Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ефанов Алексей В МРИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ Должность: Директор Невиномысского технологического института (филартистер Ации

высшего образования 49214306dd433e7a1b0f8632f645f9d53c99e3d0

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Директор НТИ (филиал) СКФУ Ефанов А.В. Ф.И.О. 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине

Информационная безопасность

Направление подготовки 09.03.02 Информационные системы и

технологии

Направленность (профиль) Информационные системы и технологии в

бизнесе

Форма обучения очная Год начала обучения 2022

Реализуется в 6 семестре

Введение

- 1. Назначение: обеспечение методической основы для организации и проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность». Текущий контроль успеваемости и промежуточная аттестация по данной дисциплине вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля успеваемости и промежуточной аттестации являются получение первичной информацию о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.
- 2. ФОС является приложением к программе дисциплины «Информационная безопасность» и в соответствии с образовательной программой высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии.
- 3. Разработчик: Кочеров Ю. Н., доцент базовой кафедры Регионального индустриального парка, кандидат технических наук
- 4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:

Мельникова Е.Н. – председатель УМК НТИ (филиал) СКФУ

Члены комиссии:

А.И. Колдаев, и.о. зав. кафедрой информационных систем, электропривода и автоматики Э.Е. Тихонов, доцент базовой кафедры территории опережающего социально-экономического развития

Представитель организации-работодателя:

Горшков М. Г., директор ООО «Арнест-информационные технологии"

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 09.03.02 Информационные системы и технологии и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Информационная безопасность».

05 марта 2022 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код	Этап	Средства и	Вид контроля,	Тип	Наименова
оцениваем	формирован	технологии	аттестация	контроля	ние
ой	ия	оценки	(текущий/промежуточ	(устный,	оценочного
компетенц	компетенци		ный)	письменный	средства
ии,	И			или с	
индикатор	(№ темы)			использован	
а (ов)	(6			ием	
	соответст			технических	
	вии с			средств)	
	рабочей				
	программой				
	дисциплины				
)				
ИД-1 опк-3					
ИД-2 опк-3					Вопросы
ИД-3 опк-3	1-3	Собеседова	Текущий	Устный	для
ИД-1 _{ОПК-7}	1-3	ние	текущий	3 СППЫИ	собеседова
ИД-2 опк-7					ния
ИД-3 опк-7					
ИД-1 опк-3					
ИД-2 опк-3					Паспорт
ИД-3 опк-3	1-3	Тестирован	Тогалинй	Устный	фонда
ИД-1 опк-7	1-3	ие	Текущий	УСТНЫИ	тестовых
ИД-2 опк-7					заданий
ИД-3 опк-7					

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

Уровни		Дескрипто	оры	
сформированн ости компетенци(ий), индикатора (ов)	Минимальный уровень не достигнут (Неудовлетворите льно) 2 балла	Минимальный уровень (удовлетворител ьно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
информационной	решать стандартные и библиографичес ых технологий и с учето Не удовлетворительно осознает задачи профессиональной деятельности с применением информационнокоммуникационных технологий и с учетом основных	кой культуры с	применением	информационно-
	требований информационной	информационной безопасности;	и с учетом основных	основные этапы

безопасности; He удовлетворительно решает задачи профессиональной деятельности применением информационнокоммуникационных технологий И учетом основных требований информационной безопасности He удовлетворительно применяет решения задач профессиональной деятельности применением информационнокоммуникационных технологий И *<u>v</u>четом* основных требований информационной безопасности;

Слабо решает залачи профессионально й деятельности с применением информационнокоммуникационн ых технологий и с учетом основных требований информационной безопасности Слабо применяет решения залач профессионально й деятельности с применением информационнокоммуникационн ых технологий и с учетом основных требований информационной безопасности;

требований информационн ой безопасности; Решает задачи профессиональ ной деятельности с применением информационн коммуникацион ных технологий c учетом И основных требований информационн ой безопасности Применяет решения задач профессиональ ной деятельности с применением информационн коммуникацион ных технологий И c учетом основных требований информационн ой безопасности;

построения систем безопасности корпоративных систем; Применяет основные этапы создания комплексной системы защиты информации;

ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем

Результаты обучения по дисциплине (модулю): *Индикатор*: ИД-1 _{ОПК-7} ИД-2 _{ОПК-7} ИД-3 _{ОПК-7}

He удовлетворительно понимает предмет и защиты объект информации; краткий обзор современных методов защиты информации; He удовлетворительно использует методы функциональной безопасности корпоративных систем; He удовлетворительно применяет методы

