МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерных сетей

УТВЕРЖДАЮ
Декан факультета ИВТ
_____ Д.Ю. Чалый
«__18__»_____мая___2021 г.

Рабочая программа дисциплины
«Информационная безопасность»

Направление подготовки
09.03.03 Прикладная информатика

Профиль
«Информационные технологии в цифровой экономике»

Квалификация выпускника
Бакалавр

Форма обучения
очная

Программа рассмотрена
на заседании кафедры
от 27 апреля 2021 г.,
протокол № 9

Программа одобрена НМК
факультета ИВТ
протокол № 7 от
17 мая 2021 года

Ярославль
2021

1. Цели освоения дисциплины

Целями дисциплины «Информационная безопасность» являются:

– освоение теоретических основ современных методов применяемых при решении задачи информационной безопасности;

– формирование конкретных практических навыков информационной безопасностив компьютерных технологиях.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Для освоения данной дисциплиной студенты должны обладать знаниями по математике и информатике в объеме школьной программы, проявлять настойчивость, целеустремленность и инициативу в процессе обучения. Для программной реализации алгоритмов студенты должны иметь понятие об одном из языков программирования.

Полученные в рамках дисциплины знания необходимы для развития алгоритмического мышления, развития навыков решения сложных задач.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.1 демонстрирует навыки использования научных и образовательных ресурсов сети интернет для разработки программ и программной документации с учетом требования информационной безопасности	Знать: } некоторые криптографические алгоритмы; } некоторые хэш функции. Уметь: } реализовывать некоторые криптографические алгоритмы Владеть навыками: } вычислять хэш значение; } создавать ЭЦП.
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.1. демонстрирует способность участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Знать: } юридические вопросы информационной безопасности } о каналах утечки информации, их классификация. Уметь: } уметь выполнять передачу или генерацию ключей. } реализовывать некоторые криптографические алгоритмы Владеть навыками: } построения модели информационной безопасности.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зач.ед., 180 акад.час.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.	Определение безопасности.	7	1	1				5	
2.	Каналы утечки информации, их классификация.	7	2	2				5	
3.	Модели информационной безопасности.	7	2	2		1		5	Самостоятельная работа
4.	Аутентикация, авторизация, пароли.	7	2	2		1		5,7	Самостоятельная работа
5.	Асимметричные шифры. Электронные цифровые подписи	7	6	6		1		8	Самостоятельная работа
6.	Безопасность программного обеспечения	7	2	2				2	Контрольная работа №1
7.	Стандарты и спецификации в области информационной безопасности.	7	2	2				2	
	в том числе с ЭО и ДОТ							*2*	Тест для самопроверки по результатам освоения дисциплины *ЭУК в LMS Moodle*
	Всего за 7 семестр 72 часов		**17**	**17**		**3**	**0,3**	**34,7**	**Зачет**
8.	Шифрование. Симметричные шифры.	8		14		2		13	Самостоятельная работа
9.	Юридические вопросы	8							

	информационной безопасности								
10.	Хэш-функции	8		7		1		9	Самостоятельная работа
11.	Поточные шифры	8		3		1		8	Контрольная работа №2
	в том числе с ЭО и ДОТ							*2*	Тест для самопроверки по результатам освоения дисциплины *ЭУК в LMS Moodle*
							0,5		**Экзамен**
	Всего за 8 семестр 108 часов			**24**		**4**	**0,5**	**32**	
	Итого		**17**	**41**		**7**	**0,8**	**67,2**	

Содержание разделов дисциплины:

Раздел 1. Определение безопасности.

Определение информации, данных, знаний. Определение безопасности. Несанкционированный доступ. Информационные системы. Доступность, целостность, конфиденциальность. Основные понятия об угрозах.

Раздел 2. Каналы утечки информации, их классификация.

Каналы утечки информации технических средств обработки, хранения и передачи информации. Каналы утечки речевой информации. Каналы утечки информации при её передаче по каналам связи. Технические каналы утечки видовой информации. Каналы утечки информации, создаваемые атаками извне и внутрикорпоративных систем ИКТ

Раздел 3. Модели защиты информации.

Модели разграничения доступа по принципу предоставления прав. Модели дискретного доступа. Вероятностные модели. Информационные модели. Модель мандатного доступа. Модель Бела-Лападулы, игровая модель. Матрица доступов.

Раздел 4. Аутентикация, авторизация, пароли.

Аутентикация, авторизация, пароли, токены, "рукопожатие". Протоколы аутентификации без передачи секретной информации, одноразовые ключи. Доказательство с нулевым знанием.

Раздел 5. Асимметричные шифры. Электронные цифровые подписи.

Асимметричные шифры, шифры с открытым ключом.Электронные цифровые подписи. Трудоемкость дешифрования. Рюкзачная криптосистема. Алгоритм RSA. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Алгоритм Эль-Гамаля. Алгоритм Рабина.

Раздел 6. Безопасность программного обеспечения.

Введение в защиту ПО. Угрозы безопасности ПО. Примеры уязвимостей ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО. Компьютерные вирусы и антивирусные программы.

Раздел 7.Стандарты и спецификации в области информационной безопасности.

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800

Раздел 8. Шифрование. Симметричные шифры.

Шифрование. Терминология шифрования. Трудоемкость дешифрования. Симметричные шифры. Рюкзачная криптосистема. Схема Фейстеля,SP-сеть.Режимы шифрования, гаммирование. Алгоритмы AES, Гост28147-89, DES, Serpent, Mars

Раздел 9. Юридические вопросы информационной безопасности

Понятие о законодательном уровне информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон «Об информации, информатизации и защите информации». Другие законы и нормативные акты.

Раздел 10. Хэш-функции

Свойства криптографических хэш-функций. Их использование в протоколах аутентификации и для контроля изменения чувствительной информации. Хэш-функции MD5, SHA1.

Раздел 11. Поточные шифры

Генераторы случайных и псевдослучайных чисел, их использование при аутентификации. Криптографические ГПСЧ, их свойства. Виды поточных шифров. Трудоемкость дешифрования. Генератор LFSR, и его модификации. Алгоритмы A5, RC4

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации, для разработки документов, презентаций, для работы с электронными таблицами -

программы OfficeStd 2013 RUSOLPNLAcdmc 021-10232, LibreOffice (свободное), издательская система LaTeX;

- компиляторы с высокоуровневых языков программирования;

– для поиска учебной литературы библиотеки ЯрГУ–Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная:

1. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968 (дата обращения: 24.11.2021).

2. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470279 (дата обращения: 24.11.2021)

3. *Лось, А. Б.* Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469133 (дата обращения: 24.11.2021).

б) дополнительная:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/473348 (дата обращения: 24.11.2021).

1. Блэк, У., Интернет протоколы безопасности : учеб. курс / У. Блэк ; пер. с англ., СПб., Питер, 2001, 282с

2. Ярочкин, В. И., Информационная безопасность : учебник для вузов, М., Международные отноше, 2000, 399с

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Аудитории, оборудованные для проведения лекций, практических занятий и консультаций,фонд библиотеки, компьютерная техника.

Автор(ы) :

Доцент кафедры компьютерных сетей, к.ф.-м.н. _____ М.В.Краснов

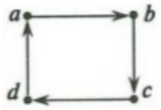
Приложение №1 к рабочей программе дисциплины
«Информационная безопасность»
Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

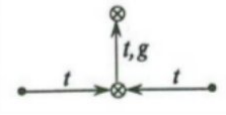
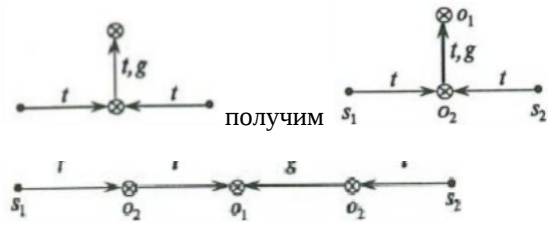
1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1. Контрольные задания и иные материалы,используемые в процессе текущей аттестации

Заданиядля самостоятельной работы

Пример заданийдля самостоятельной работык разделу3
(проверка ОПК-4)

Задания	Ответы:
1.Задает ли решетку граф 	Напомним несколько определений: Опр1. Бинарное отношение «$\pounds$» на множестве X назовемотношением частичного порядка, когда для любых $a,b,c \in X$ выполняются три свойства: - рефлексивность $a \pounds a$; - транзитивность $(a \pounds b, b \pounds c) \Rightarrow (a \pounds c)$ - антисимметричность $(a \pounds b, b \pounds a) \Rightarrow (a = b)$ Опр2. Для $a,b \in X$ элемент $c = a \wedge b \in X$ называется наименьшей верхней границей, когда выполняются условия: - $a \pounds c, b \pounds c$ - для $d \in X$ истинно $(a \pounds d, b \pounds d) \Rightarrow (c \pounds d)$ Опр 3. Для $a,b \in X$ элемент $c = a \vee b \in X$ называется наибольшей нижней границей, когда выполняются условия: - $c \pounds a, c \pounds b$ - для $d \in X$ истинно $(d \pounds a, d \pounds b) \Rightarrow (d \pounds c)$ Опр 4. Пусть X - частично упорядоченное множество. $(X, \pounds)$ - называется решеткой, когда для любых существуют и $a \wedge b \in X$ Рассмотрим заданный граф Выполняются условия: $(a \pounds b, b \pounds c) \Rightarrow (a \pounds c)$ $(a \pounds c, c \pounds d) \Rightarrow (a \pounds d)$ $(a \pounds d, d \pounds a) \Rightarrow (a = d)$, но $a \neq d$ и в соответствии с Опр1 не выполняется свойство антисимметричности отношения частичного порядка «$\pounds$» на множестве $\{a,b,c,d\}$. Следовательно, по Опр2 граф не задает решетку.
2.Модель Харрисона-Руззо-Ульмана (ХРУ) Сформулируйте команду создания субъектом s личного файла f	CommandCreateFile(s, f) «создать» объект f; «внести» право владения ownв $M[s, f]$; «внести» право чтение readв $M[s, f]$; «внести» право запись writeв $M[s, f]$; End.
3.Классическая модель Take-Grant. Проверьте, является ли мостом граф доступов	Опр Мостом в графе доступов G_0 называется tg-путь, концами которого являются вершины субъекты, проходящий через вершины объекты, словарная запись которого имеет вид $t^*, t^* g t^*, t^* g t^*$,где * означает многократное (в том числе нулевое) повторение. Используем следующие обозначения для вершин графа доступов s_1, s_2 - субъекты; o_1, o_2 - объекты

	 получим Так как в определении нет ограничений на повтор объектов на мосту, то граф доступов задает мост со словарной записью r,t,g,t,r с концами в вершинах-субъектах s_1, s_2 и проходящий через объекты o_2, o_1, o_2.

Критериоценивания

Номер задачи	Критерии	Шкала оценивания
1	*Владеть навыками:*построение модели информационной безопасности.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	*Владеть навыками:* построение модели информационной безопасности	0 баллов – студент полностью не верно решил задачу 2 балла – студент полностью разобрался в решении задачи
3	*Владеть навыками:* построение модели информационной безопасности	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 3 баллов— оценка «неудовлетворительно»;
- от 3 до 4 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- 5 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 6 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу 4

(проверка ОПК-4)

Задания	Ответы:
1.Приведите пример работы протокола типа «точка-точка» Предположим, что пользователи A и обладают общей секретной информацией (секретным ключом k_{AB}).	Два варианта ответа: 1. передачу сеансового ключа можно описать следующей символьной записью: $A \to B: \quad E_{k_{AB}}(k,T,b)$ которая означает, что пользователь A создал сеансовый ключ k и отправил пользователю B сообщение $E_{k_{AB}}(k,T,b)$ где $E_{k_{AB}}$ - алгоритм шифрования с ключом k_{AB}, - сеансовый ключ, T - временная метка, b-идентификатор пользователя . Зная секретный ключ k_{AB} пользователь B легко может найти ключ k. 2. Если дополнительно требуется аутентификация сеанса, то можно использовать протокол, состоящий из следующих действий: a) $B \to A: \quad r_B$ b) $A \to B: \quad E_{k_{AB}}(k,r_B,T,b)$

