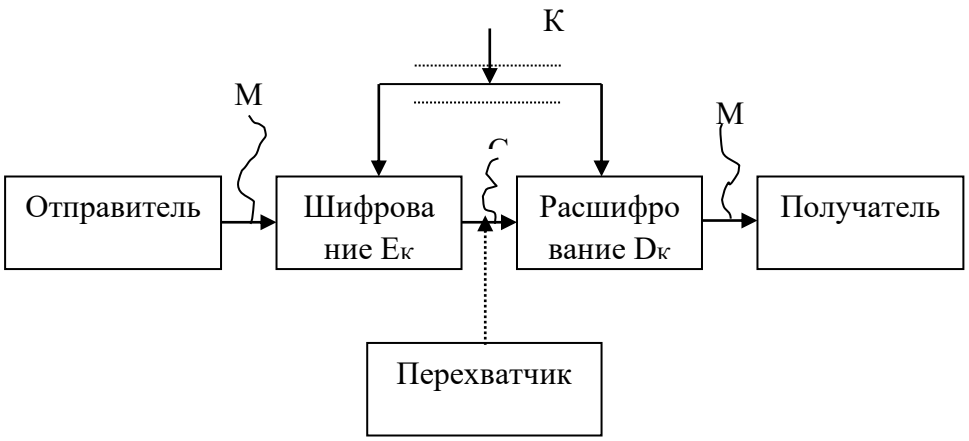
10. Укажите правильный ответ

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

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

7.2.2 Примерный перечень заданий для решения стандартных задач

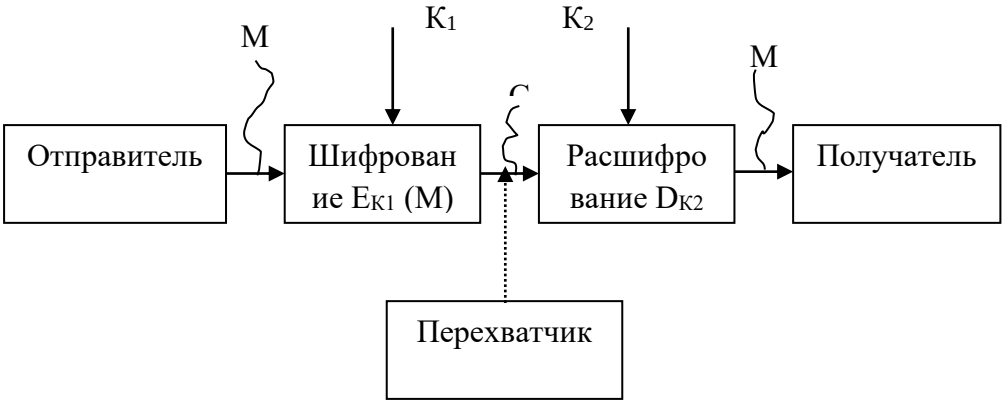
1. Представлена схема криптосистемы



Данная схема является:

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

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.

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.

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.

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.

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.

7. … использует несколько алфавитов шифртекста.

Пусть используется k алфавитов. Тогда открытый текст: $X=X_1X_2...X_k \quad X_{k+1}...X_{2k} X_{2k+1}...$ 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.

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.

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.

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 $s_i=|x_1,x_2,...,x_n|$, $x_k \in \{0,1\}$. Шифртекст получается как скалярное произведение $C \cdot s_i$.

а) Задача об укладке ранца;

б) Задача умножения матриц;

в) Задача вычисления значения полинома по модулю.

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

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1 Основные направления защиты компьютерной информации

2 Информация как предмет защиты, конфиденциальная информация, защищаемая информация, уровень секретности, защита информации

3 Определения: безопасность информации, целостность информации, конфиденциальность информации

4 Определения: угроза безопасности информации, несанкционированный доступ к информации, политика безопасности

5 Основные угрозы информации по предмету направленности, по источнику возникновения

6 Виды воздействий, реализующие угрозу безопасности данных

7 Косвенные и прямые каналы утечки данных

8 Модель потенциального нарушителя

9 Определения: методы защиты, средства защиты, механизмы защиты

10 Определение метода защиты. Методы защиты: управление, препятствия, маскировка.

11 Определение метода защиты. Методы защиты: регламентация, побуждение, принуждение.