сообщения

Слабо понимает предмет и объект защиты информации; краткий обзор современных метолов зашиты информации; Слабо использует методы функциональной безопасности корпоративных систем; Слабо применяет методы сообщения и шифрования; стеганографии;

Понимает предмет И объект защиты информации; краткий обзор современных метолов защиты информации; Использует методы функционально й безопасности корпоративных систем; применяет методы сообщения И шифрования; стеганографии;

Понимает интегрированн систему информационн ой безопасности; зашита документообор ота вычислительны системах; средства зашиты информации; применяет моделирования комплексных систем защиты информации; методы оценки

сте код алг ши	ифрования; еганографии; дирования; горитмы ифрования с крытым ключом;	кодирования; алгоритмы шифрования с открытым ключом;	кодирования; алгоритмы шифрования с открытым ключом;	систем защиты информации; применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографиче ские средства защиты;
-------------------------	--	--	--	--

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль Рейтинговая оценка знаний студента (в случаях, предусмотренных нормативными актами СКФУ).

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	5 семестр		
1	Собеседование по темам 1-3, Защита практических работ	8	25
2	Собеседование по теме 2-3, Защита лабораторных работ	16	30
	Итого за 5 семестр:		55
	Итого:		55

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
<i>Удовлетворительный</i>	60
Неудвлетворительный	0

Промежуточная аттестация

Промежуточная аттестация в форме зачета или зачета с оценкой

Процедура зачета (зачета с оценкой) как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра

обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{\text{зач}}$) при различных рейтинговых баллах

по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине	Количество баллов за зачет (S_{3a4})
по результатам работы в семестре (R_{cem})	
$50 \le R_{cen} \le 60$	40
$39 \le R_{cen} < 50$	35
$33 \leq R_{cem} < 39$	27
$R_{cem} < 33$	0

При зачете с оценкой используется шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Шкала пересчета рейтингового балла по дисциплине

в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	Оценка по 5-балльной системе
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
< 53	Неудовлетворительно

2. Типовые контрольные задания и иные материалы, характеризующие этапы формирования компетенций

Вопросы для собеседования

Пороговый уровень Тема 1. Средства защиты информации

- 1. Что такое LFSR?
- 2. Как построить псевдослучайный генератор на основе регистра сдвига?
- 3. На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?
- 4. Как реализовать возведение в степень чисел большой разрядности по большому модулю?
- 5. Какая информация является конфиденциальной?
- 6. Что относится к защищаемой информации?
- 7. Что понимается под политикой безопасности?
- 8. Что понимается под несанкционированным воздействием на защищаемую информацию?
- 9. Дайте понятие конфиденциальности, целостности и доступности информации.

Тема 2. Функциональная безопасность корпоративных систем

- 1. Что такое симметричное шифрование?
- 2. В чем особенность блочных шифров?
- 3. В чем особенность асимметричных систем шифрования?
- 4. На чем базируется криптостойкость RSA?
- 5. Как увеличить производительность системы шифрования RSA?
- 6. Составляющие функциональной безопасности

7. Этапы построения систем безопасности

Тема 3. Криптографические средства защиты

- 1. Назначение цифровой подписи.
- 2. В чем отличие криптосхемы ЭльГамаля от RSA?
- 3. Почему шифр RSA называется асимметричным?
- 4. На чем основана стойкость шифра RSA?
- 5. Что такое цифровой конверт?
- 6. Опишите общую схему ЭЦП.
- 7. Каково назначение хеш-функции?
- 8. Какими свойствами противодействия должна обладать криптографическая хешфункция?
- 9. Что такое МАС и как он формируется?

Повышенный уровень

Тема 1. Средства защиты информации

- 1. Какие тесты на случайность вам известны?
- 2. Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы
- 3. Дайте определение информационной безопасности.
- 4. Какие цели и задачи включает в себя концепция национальной безопасности РФ?
- 5. Перечислите основные виды угроз информационной безопасности РФ.
- 6. Дайте определение комплексного обеспечения информационной безопасности.
- 7. Перечислите основные элементы организационной основы государственной системы обеспечения информационной безопасности $P\Phi$

Тема 2. Функциональная безопасность корпоративных систем

- 1. Какова длина ключа блочного шифра?
- 2. На чем базируется криптостойкость блочного шифра?
- 3. Какие элементарные операции используются в симметричном шифровании?
- 4. Какие атаки на систему RSA вам известны?
- 5. Как противодействовать атакам на систему RSA?
- 6. Анализ рисков и показатели функциональной безопасности

Тема 3. Криптографические средства защиты

- 1. На чем базируется криптостойкость системы ЭльГамаля?
- 2. Почему шифр RSA называется асимметричным?
- 3. На чем основана стойкость шифра RSA?
- 4. Что такое цифровой конверт?
- 5. Опишите общую схему ЭЦП.
- 6. Каково назначение хеш-функции?
- 7. Какими свойствами противодействия должна обладать криптографическая хешфункция?
- 8. Что такое МАС и как он формируется?
- 9. Каковы функции удостоверяющего центра ЭП? Какие сведения заносятся в сертификат открытого ключа ЭП?