	где запись $B \to A: r_B$ означает, что пользователь B сгенерировал случайное число r_B и отправил его пользователю A; запись $A \to B: E_{k_{AB}}(k, r_B, T, b)$ означает, что пользователь A создал сеансовый ключ k и отправил пользователю B сообщение $E_{k_{AB}}(k, r_B, T, b)$ где $E_{k_{AB}}$ - алгоритм шифрования с ключом k_{AB}, - сеансовый ключ, T - временная метка, b-идентификатор пользователя B. Зная секретный ключ k_{AB} пользователь B легко может найти ключ k, а по числу r_B убедиться, что его послал пользовать A.
2. Есть два пользователя A B используя протокол DIFFIE-HELLMAN сгенерируйте общий секретный ключ	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A и B выбирают в открытом доступе большое простое число n и g, где g образующий элемент мультипликативной группы Z_n^*. Пусть $n = 13$ и $g = 2$ 2. Пользователь A выбирает случайное большое натуральное число x и отправляет пользователю B величину $X = g^x \bmod n$; Пусть $x = 5$ и $X = 6$ 3. Пользователь B выбирает случайное большое натуральноечисло y и отправляет пользователю A величину $Y = g^y \bmod n$; Пусть $y = 7$ и $Y = 11$ 4. Пользователь A вычисляет величину $k = Y^x \bmod n$; Вычисляем $k = 11^5 \bmod 13 = 7$ 5. Пользователь B вычисляет величину $\tilde{k} = X^y \bmod n$. Вычисляем $\tilde{k} = 6^7 \bmod 13 = 7$ Получили $\tilde{k} = k = 7$
3. Есть два пользователя A B используя протокол MTI сгенерируйте общий секретный ключ	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A и B выбирают в открытом доступе большое простое число n и g, где g образующий элемент мультипликативной группы Z_n^*. Пусть $n = 13$ и $g = 2$ 2. Пользователи A и B должны сгенерировать секретные ключи $a, 1 \le a \le n-2$, и $b, 1 \le b \le n-2$, соответственно, и публикуют свои открытые ключи $z_A = g^a \bmod n$ и $z_B = g^b \bmod n$; Пусть Пользователь A генерирует число $a = 5$ и публикует $z_A = 2^5 \bmod 13 = 6$, соответственно пользователь B генерирует число $b = 3$ и публикует $z_B = 2^3 \bmod 13 = 8$; 3. Пользователь A выбирает случайное натуральное число x, $1 \le x \le n-2$ и отправляет пользователю B величину $X = g^x \bmod n$; Пусть пользователь A генерирует число $x = 2$ и отправляет пользователю B величину $X = 2^2 \bmod 13 = 4$; 4. Пользователь B выбирает случайное большое натуральное число $, 1 \le y \le n-2$ и отправляет пользователю A величину $Y = g^y \bmod n$; Пусть пользователь B генерирует число $y = 4$ и отправляет

	пользователю величину $Y = 2^4 \bmod 13 = 3$; 5. Пользователь A вычисляет величину $k = Y^a z_B^x \bmod n$; Пусть пользователь A на настоящий момент знает величины: $n, g, a, z_A, z_B, x, X, Y$. Пользователь A вычисляет величину $k = \left(Y^a z_B^x\right) \bmod n = \left(3^3 8^2\right) \bmod 13 = (9*12) \bmod 13 = 4$ 6. Пользователь B вычисляет величину $\tilde{k} = X^b z_A^y \bmod n$. Пусть пользователь B на настоящий момент знает величины: $n, g, b, z_A, z_B, y, X, Y$. Пользователь B вычисляет величину $\tilde{k} = \left(X^b z_A^y\right) \bmod n = \left(4^3 6^4\right) \bmod 13 = 12*9 \bmod 13 = 4$ Получили $\tilde{k} = k = 4$
4. Постройте схему разделения секрета на примере пороговой схемы Шамира (n,t), где $n=5, t=3$. В качестве конечного поля возьмем Z_{13}, секретной информацией будем считать число 11	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема разделения секрета включает два протокола: • протокол формирования частичных секретов и распределения их между пользователями; • протокол восстановления секрета группой пользователей. В качестве примера рассмотрим пороговую схему Шамира. Для построения пороговой схемы (n,t) Шамир воспользовался многочленами вида $f(x) = b_{t-1}x^{t-1} + b_{t-2}x^{t-2} + \mathrm{K} + b_1 x + b_0$ в конечном поле. Секретным считается свободный член b_0. В качестве конечного поля возьмем Z_{13}, а в качестве многочлена,на котором основана схема Шамира $(5,3)$; возьмем $f(x) = \left(7x^2 + 8x + 11\right) \bmod 13$. • протокол формирования частичных секретов состоит в вычислении $f(x)$ $a_1 = f(1) = (7 + 8 + 11) \bmod 13 = 0$; $a_2 = f(2) = (28 + 16 + 11) \bmod 13 = 3$; $a_3 = f(3) = (63 + 24 + 11) \bmod 13 = 7$; $a_4 = f(4) = (112 + 32 + 11) \bmod 13 = 12$; $a_5 = f(5) = (175 + 40 + 11) \bmod 13 = 5$. • протокол восстановления секрета группой пользователей из t человек. Чтобы восстановить $f(x)$ из трех частичных секретов a_2, a_3, a_5. Будем считать, что нам дано тогда решается система линейных уравнений: $\begin{cases} f(2) = \left(4b_2 + 2b_1 + b_0\right) \bmod 13 = 3 \\ f(3) = \left(9b_2 + 3b_1 + b_0\right) \bmod 13 = 7 \\ f(5) = \left(25b_2 + 5b_1 + b_0\right) \bmod 13 = 5 \end{cases}$ Решением будет $b_2 = 7, b_1 = 8, b_0 = 11$.