11 Классификация средств защиты

12 Физические средства защиты данных

13 Законодательные средства защиты компьютерной информации

14 Организационные средства защиты компьютерной информации

15 Аппаратные средства защиты

16 Программные средства защиты компьютерной информации

17 Требования к комплексным системам защиты компьютерной информации

18 Стандарты безопасности КС

19 Криптография. Шифрование. Шифр. Ключ. Криптоанализ. Криптология.

20 Симметричные системы шифрования.

21 Асимметричные системы шифрования.

22 Классификация криптографических методов.

23 Методы замены: моноалфавитная, гомофоническая, полиалфавитная, полиграммная.

24 Методы перестановки. Методы гаммирования

25 Обобщенная схема симметричной криптосистемы

26 Обобщенная схема асимметричной криптосистемы

27 Шифрование данных с использованием алгоритма DES

28 Отечественный стандарт шифрования

36 Процедуры шифрования и расшифрования в криптосистеме RSA

37 Безопасность электронной коммерции. Информационная безопасность. Направления информационной безопасности.

38 Принципы защиты электронной коммерции (общие принципы, организационные, принципы реализации).

39 Методика построения системы безопасности электронной коммерции.

40 Основные угрозы информационной безопасности электронной коммерции.

41 Убытки. Прямые убытки. Косвенные убытки. Специфические риски электронной коммерции.

42 Направления обеспечения безопасности информации при организации электронных платежей.

43 Стандарты безопасности платежных систем.

44 Электронная цифровая подпись (ЭЦП). Электронный документ. Задачи, решаемые ЭЦП.

45 Открытый и закрытый ключи ЭЦП. Регистрационное свидетельство.

46 Формирование и проверка ЭЦП. Алгоритмы формирования ЭЦП.

47 Стандарт цифровой подписи ГОСТ Р34.10-94.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

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

Оценка на экзамене выставляется следующим образом.

1. Оценка «Неудовлетворительно» ставится в случае, если студент не ответил ни на один вопрос

2. Оценка «Удовлетворительно» ставится в случае, если студент ответил на один вопрос в полном объеме, изложив общие понятия и методики

3. Оценка «Хорошо» ставится в случае, если студент ответил на два вопроса в полном объеме, но не ответил на уточняющие вопросы по тематике вопросов билета.

4. Оценка «Отлично» ставится, если ответил на два вопроса в полном объеме, а также ответил на уточняющие вопросы по тематике вопросов ответа.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в основы защиты информации	ОПК-1, ПК-9	Тест, контрольная работа (для заочников), защита лабораторных работ, экзамен, устный опрос
2	Методы и средства защиты информации	ОПК-1, ПК-9	Тест, контрольная работа (для заочников), защита лабораторных работ, экзамен, устный опрос
3	Организация безопасности информационных систем в бизнесе	ОПК-1, ПК-9	Защита лабораторных работ, экзамен, 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.

Экзамен сдается по билетам из двух вопросов. Допуском к экзамену 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. 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»

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
LibreOffice

Ресурс информационно-телекоммуникационной сети «Интернет»
http://www.edu.ru/

Образовательный портал ВГТУ

Информационная справочная система
http://window.edu.ru
https://wiki.cchgeu.ru/

Современные профессиональные базы данных
Information Security Информационная безопасность
http://www.itsec.ru/
Securitylab.ru by Positive Technologies
https://www.securitylab.ru/
Anti-Malware.ru
https://www.anti-malware.ru/news
Iso27000.ru Искусство управления информационной безопасностью
http://www.iso27000.ru/
SecurityPolicy.ru Документы по информационной безопасности
http://securitypolicy.ru/
SearchInform – Информационная безопасность
https://searchinform.ru/informatsionnaya-bezopasnost/
Ekrost.ru - Информационная безопасность предприятия

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Лекционная аудитория и аудитории для практических занятий, оснащённые мультимедийным демонстрационным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим демонстрацию мультимедиаматериалов.

Аудитории для лабораторных занятий, оснащенные компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно образовательную среду университета.

Аудитории для самостоятельной работы, оборудованные техническими средствами обучения: персональными компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду университета

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

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе. Это 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 экзамене.

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. Три дня перед экзаменом эффективнее всего использовать для повторения и систематизации материала.

6 Лист регистрации изменений

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