- 10. Для каких целей используется СКЗИ «Верба-OW»?
- 11. Какие отечественные криптоалгоритмы реализуются в «КриптоПро CSP»?
- 12. Каково назначение ПАК «КриптоПро УЦ»?

Компетентностно-ориентированные задания

- 1. Проанализировать, 4-битовый LFSR с отводом от первого и четвертого битов со значением 1010
- 2. Для сообщения длинно 4 бита, шифруемого алгоритмом RSA задаются начальные параметры: генерируется два секретных больших простых числа р и q, необходимо вычислить n и $\varphi(n)$
- 3. Изобразите схему конструкции Фейстеля и поясните ее
- 4. Изобразите схема DES-преобразования
- 5. Рассчитайте значение 1570¹⁰¹⁹ mod 3337
- 6. Для генерации пары ключей для сообщения длинной 4 вычислите открытый и закрытый ключи

1. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он

Понимает средства защиты информации; угрозы безопасности информации в компьютерных системах;

Решает основные этапы построения систем безопасности корпоративных систем;

Применяет основные этапы создания комплексной системы защиты информации;

Понимает интегрированную систему информационной безопасности; защита документооборота в вычислительных системах; средства защиты информации;

применяет моделирования комплексных систем защиты информации; методы оценки систем защиты информации;

применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографические средства защиты;

Оценка «хорошо» выставляется студенту, если он

Осознает задачи профессиональной деятельности с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности;

Решает задачи профессиональной деятельности с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности

Применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Использует методы функциональной безопасности корпоративных систем; применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «удовлетворительно» выставляется студенту, если он

Слабо осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Слабо применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Слабо использует методы функциональной безопасности корпоративных систем;

Слабо применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «неудовлетворительно» выставляется студенту, если он

Не удовлетворительно осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Не удовлетворительно применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Не удовлетворительно использует методы функциональной безопасности корпоративных систем;

Не удовлетворительно применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла
	за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Пример:

Процедура проведения данного оценочного мероприятия включает в себя: защиту лабораторных и практических занятий

Предлагаемые студенту вопросы позволяют проверить ИД-1 $_{\rm OПK-3}$, ИД-2 $_{\rm OПK-3}$, ИД-3 $_{\rm OПK-3}$, ИД-1 $_{\rm OПK-7}$, ИД-2 $_{\rm OПK-7}$, ИД-3 $_{\rm OПK-7}$ компетенции

Для подготовки к данному оценочному мероприятию необходимо 10 минут.

При подготовке к ответу студенту предоставляется право пользования отчетами о выполненных лабораторных и практических занятий.

При проверке задания, оцениваются последовательность и логика ответа

Оценочный лист

No	Фамили			-	Вид работы			Итог
Π/	я, имя	Соответств	Раскрыт	Ясность,	Обоснованно	Самостоятельно	Четкость,	
П	студент	ие ответа	ие	четкость,	сть	сть в	обоснован	
	a	заданию	проблем	логичнос	излагаемой	формулировке	ность,	
			ы, темы	ть,	позиции,	позиции	научность	
				научност	ответа		выводов	
				ь				
				изложени				
				Я				

Паспорт фонда тестовых заданий по дисциплине Информационная безопасность

Nº	Тест	Ключ
п/п		
1.	Какова цель использования генераторов псевдослучайных чисел при поточном шифровании?	получение «бесконечной» гаммы (ключевой последовательности),
	 формирование открытых ключей защита информации от всех случайных или преднамеренных изменений получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа защита информации от случайных помех при передаче и хранении сжатие информации 	располагая относительно малой длиной самого секретного ключа
2.	 Чем определяется разрядность сдвигового регистра с обратной связью? – скоростью работы регистра – температурой окружающей среды – количеством входов в устройстве генерации функции обратной связи – количеством бит, которое может одновременно храниться в регистре сдвига 	количеством бит, которое может одновременно храниться в регистре сдвига
3.	Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии — функцией Диффи-Хеллмана — односторонней функцией — функцией Эйлера — криптографической функцией	односторонней функцией
4.	Алгоритм ГОСТ 28147-89 является — алгоритмом вычисления функции хеширования — блочным алгоритмом асимметричного шифрования	блочным алгоритмом симметричного шифрования