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью неверно решил задачу

		1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или была допущена вычислительная ошибка. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или была допущена вычислительная ошибка.. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или была допущена вычислительная ошибка.. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно»;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу5

(проверка ОПК-3)

Задания	Ответы:
1. Вычислить $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 3 \mod 11 \\ x \equiv 7 \mod 13 \end{cases}$	Напомним процесс вычисления.Пусть задано: множество натуральных чисел $(m_1, m_2, ..., m_k)$не равныхединице, которые являются попарно взаимно простыми множество натуральных чисел $(b_1, b_2, ..., b_k)$.Системасравнений $\begin{cases} x \equiv b_1 \mod m_1 \\ ... \\ x \equiv b_k \mod m_k \end{cases}$ имеет решение $x = x_0 \mod(m_1 m_2 ... m_k)$; где $x_0 = M_1 M_1^{-1} b_1 + ... + M_k M_k^{-1} b_k$; числа M_s и M_s^{-1} определяется изусловий $m_1 m_2 ... m_k = M_s m_s$, $M_s M_s^{-1} = 1 \mod m_s$ Рассмотрим наше уравнение $M_1 = 5005, M_2 = 3003, M_3 = 2145, M_4 = 1365, M_5 = 1155.$ $M_1^{-1} = 1, M_2^{-1} = 2, M_3^{-1} = 5, M_4^{-1} = 1, M_5^{-1} = 6.$ $m_1 m_2 ... m_5 = 15015$ $x_0 = 5005*1*1 + 3003*2*2 + 2145*5*3 +$ $+ 1365*3*1 + 1155*6*7 = 101797$ $x = 11707$
2.Построить криптосистемуЭль-Гамаляи закодируйте число 7	Числовые значения могут отличаться от тех, которые приведены в данном решении Криптосистема Эль-Гамаля строится следующим образом:

	• сначала выбирается большое простое число p • выбирается число a которое является примитивным для Z_p • выбирается случайное натуральноечисло x, причем $x < p$ • вычисляем $y = g^x \bmod p$ Для того чтобы зашифровать сообщение M надо выполнить следующие действия: • выбрать случайное натуральное число k, $1 < k < p-1$, такое что числа k и $p-1$ взаимно простые. • вычислить $a = q^k \bmod p$ и $b = (y^k M) \bmod p$. Пара чисел (a,b) и есть шифрованный текст Для того чтобы расшифровать сообщение, надо вычислить $M = \frac{b}{a^x} \bmod p$. Построим криптосистему Эль-Гамаля и закодируем число 7 Строим криптосистему • выбираем $p = 13; q = 2$, выбираемсекретный ключ $x = 8$ • вычисляем $y = 2^8 \bmod 13 = 9$ Для того чтобы зашифровать сообщение $M = 7$ надо выполнить следующие действия: • выбрать случайное натуральное число $k = 7$ заметим, что числа 7 и 12 взаимно простые. • вычислить $a = 2^7 \bmod 13 = 11$ и $b = (9^7 * 7) \bmod 13 = 11$. Шифрованный текст – пара чисел (11,11)
3. Сформулировать алгоритм установки ЭЦП DSA. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема DSA строится следующим образом: • сначала выбирается большое простое число p • выбирается простое число q которое является делителем $p-1$ • выбирается натуральноечисло t которое $0 < t < p$. Если число $t^{\frac{p-1}{q}} = 1 \bmod p$, то выбираем другое число t. В противном случае $g = t^{\frac{p-1}{q}} \bmod p$. • выбирается натуральноечисло x, которое является секретным ключом причем $1 < x < q$ • вычисляем $y = g^x \bmod p$ Установка подписи: • проверяем выполняется ли условие для хэш значение m текста M, что $0 < m < q$ • выбирается натуральноечисло k, $(0 < k < q)$. • вычисляем k^{-1}, для которого выполняется условие $k * k^{-1} = 1 \bmod q$ • вычисляем два числа r и s по следующим правилам: $r = (k^d \bmod p) \bmod q$ и $s = k^{-1}(xr + m) \bmod q$ Если не выполняются условия $0 < r < q, 0 < s < q$ поменяйте входные параметры.

	Подписью является пара чисел (r, s) Проверка подписи Предположим, что к нам пришло сообщение M с хэш значением m и подписью (r', s') • если хотя бы одно из условий $0 < r' < q, 0 < s' < q$ не выполняется, то подпись считается недействительной • вычисляем $v = (s')^{-1} \bmod q$ • вычисляем: $z_1 = (m \cdot v) \bmod q$ $z_2 = (r' \cdot v) \bmod q$ $u = \left((g^{z_1} y^{z_2}) \bmod p\right) \bmod q$ • проверяем условие $r' = u$. Если оно выполняется то подпись считается подлинной а сообщение –неизмененным. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA. Строим схему DSA • выбираем $p = 23, q = 11, r = 3$ • вычисляем $g = 3^2 \bmod 23 = 9$ • выбираем $x = 2$ • вычисляем $y = 9^2 \bmod 23 = 12$ Установка подписи: • выбираем $k = 4$ • вычисляем: $k^{-1} = 3$, $r = (9^4 \bmod 23) \bmod 11 = 6$, $s = (3 * (2 * 6 + 7)) \bmod 11 = 2$ Подписью является пара чисел $(6, 2)$
4. Применяя расширенный алгоритм Евклида: а) найти d, x, y для которых выполняется $d = НОД(a,b) = ax + by$, где a=342; b=612 b) найти q для которого выполняется $8q \bmod 101 = 1$	а) 18=342*9+612*(-5), следовательно $d = 18, x = 9, y = -5$ b) После применении расширенного алгоритма Евклида $d = НОД(a,b) = ax + by$, где $a = 101, b = 8$. Мы получим: $1 = НОД(101,8) = 101 * (-3) + 8 * 38$, возьмем указанное выражение по модулю 101. В результате $(101 * (-3) + 8 * 38) \bmod 101 = (8 * 38) \bmod 101 = q = 38$

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:* создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:* создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил

		вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:*создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:*создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил только одноподзадачу. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно»;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу 8

(проверка ОПК-3)

Задания	Ответы:
1.Постройте аффинную криптосистему $f(x)=(ax+b)\bmod m,$ для русского алфавита. Закодируйте слово «кокос»	Числовые значения могут отличаться от тех, которые приведены в данном решении Напомним, что аффинная криптосистема определяется тремя натуральными числами $a,b,m.$ Шифрование происходит заменой символа с порядковым номером xна символ порядковыйномер которого вычисляется по формуле $f(x)=(ax+b)\bmod m.$Заметим, что на пару чисел aи m наложено условие взаимной простоты. Закодируйте слово «кокос». Будем рассматривать $f(x)=(5x+2)\bmod 33.$Нам надо закодировать $(11,15,11,15,18).$В результате получим $(24,11,24,11,26).$
2. Взломайте аффинную криптосистему $f(x)=(ax+b)\bmod m,$ для русского алфавита. Известно, что в исходном тексте чаще всего встречаются символы с порядковыми номерами 10 и 15, а в шифрованном тексте с порядковыми номерами 7 и 12.	Нам надо решить систему $\begin{cases}10a+b=7\bmod 33\\15a+b=12\bmod 33\end{cases}$ или $\begin{cases}10a+b=12\bmod 33\\15a+b=7\bmod 33\end{cases}$ Ответ $a=1\quad b=30$ или $a=32\quad b=22$
3. Выполните операцию умножения байтов в поле $GF(2^8),$ которая используется в алгоритме AES. x^7+x+1и $x^6+x^4+x^2+x+1$	Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8).$Поскольку байты оперируют в поле $GF(2^8),$ то заданы операции сложения и умножения: • сложение - суть операция поразрядного XOR. • умножение- это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена $J(x)$ и использованием операции XOR при приведении подобных членов. В качестве неприводимого многочлена $J(x)=x^8+x^7+x^3+x+1.$