- блочным алгоритмом симметричного шифрования - алгоритмом формирования элсктронной цифровой подписи 5. Что вяляется особенностью использования режима СВС блочного шифра? - одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст - сообщение, запиифровать, выбирая блоки шифротскета преобразуются в одинаковый шифротекст - отот режим работает очень медлению, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщение, запиифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равец результат выполнения побитовой операции чеся 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или пистнадцатеричных числа необходимо сначала перевести в двоичный вид 7. Можст ли пифр е копечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с эакрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования информации используется перестановка символов — в них калуно пограций шифрования ирасшифрования информации используется перестановка символов — в имх для шифрования и расшифрования информации		T	1
- алгоритмом формирования электронной шифровой подписи ТОВС блочного шифра? - Одинаковые сообщения при использования режима СВС блочного шифра? - одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст - сообщение, запифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста преобразуются в одинаковый шифротекста преобразуются в одинаковый шифротекст - этот режим работаст очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений - сообщений - сообщений - сообщений сообщений подкленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений - сообщений сообщений подкления побитовой операции «сумма по модулю 2» для шестнадцатеричных чиссл ОВ5 и 379 Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо свачала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? - да, если это алгоритм шифрования с открытым ключом? - в зависимости от параметров шифра пет дя - дя, если это алгоритм шифрования с открытым ключом? - в них для пифрования информации информация информации информация информации информации информация несевроснучайных чисел информаци			
 1. Что является особенностью использования режима СВС блочного пифра? Одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст — сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке — одинаковый вифротекст — одинаковые блоки исходного текста преобразуются в одинаковый пифротекст — этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений — сообщение, зашифрованное в данном режиме, можно расшифрованть только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модуло ≥» для нестандиатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестпадиатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с копечным ключом быть совершенным? — да, если это алгоритм шифрования с эткрытым ключом? — в викх для шифрования информации используется один ключ, а для расшифрования и расшифрования и расшифрования и расшифрования и прасшифрования и расшифрования и ноформации используется два разных ключа – открытый и закрытый — в них для шифрования и расшифрования и ниформации используется два разных ключа – открытый и закрытый — в них для шифрования и постанова символов – в них для шифрования и расшифрования и ниформации используется два разных ключа – открытый информации используется два разных ключа – теперации шковользуется один и тот же ключ – теперации шковользуется один и тот же ключ – теперации псевдослучайных чисел (ВВS)? 		11	
 5. Что является особенностью использования режима СВС блочного шифра? — одинаковый шифротекст — сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке — одинаковый шифротекст а произвольном порядке — одинаковые блоки исходного текста преобразуются в одинаковый шифротекст тото практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений — сообщений — сообщений — сообщений, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнеция побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа псобходимо спачала перевссти в двоичный вид 7. Может ли пифр с конечным ключом быть совершенным? — да, если это алторитм шифрования с открытым ключом — в зависимости от параметров шифра — ист — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для пифрования информации используется один ключ, а для расшифрования и перестаповка символов — в их для операций шифрования и расшифрования и нерормации используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования и ниформации используется один и тот же ключ — в них для шифрования и расшифрования и ниформации используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ — в них для шифрования и расшифрования информации используется один и тот же ключ — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ — открытый и закрытый песедослучайных чисел (ВВS)? 7. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)? 			
СВС блочного шифра? — одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст — сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке — одинаковые блоки исходного текста преобразуются в одинаковый шифротекст — этот режим работает очень медленно, что практически не позволяет использовать сто для обработки больших (> 1 Кбайт) исходных сообщений — сообщений — сообщение, запифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнаднатеричных числ 0В5 и 377 Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнаднатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с копечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в вих для шифрования информации используется один ключ, а для расшифрования — другой ключ — в пих входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для пифрования и расшифрования и перестановка символов — в них для пифрования и расшифрования и расшифрования и наспользуется один и тот же ключ — в них для пифрования и расшифрования и ноформации используется один и тот же ключ — в них для пифрования и расшифрования информации используется один и тот же ключ — в них для пифрования и расшифрования информации используется один и тот же ключ — открытый и закрытый — в них для пифрования и расшифрования информации используется один и тот же ключ — открытый и закрытый — в них для пифрования и поседослучайных чисел (ВВS)?			-
	5.		
разных векторов инициализации преобразуются в одинаковый шифротекст — сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке — одинаковые блоки исходного текста преобразуются в одинаковый шифротекст — этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений — сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, пачиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двончной системе счисления Примечание: десятичные или шестнадцатеричные числа песобходимо спачала перевести в двончный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в завноимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования и пастифрования и расшифрования и расшифрования и расшифрования и пререстановка симколов — в них для операций шифрования и расшифрования и расшифрования и преставовка симколов — в них для инфрования и расшифрования информации используется два разных ключа — открытый и закрытый — в них для инфрования и расшифрования информации используется два разных ключа — открытый и закрытый — в них для шифрования и пот же ключ — открытый и закрытый — в них для шифрования и пот же ключ — открытый и закрытый — в них для шифрования и пот же ключ — открытый и закрытый — в них для шифрования и песедослучайных чисел (ввях)?			
в одипаковый шифротекст - сообщение, защифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке - одинаковые блоки исходного текста преобразуются в одинаковый пифротекст - этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений - сообщение, защифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для пнестнадцатеричных чисел 105 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с копечным ключом быть совершенным? - да, если это алгоритм шифрования с открытым ключом - в зависимости от параметров пифра - нет - да 8. Что общего имеют все методы шифрования с закрытым ключом? - в них для шифрования информации используется один ключ, а для расшифрования и расшифрования и расшифрования и расшифрования и расшифрования и праспифрования и расшифрования и праспифрования и иформации шифрования и распифрования и информации используется два разных ключа - открытый и закрытый - в них для пифрования и распифрования информации используется два разных ключа - открытый и закрытый - в них для пифрования и распифрования информации используется два разных ключа - открытый и закрытый - в них для пифрования и распифрования информации используется два разных ключа - открытый и закрытый - в них для пифрования и распифрования информации используется два разных ключа - открытый и закрытый - в них для пифрования и распифрования информации используется два разных ключа - открытый и закрытый и распифрования информации используется один и тот же ключ 9. Для чего предназначен алгориты Блюм-Блюма-Шуба псевдослучайных чисел		-	*
с первого блока пинфровать, выбирая блоки пинфротекста в произвольном порядке одинаковые блоки исходного текста преобразуются в одинаковый шифротекст этот режим работаст очень медленно, что практически пе позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений сообщение, запифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестпадцатеричных чисел 0В5 и 37? Вариапты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в завнеимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и расшифрования — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)? перестации песеросучайных чисел			1
можно расшифровать, выбирая блоки шифрогекста в произвольном порядке одинаковые блоки исходного текста преобразуются в одинаковый шифротекст этот режим работает очень медленно, что практически не позволяет непользовать его для обработки больших (> 1 Кбайт) исходных сообщений сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для пнестнадцатеричных чисел 0В5 и 377 Варананть ответов представлены в двоичной системе счисления Примечание: десятичные или пнестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? да, если это алгоритм шифрования с эакрытым ключом в зависимости от параметров шифра пет да Ито общего имеют все методы шифрования с закрытым ключом? в них для шифрования информации используется один ключ, а для расшифрования — другой ключ в них для пифрования информации используется один ключ, а для расшифрования — другой ключ в них для пифрования и престановка символов в них для операций шифрования и расшифрования и расшифрования и прасшифрования и расшифрования и прасшифрования и расшифрования информации используется два разных ключа — открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?		11	