	Выполняем умножение $((x^7 + x + 1) * (x^6 + x^4 + x^2 + x + 1)) \mod(x^8 + x^4 + x^3 + x + 1) =$ $= x^7 + x^6 + 1.$
4. Примените процедуру MixColunmsалгоритма AES к вектору $(e0, b4, 52, ae)$, результат запишите в виде четырехбайтового слова	ПроцедураMixColunms, одна из процедур используемых в раунде алгоритма AES. Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$.Поскольку байты оперируют в поле $GF(2^8)$, то заданы операции сложения и умножения: • сложение Â - суть операция поразрядного XOR. • умножение- это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена J (x) и использованием операции XOR при приведении подобных членов. В качестве неприводимого многочлена J (x) = $x^8 + x^4 + x^3 + x + 1$. Раундовые преобразования работают с четырехбайтовыми словами. Этому слову можно поставить в соответствие многочлен $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, где $a_i \in GF(2^8)$.Рассмотрим как будет происходить сложение и умножение четырехбайтовых слов $a(x)$ и $b(x)$, где $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0, b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$: • сложение $a(x) + b(x) = (a_3 Â b_3)x^3 + (a_2 Â b_2)x^2 + (a_1 Â b_1)x + (a_0 Â b_0)$ • умножение Для того, чтобы результат умножения был снова представлен в виде четырехбайтового слова, его надо взять по модулю многочлена Следовательно, в результате получим вектор $x^4 + 1$. $d(x) = d_3x^3 + d_2x^2 + d_1x + d_0$ ПроцедураMixColunmsалгоритма AESсостоит из трех операций: • вектор записывается как многочлен вида • мы должны вычислить где $d(x) = a(x) Â g(x).$ • записать многочлен виде вектора Решение • вектор , записываем как многочлен $(e0, b4, 52, ae)$ • вычисляем $a(x) = \{ae\}x^3 + \{52\}x^2 + \{b4\}x + \{e0\}$. • записываем ответ $d(x) = a(x) Â g(x)$ $(e0, eb, 19, 9a)$

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил одну вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи

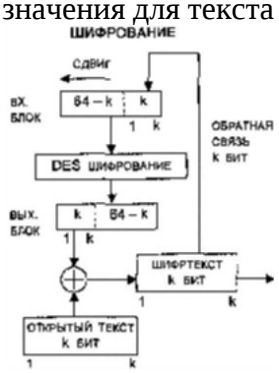
2	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи
3	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно»;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданийдля самостоятельной работык разделу10

(проверка ОПК-3)

Задания	Ответы:
1.Дайте определение хэш-функции	Хэш-функция h — это функция, определенная на битовых строках произвольной длины со значениями в строках битов фиксированной длины.. Хэш-функция h() принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение h(M) = H фиксированной длины. Предполагается, что алгоритм вычисления хэш-значения является эффективным и общедоступным.
2.Укажите, каким условиям должна удовлетворять хэш-функция	Хэш-функция должна удовлетворять целому ряду условий: • хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки • хэш-функция должна обладать свойством необратимости, то есть задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно трудная; • вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала Проиллюстрируем, что условия накладываемые на хеш функцию очень важны Предположим, что есть два пользователя A и B **условие 1**хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки, предположим противное. Тогда фразы «Казнить, нельзя помиловать» и «Казнить нельзя, помиловать» будут иметь одно хэш-значение и текст можно подменить.

	Для иллюстрации оставшихся условий рассмотрим ЭЦП RSA. Дано текст M и его хэш-значение $h(M)$. Все параметры, которые используются в криптосистеме RSA. Установка подписи вычисляем: $S = h(M)^d \bmod n$ Проверка подписи: • вычисляем $Hc = S^e \bmod n$ • вычисляем $h(M)$ • проверяем равенство $Hc = h(M)$. Если оно верно, то подпись законна. **условие 2**это условие препятствует криптоаналитику фабриковать сообщение с данной подписью, предположим условие не выполняется. Тогда возможна следующая атака. - В вычисляет $Hc = R^e \bmod n$с некоторым выбранным наугад целым числом R. - Кроме того, В находит прообраз значения Hcпри отображении $h(\ )$, т.е. В определяет $M = h^{-1}(m')$. Теперь В обладает Вашей подписью R длясообщения М. **условие 3** вероятность того, что значения хэш-функций двух различных документов совпадут, должна быть ничтожно мала, предположим противное. Тогда возможна следующая атака - А выбирает два сообщения M и Mc удовлетворяющие соотношению $Hc = h(M) = h(Mc)$ - А подписывает M и получает (M, S) - Потом А отказывается от своего сообщения, утверждая, что посылал сообщение Mc
3. Основной принцип проектирования хэш-функции.	Основной принцип проектирования хэш-функции заключается в том, что ее значения должны производить лавинный эффект. Другими словами, небольшое изменение в аргументе хэш-функции должно очень сильно повлиять на ее значение.
4.Постройте однонаправленную хэш-функцию используя симметричный блочный алгоритм DES, хэш-значение состоит из k бит.	Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритмDES, например используя режим «обратная связь по шифру». Последний блок шифротекста можно рассматривать в качествехэш-значения для текста M. 