вифротекста в произвольном порядке одинаковые блоки исходного текста преобразуются в одинаковый шфротекст тото грежим работает очень медленно, что практически не позволяст использовать его для обработки больших (> 1 Кбайт) исходных сообщений сообщений сообщений сообщений, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 4. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? да, сели это алгоритм шифрования с открытым ключом в зависимости от параметров шифра нет да нет да 4. Что общего имеют все методы шифрования с закрытым ключом? в них для шифрования информации используется одни ключ, а для расшифрования — другой ключ в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов в них для операций шифрования и расшифрования и прасшифрования прасшифрования и прасшифрования прасшифрования и расшифрования информации используется два разных ключа — открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			с первого олока
 — одинаковые блоки исходного текста преобразуются в одинаковый шифротекст — этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений — сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования ирформации используется перестановка символов — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования ирасшифрования ирасшифрования ирасшифрования ирасшифрования информации используется дав разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)? 			
преобразуются в одинаковый шифротекст — этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений — сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — пет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — один и тот же ключ — в них для спераций шифрования и расшифрования и прасшифрования и прасшифрования и прасшифрования и наспользуется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования и прасшифрования и информации используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования и прасшифрования и наспользуется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
— этот режим работает очень медленно, что практически ие позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений — сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: дсеятичные или шестнадцатеричные числа пеобходимо спачала перевести в двоичный вид 7. Может ли шифр с копечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования ирасшифрования ирасшифрования и расшифрования и наспользуется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и расшифрования и прасшифрования и спользуется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования и наспользуется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба геперации псевдослучайных чисел			
обработки больших (> 1 Кбайт) исходных сообщений — сообщений — сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, пачиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — один и тот же ключ — в них для операций шифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и расшифрования и расшифрования и расшифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и расшифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и прасшифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и расшифрования и прасшифрования и прасшифровани			
сообщений — сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования информации используется перестановка символов — в них для операций шифрования и расшифрования и расшифрования и прасшифрования и накрытый и закрытый — в них для шифрования и расшифрования и накрытый и закрытый — в них для шифрования и расшифрования информации используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
- сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и на виж для операций шифрования и расшифрования и на виж для операций шифрования и расшифрования и на виж для шифрования и расшифрования и на виж для шифрования и расшифрования и на виж для шифрования и на виж для шифрования и на виж для шифрования и расшифрования и на виж для шифрования и на виж для шифрования и на виж для шифрования и на тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
можно расшифровать только последовательно, начиная с первого блока 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала первести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них для шифрования информации используется один ключо, а для расшифрования — один и тот же ключ в них для операций шифрования и расшифрования и расшифрования и прасшифрования и прасшифрования и закрытый — в них для пифрования и расшифрования и на вних для шифрования и расшифрования и на вних для шифрования и расшифрования и на вних для шифрования и расшифрования и на вних для пифрования и расшифрования и по ткрытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
пачиная с первого блока Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, ссли это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования и расшифрования и перестановка символов — в них для операций шифрования и расшифрования и неточто в них для шифрования и расшифрования и расшифрования и неточто в них для шифрования и расшифрования и расшифрования и расшифрования и неточто в них для шифрования и неточто в ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
 6. Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и расшифрования иглользуется два разных ключа — открытый и закрытый — в них для шифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВЅ)? 			
 «сумма по модулю 2» для шестнадцатеричных чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и готкрытый и закрытый — в них для шифрования и расшифрования и насшифрования и готкрытый и закрытый — в них для шифрования и расшифрования и насшифрования и расшифрования и готкрытый и закрытый — в них для шифрования и расшифрования и насшифрования и расшифрования и генерации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)? 	6		10000010
чисел 0В5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?	0.		10000010
Двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и соткрытый — в них для операций шифрования и расшифрования и расшифрования информации используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид 7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования и расшифрования и другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и расшифрования и от же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)? нет нет нет нет нет			
тисла необходимо сначала перевести в двоичный вид Может ли шифр с конечным ключом быть совершенным?			
7. Может ли шифр с конечным ключом быть совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и спользуется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования и информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?		_ ·	
совершенным? — да, если это алгоритм шифрования с открытым ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и стользуется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?	7.		нет
ключом — в зависимости от параметров шифра — нет — да 8. Что общего имеют все методы шифрования с закрытым ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования и готкрытый и закрытый — в них для шифрования и расшифрования и ниформации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
В зависимости от параметров шифра нет нет да Ито общего имеют все методы шифрования с закрытым ключом? в них для шифрования информации используется один ключ, а для расшифрования – другой ключ в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ Яля чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)? В них для шифрования и генерации псевдослучайных чисел		 да, если это алгоритм шифрования с открытым 	
Что общего имеют все методы шифрования с закрытым ключом? них для шифрования информации используется один ключ, а для расшифрования информации используется один ключ, а для расшифрования информации используется один и тот же ключ них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый них для шифрования и расшифрования информации используется один и тот же ключ 7. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?		ключом	
То общего имеют все методы шифрования с закрытым ключом?		 в зависимости от параметров шифра 	
8. Что общего имеют все методы шифрования с закрытым ключом?		– нет	
ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)?		– да	
ключом? — в них для шифрования информации используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)?			
в них для шифрования информации используется один ключ, а для расшифрования — другой ключ в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)? тенерации псевдослучайных чисел	8.	Что общего имеют все методы шифрования с закрытым	в них для шифрования и
используется один ключ, а для расшифрования — другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел		ключом?	
другой ключ — в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел		– в них для шифрования информации	
в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел		используется один ключ, а для расшифрования –	один и тот же ключ
на блоки, в каждом из которых выполняется перестановка символов — в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел			
перестановка символов — в них для операций шифрования и расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (ВВS)?			
в них для операций шифрования и расшифрования используется два разных ключа открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел		_	
расшифрования используется два разных ключа — открытый и закрытый — в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел		_	
		<u> </u>	
в них для шифрования и расшифрования информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)? генерации псевдослучайных чисел			
информации используется один и тот же ключ 9. Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)? генерации псевдослучайных чисел			
9. Для чего предназначен алгоритм Блюм-Блюма-Шуба генерации псевдослучайных чисел			
(BBS)? псевдослучайных чисел	_		
	9.	_ · · · · · · · · · · · · · · · · · · ·	=
– генерации псевдослучайных чисел			псевдослучайных чисел
		 генерации псевдослучайных чисел 	

	 для сжатия информации 	
	 для формирования открытых ключей 	
	 для формирования хеш-кода 	
10.	Выберите вариант ответа, содержащий только простые	2, 5, 19, 37, 59, 101
	числа	
	- 2, 5, 19, 37, 59, 101	
	- 2, 7, 17, 37, 57, 107	
	- 2, 5, 19, 37, 59, 133	
	- 3, 7, 19, 39, 59, 10	
11.	К правовым методам, обеспечивающим	Разработка и
	информационную безопасность, относятся:	конкретизация правовых
	 Разработка аппаратных средств обеспечения 	нормативных актов
	правовых данных	обеспечения безопасности
	 Разработка и установка во всех компьютерных 	
	правовых сетях журналов учета действий	
	 Разработка и конкретизация правовых 	
	нормативных актов обеспечения безопасности	
12.	Основными источниками угроз информационной	Перехват данных,
14.	безопасности являются все указанное в списке:	хищение данных,
	 Хищение жестких дисков, подключение к сети, 	изменение архитектуры
	 – Хищение жестких дисков, подключение к сети, инсайдерство 	системы
	±	CHCICMBI
	 Перехват данных, хищение данных, изменение 	
	архитектуры системы	
	 Хищение данных, подкуп системных 	
	администраторов, нарушение регламента	
12	работы	H
13.	Виды информационной безопасности:	Персональная,
	 Персональная, корпоративная, государственная 	корпоративная,
	 Клиентская, серверная, сетевая 	государственная
	Помоничес писбоничес сменичес	
	 Локальная, глобальная, смешанная 	
14.	Цели информационной безопасности – своевременное	
14.	Цели информационной безопасности – своевременное обнаружение, предупреждение:	
14.	Цели информационной безопасности – своевременное	
14.	Цели информационной безопасности – своевременное обнаружение, предупреждение:	
14.	Цели информационной безопасности – своевременное обнаружение, предупреждение:несанкционированного доступа, воздействия в	
14.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети 	
14.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации 	Компьютерные сети, базы
	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций 	Компьютерные сети, базы данных
	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных 	_
	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: 	_
	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей 	_
	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое 	_
	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы 	данных
15.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие 	Потеря, искажение,
15.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы Основными рисками информационной безопасности являются: 	данных
15.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы Основными рисками информационной безопасности являются: Искажение, уменьшение объема, перекодировка 	Потеря, искажение,
15.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы Основными рисками информационной безопасности являются: Искажение, уменьшение объема, перекодировка информации 	Потеря, искажение,
15.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы Основными рисками информационной безопасности являются: Искажение, уменьшение объема, перекодировка информации Техническое вмешательство, выведение из 	Потеря, искажение,
15.	 Цели информационной безопасности – своевременное обнаружение, предупреждение: несанкционированного доступа, воздействия в сети инсайдерства в организации чрезвычайных ситуаций Основные объекты информационной безопасности: Компьютерные сети, базы данных Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы Основными рисками информационной безопасности являются: Искажение, уменьшение объема, перекодировка информации 	Потеря, искажение,