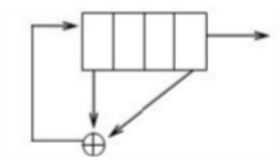
Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Владеть навыками:*вычислять хэш значение	0 баллов – студент полностью

		неверно решил задачу 2 балла – студент полностью верно дал определение.
2	*Владеть навыками:*вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	*Владеть навыками:*вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью верно дал определение.
4	*Владеть навыками:*вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения (без схемы шифрования). 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно»;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции

Пример заданийдля самостоятельной работык разделу 11
(проверка ОПК-3)

<table>
<tr><td>Задания</td><td>Ответы:</td></tr>
<tr><td>1. Постройтерегистр сдвига с линейной обратной связью с ассоциированным многочленом $x^4 + x + 1$ и выпишем состояние регистра, если он был инициализирован вектором $(1,1,1,1)$.</td><td> 
<table>
<tr><td colspan="2">Состояние регистра</td><td>выход</td><td colspan="2">Состояние регистра</td><td>выход</td></tr>
<tr><td>итерация</td><td>состояние рег. стало</td><td></td><td>итерация</td><td>состояние рег. стало</td><td></td></tr>
<tr><td>0</td><td>1111</td><td></td><td>9</td><td>0100</td><td>1</td></tr>
<tr><td>1</td><td>0111</td><td>1</td><td>10</td><td>0010</td><td>0</td></tr>
<tr><td>2</td><td>1011</td><td>1</td><td>11</td><td>0001</td><td>0</td></tr>
<tr><td>3</td><td>0101</td><td>1</td><td>12</td><td>1000</td><td>1</td></tr>
<tr><td>4</td><td>1010</td><td>1</td><td>13</td><td>1100</td><td>0</td></tr>
<tr><td>5</td><td>1101</td><td>0</td><td>14</td><td>1110</td><td>0</td></tr>
<tr><td>6</td><td>0110</td><td>1</td><td>15</td><td>1111</td><td>0</td></tr>
<tr><td>7</td><td>0011</td><td>0</td><td></td><td></td><td></td></tr>
<tr><td>8</td><td>1001</td><td>1</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2. Постройте10 битную псевдослучайную последовательность с помощью BBS-генератора.</td><td>Числовые значения могут отличаться от тех, которые приведены в данном решении
Напомним, что BBS-генератор строится следующим образом:
• вначале выбираются pи q- два больших простых числа примерно одинакового размера, причем $p \equiv 3 \bmod 4$ и $q \equiv 3 \bmod 4$.
• вычисляемчисло $n = pq$;</td></tr>
</table>

- выбираем случайное целое число x, что числа x и n являются взаимно простыми;
- вычисляем число $x_0 = x^2 \bmod n$, которое называется стартовым числом генератора;
- искомой последовательностью бит длиной m будет являться последовательность

$$BBS_{n,m}(x_0) = b_0 b_1 b_2 \text{K } b_i \text{K } b_{m-1}, \quad i = 0, \text{K}, m-1,$$

где b_i - младший бит числа x_i, $x_{i+1} = x_i^2 \bmod n$.

Постройте 10 битную псевдослучайную последовательность

- Пусть $p = 11, q = 19$, тогда $n = 209$. Пусть $x = 2$.
- Стартовое число генератора $x_0 = x^2 \bmod n$ Þ $x_0 = 2^2 \bmod 209$ Þ $x_0 = 4$.
- В качестве элементов псевдослучайной последовательности будем брать младший бит в двоичной записи чисел $x_{i+1} = x_i^2 \bmod n$

В результате получимпоследовательность $BBS_{209,10}(4) = 0011010001$

3. Создайте комбинирующий генератор, состоящий из двух регистров сдвига с линейной обратной связью.

Первый регистр с ассоциированным многочленом $x^6 + x + 1$, он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра y_1.

Второй регистр с ассоциированным многочленом $x^4 + x + 1$ он был инициализирован вектором $(1,1,1,1)$. Выход регистра y_2.

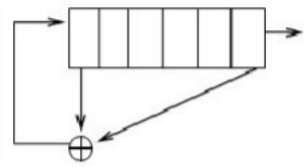
В качестве комбинирующей функции возьмем $f(y_1, y_2) = y_1 \text{Å } y_2$

Постройте 7 битную псевдослучайную последовательность

Напомним, что комбинирующий генератор проиллюстрировать следующей схемой

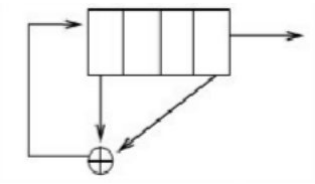
Решение

- Первыйрегистр



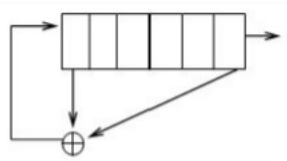
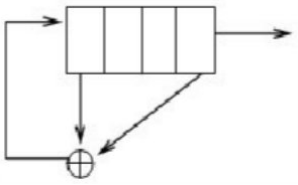
Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_1.	итерация	состояние рег. стало	y_1.
0	111111		4	101011	1
1	011111	1	5	010101	1
2	101111	1	6	101010	1
3	010111	1	7	110101	0

- Второй регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_2.	итерация	состояние рег. стало	y_2.
0	1111		4	1010	1
1	0111	1	5	1101	0
2	1011	1	6	0110	1
3	0101	1	7	0011	0

<table>
<tr><td></td><td>В результате получимпоследовательность 0000100</td></tr>
<tr><td>4. Создайте сжимающий генератор, состоящий из двух регистров сдвига с линейной обратной связью.
Первый регистр с ассоциированным многочленом $x^6 + x + 1$, он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра b_i.
Второй регистр с ассоциированным многочленом $x^4 + x + 1$ он был инициализирован вектором $(1,1,1,1)$. Выход регистра c_i.
Постройте 7 битную псевдослучайную последовательность</td><td>Напомним, что сжимающий генератор описывается следующей образом:
Используется 2 регистра с линейной обратной связью. Тактовые импульсы поступают на оба LFSR. Предположим, что
$b = b_0 b_1 b_2 \mathrm{K}$ последовательность с выхода LFSR1.
$c = c_0 c_1 c_2 \mathrm{K}$ - последовательность с выхода LFSR2,
Тогда результирующая последовательность $z = z_0 z_1 z_2 \mathrm{K}$ включает в себя те биты b_i, для которых соответствующие биты $c_i = 1$. Остальные биты последовательности b игнорируются.