17.	К основным принципам обеспечения информационной	Экономической
17.	безопасности относится:	эффективности системы
	 Экономической эффективности системы 	безопасности
	безопасности	
	 - Многоплатформенной реализации системы 	
	 Усиления защищенности всех звеньев системы 	
18.	Основными субъектами информационной	органы права,
10.	безопасности являются:	государства, бизнеса
	 руководители, менеджеры, администраторы 	
	компаний	
	 органы права, государства, бизнеса 	
	 сетевые базы данных, фаерволлы 	
19.	К основным функциям системы безопасности можно	Установление регламента,
	отнести все перечисленное:	аудит системы, выявление
	– Установление регламента, аудит системы,	рисков
	выявление рисков	
	- Установка новых офисных приложений, смена	
	хостинг-компании	
	 Внедрение аутентификации, проверки 	
	контактных данных пользователей	
20.	Принципом информационной безопасности является	Неоправданных
	принцип недопущения:	ограничений при работе в
	 Неоправданных ограничений при работе в сети 	сети (системе)
	(системе)	
	 Рисков безопасности сети, системы 	
21.	 Презумпции секретности Принципом политики информационной безопасности 	Невозможности миновать
21.	является принцип:	защитные средства сети
	 Невозможности миновать защитные средства 	(системы)
	сети (системы)	(energing)
	 Усиления основного звена сети, системы 	
	 Полного блокирования доступа при риск- 	
	ситуациях	
22.	Принцип Кирхгофа:	Секретность закрытого
	 Секретность ключа определена секретностью 	сообщения определяется
	открытого сообщения	секретностью ключа
	- Секретность информации определена скоростью	
	передачи данных	
	 Секретность закрытого сообщения определяется 	
0.0	секретностью ключа	
23.	ЭЩС – ЭТО:	Электронно-цифровая
	 Электронно-цифровой преобразователь 	подпись
	 Электронно-цифровая подпись 	
24	 Электронно-цифровой процессор 	05
24.	Наиболее распространены угрозы информационной	Ошибки эксплуатации и
	безопасности корпоративной системы:	неумышленного
	 Покупка нелицензионного ПО 	изменения режима работы системы
	 Ошибки эксплуатации и неумышленного 	CHOTOMBI
	Ошиоки эксплуатации и неумышленного изменения режима работы системыСознательного внедрения сетевых вирусов	CHCTCMBI

25.	Наиболее распространены средства воздействия на	Runyell B cett
43.	сеть офиса:	Вирусы в сети,
	1	логические мины
	 Слабый трафик, информационный обман, 	(закладки), информационный
	вирусы в интернет	1
	 Вирусы в сети, логические мины (закладки), 	перехват
	информационный перехват	
	 Компьютерные сбои, изменение 	
	админстрирования, топологии	
26.	Утечкой информации в системе называется ситуация,	Потерей данных в
	характеризуемая:	системе
	 Потерей данных в системе 	
	 Изменением формы информации 	
	 Изменением содержания информации 	
27.	Угроза информационной системе (компьютерной сети)	Вероятное событие
	– это:	
	 Вероятное событие 	
	 Детерминированное (всегда определенное) 	
	событие	
	 Событие, происходящее периодически 	
28.	Информация, которую следует защищать (по	
	нормативам, правилам сети, системы) называется:	
	Регламентированной	
	– Правовой	
	Защищаемой	
29.	Разновидностями угроз безопасности (сети, системы)	Программные,
	являются все перчисленное в списке:	технические,
	 Программные, технические, организационные, 	организационные,
	технологические	технологические
	- Серверные, клиентские, спутниковые, наземные	
	 Личные, корпоративные, социальные, 	
	национальные	
30.	Что такое «минимальное кодовое расстояние»?	наименьшее из всех
	 характеристика помехоустойчивого кода, 	расстояний по Хэммингу
	показывающая, насколько увеличена длина	для любых пар различных
	кодового слова по сравнению с обычным	кодовых слов,
	непомехоустойчивым кодом	образующих код
	 число разрядов двух кодовых слов, в которых 	
	они различны	
	 число контрольных разрядов в кодовом слове 	
	 наименьшее из всех расстояний по Хэммингу 	
	– наименьшее из всех расстоянии по хэммингу для любых пар различных кодовых слов,	
	для люоых пар различных кодовых слов, образующих код	
	ооразующих код 1. Критерии опенивания компетенций*	

1. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он

Понимает средства защиты информации; угрозы безопасности информации в компьютерных системах;

Решает основные этапы построения систем безопасности корпоративных систем; Применяет основные этапы создания комплексной системы защиты информации; Понимает интегрированную систему информационной безопасности; защита документооборота в вычислительных системах; средства защиты информации;

применяет моделирования комплексных систем защиты информации; методы оценки систем защиты информации;

применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографические средства защиты;

Оценка «хорошо» выставляется студенту, если он

Осознает задачи профессиональной деятельности с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности;

Решает задачи профессиональной деятельности с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности

Применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Использует методы функциональной безопасности корпоративных систем; применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «удовлетворительно» выставляется студенту, если он

Слабо осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Слабо применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Слабо понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Слабо использует методы функциональной безопасности корпоративных систем;

Слабо применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;

Оценка «неудовлетворительно» выставляется студенту, если он

Не удовлетворительно осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Не удовлетворительно применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Не удовлетворительно понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;

Не удовлетворительно использует методы функциональной безопасности корпоративных систем;

Не удовлетворительно применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;