Решение
• Первыйрегистр
 
<table><tr><td colspan="2">Состояние регистра</td><td>выход</td><td colspan="2">Состояние регистра</td><td>выход</td></tr><tr><td>итерация</td><td>состояние рег. стало</td><td>b_i</td><td>итерация</td><td>состояние рег. стало</td><td>b_i</td></tr><tr><td>0</td><td>111111</td><td></td><td>5</td><td>010101</td><td>1</td></tr><tr><td>1</td><td>011111</td><td>1</td><td>6</td><td>101010</td><td>1</td></tr><tr><td>2</td><td>101111</td><td>1</td><td>7</td><td>110101</td><td>0</td></tr><tr><td>3</td><td>010111</td><td>1</td><td>8</td><td>011010</td><td>1</td></tr><tr><td>4</td><td>101011</td><td>1</td><td>9</td><td>001101</td><td>0</td></tr></table>
• Второй регистр
 
<table><tr><td colspan="2">Состояние регистра</td><td>выход</td><td colspan="2">Состояние регистра</td><td>выход</td></tr><tr><td>итерация</td><td>Состояние рег. стало</td><td>c_i</td><td>итерация</td><td>состояние рег. стало</td><td>c_i</td></tr><tr><td>0</td><td>1111</td><td></td><td>5</td><td>1101</td><td>0</td></tr><tr><td>1</td><td>0111</td><td>1</td><td>6</td><td>0110</td><td>1</td></tr><tr><td>2</td><td>1011</td><td>1</td><td>7</td><td>0011</td><td>0</td></tr><tr><td>3</td><td>0101</td><td>1</td><td>8</td><td>1001</td><td>1</td></tr><tr><td>4</td><td>1010</td><td>1</td><td>9</td><td>0100</td><td>1</td></tr></table>
В результате получимпоследовательность 1111110</td></tr>
</table>

Критерии оценивания

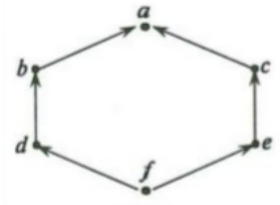
Номер задачи	Критерии	Шкала оценивания
1	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу,

		но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно»;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции

Типовой вариант контрольной работы

На контрольных работах студентам предлагается следующие типовые задания:
Контрольная работа 1

(проверка ОПК-4)	
Задания	Ответы:
1.Задает ли решетку граф 	Опр 1. Бинарное отношение «$\pounds$» на множестве X назовемотношением частичного порядка, когда для любых $a,b,c \in X$ выполняются три свойства: - рефлексивность $a \pounds a$; - транзитивность $(a \pounds b, b \pounds c) \Rightarrow (a \pounds c)$ - антисимметричность $(a \pounds b, b \pounds a) \Rightarrow (a = b)$ Опр2. Для $a,b \in X$ элемент $c = a \wedge b \in X$ называется наименьшей верхней границей, когда выполняются условия: - $a \pounds c, b \pounds c$ - для $d \in X$ истинно $(a \pounds d, b \pounds d) \Rightarrow (c \pounds d)$ Опр 3. Для $a,b \in X$ элемент $c = a \vee b \in X$ называется наибольшей нижней границей, когда выполняются условия: - $c \pounds a, c \pounds b$ - для $d \in X$ истинно $(d \pounds a, d \pounds b) \Rightarrow (d \pounds c)$ Опр 4. Пусть X - частично упорядоченное множество. $(X, \pounds)$ - называется решеткой, когда для любых $a,b \in X$ существуют $a \wedge b \in X$ и $a \vee b \in X$ Рассмотрим заданный граф. В соответствии с определением выполняются все свойства отношения

	частичного порядка на множестве $\{a,b,c,d,e,f\}$Для каждой пары вершин, соединенныхв графе путем, существует наименьшая верхняя и наибольшая нижняя граница. Другими словами: $d \text{Å} e = a, d \text{A} e = f; b \text{Å} e = a, b \text{A} e = f;$ $d \text{Å} c = a, d \text{Å} c = f; b \text{Å} c = a, b \text{Å} c = f.$ Следовательно, по Опр4 граф задает решетку.

2.Модель Харрисона-Руззо-Ульмана (ХРУ) Сформулируйте команду передачи субъекту sc права readк файлу f его владельцем субъектом s	*CommandGrantFile*($s, s\$, f$)
	IF (*own* $\in M[s, f]$) *then*
	«внести» право чтение *read*в $M[s\$, f]$;
	endIF
	End.

3. Есть три пользователя A, B и C используя протокол DIFFIE-HELLMAN сгенерируйте общий секретный ключ	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A, B и C выбирают в открытом доступе большое простое число nи g. Пусть $n = 13$и $g = 2$ 2. Пользователь A выбирает случайное большое натуральное число x и отправляет пользователю B величину $X = g^x \bmod n$; Пусть $x = 5$и $X = 6$ 3. Пользователь B выбирает случайное большое натуральное число y и отправляет пользователю C величину $Y = g^y \bmod n$; Пусть $y = 7$и $Y = 11$ 4. Пользователь C выбирает случайное большое натуральное число z и отправляет пользователю A величину $Z = g^z \bmod n$; Пусть $z = 3$и $Z = 8$ 5. Пользователь A отправляет пользователю B следующую величину $Zc = Z^x \bmod n$; Вычисляем $Zc = 8^5 \bmod 13 = 8$ 6. Пользователь B отправляет пользователю C следующую величину $Xc = X^y \bmod n$; Вычисляем $Xc = 6^7 \bmod 13 = 7$ 7. Пользователь C отправляет пользователю A следующую величину $Yc = Y^z \bmod$; Вычисляем $Yc = 11^3 \bmod 13 = 5$ 8. Пользователь A вычисляет величину $k = Y\$^x \bmod n$; Вычисляем $k = 5^5 \bmod 13 = 5$ 9. Пользователь B вычисляет величину $\tilde{k} = Zc^y \bmod n$. Вычисляем $\tilde{k} = 8^7 \bmod 13 = 5$ 10. Пользователь C вычисляет величину $\tilde{\tilde{k}} = Xc^z \bmod n$. Вычисляем $\tilde{\tilde{k}} = 7^3 \bmod 13 = 5$ Получили $k = k = \tilde{k} = 5$
4. Есть два пользователя Aи Bиспользуя протокол MTI сгенерируйте общий секретный ключ, если известно, что $n = 17$	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A и B выбирают в открытом доступе большое простое число nи g, где g образующий элемент мультипликативной группы Z_n^*. Пусть $n = 17$и $g = 3$ 2. Пользователи A и B должны сгенерировать секретные ключи a, $1 \le a \le$ и b, $1 \le b \le n - 2$, соответственно, и публикуют свои открытые ключи $z_A = g^a \bmod n$ и $z_B = g^b \bmod n$; Пусть Пользователь A генерирует число $a = 2$ и публикует $z_A = 3^2 \bmod 17 = 9$, соответственно пользователь B генерирует число $b = 3$ и публикует $z_B = 3^3 \bmod 17 = 10$; 3. Пользователь A выбирает случайное натуральное число x $1 \le x \le n - 2$ и

	отправляет пользователю B величину $X = g^x \bmod n$; Пусть пользователь A генерирует число $x = 4$ и отправляет пользователю B величину $X = 3^4 \bmod 17 = 13$; 4. Пользователь B выбирает случайное большое натуральное число y, $1 \le y \le n-2$ и отправляет пользователю A величину $Y = g^y \bmod n$; Пусть пользователь B генерирует число $y = 5$ и отправляет пользователю величину $Y = 3^5 \bmod 17 = 5$; 5. Пользователь A вычисляет величину $k = Y^a z_A^x \bmod n$; Пусть пользователь A на настоящий момент знает величины: $n, g, a, z_A, z_B, x, X, Y$. Пользователь A вычисляет величину $k = (Y^a z_B^X) \bmod n = (5^3 \cdot 10^4) \bmod 17 = (15 * 10000) \bmod 17 = 15$ 6. Пользователь B вычисляет величину $\tilde{k} = X^b z_A^y \bmod n$. Пусть пользователь B на настоящий момент знает величины: $n, g, b, z_A, z_B, y, X, Y$. Пользователь B вычисляет величину $\tilde{k} = (X^b z_A^y) \bmod n = (13^3 9^5) \bmod 17 = (2197 * 59049) \bmod 17 = 15$ Получили $\tilde{k} = k = 15$
5. Постройте схему разделения секрета на примере пороговой схемы Шамира (n,t), где $n = 5, t = 3$. В качестве конечного поля возьмем Z_{17}.	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема разделения секрета включает два протокола: В качестве конечного поля возьмем Z_{17}, а в качестве многочлена,на котором основана схема Шамира $(5,3)$. • Рассмотрим протокол формирования частичных секретов. Возьмем $f(x) = (2x^2 + 2x + 2) \bmod 17$. протокол формирования частичных секретов состоит в вычислении $f(x)$ $a_1 = f(1) = (2 + 2 + 2) \bmod 17 = 6$; $a_2 = f(2) = (8 + 4 + 2) \bmod 17 = 14$; $a_3 = f(3) = (18 + 6 + 2) \bmod 17 = 9$; $a_4 = f(4) = (32 + 8 + 2) \bmod 17 = 8$; $a_5 = f(5) = (50 + 10 + 2) \bmod 17 = 11$. • Рассмотрим протокол восстановления секрета группой пользователей из t человек, и найдем секретную информацию b_0 Чтобы восстановить $f(x)$ из трех частичных секретов. Будем считать, что нам дано $a_1 = 12, a_2 = 5, a_3 = 4$ тогда решается система линейных уравнений: $\begin{cases} f(1) = (b_2 + b_1 + b_0) \bmod 17 = 12 \\ f(2) = (4b_2 + 2b_1 + b_0) \bmod 17 = 5 \\ f(3) = (9b_2 + 3b_1 + b_0) \bmod 17 = 4 \end{cases}$ Решением будет $b_2 = 3, b_1 = 1, b_0 = 8$.
(проверка ОПК-3)	
Задания	Ответы:
1.Применяя расширенный алгоритм Евклида: а) найти d, x, y для которых выполняется $d = НОД(a,b) = ax + by$, где a=512; b=724 b) найти x для которого выполняется $8x \bmod 107$	а) $4 = НОД(512,724) = 512 * (-41) + 724 * 29$, следовательно $d = 4, x = -41, y = 29$ b) После применении расширенного алгоритма Евклида $d = НОД(a,b) = ax + by$, где $a = 107, b = 8$. Мы получим: $1 = НОД(107,8) = 107 * 3 + 8 * (-40)$, возьмем указанное выражение по модулю 107. В результате $(107 * 3 + 8 * (-40)) \bmod 107 \Rightarrow (8 * (-40)) \bmod 107 \Rightarrow q = -40 = 67$
2.Построить криптосистему RSA и	Числовые значения могут отличаться от тех, которые приведены в данном решении

закодируйте число 7	Криптосистема RSA строится следующим образом: • сначала выбираются два больших простых числа p и q • вычисляем $n = pq$ и $f(n) = (p-1)(q-1)$ • выбирается открытый ключ натуральное число e такой, что $1 \le e \le n-1$ и который является взаимно простым с $f(n) = (p-1)(q-1)$ • вычисляем секретный ключ d такой, что $1 \le d \le n-1$ и $ed \equiv 1 \bmod f(n)$ Для того чтобы зашифровать блок сообщения $M \quad (0 < M < n)$ надо выполнить следующие действия: $C = M^e \bmod n$ Для того чтобы расшифровать блок сообщения $C \quad (0 < C < n)$ надо выполнить следующие действия: $M = C^d \bmod n$ Построим криптосистемуRSA и закодируем число 7 Строим криптосистему • выбираем $p = 3$ и $q = 11$; • вычисляем $n = 33$ и $f(n) = 20$ • выбираем $e = 3$ • вычисляем $d = 7$ Для того чтобы зашифровать сообщение $M = 7$ надо выполнить следующие действия: $C = M^e \bmod n = 7^3 \bmod 33 = 13$
3. Вычислить $\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$	Напомним процесс вычисления.Пусть задано: множество натуральных чисел $(m_1, m_2, ..., m_k)$ не равных единице, которые являются попарно взаимно простыми множество натуральных чисел $(b_1, b_2, ... b_k)$. Система сравнений $\begin{cases} x \equiv b_1 \bmod m_1 \\ ... \\ x \equiv b_k \bmod m_k \end{cases}$ имеет решение $x = x_0 \bmod (m_1 m_2 ... m_k)$; где $x_0 = M_1 M_1' b_1 + ... + M_k M_k' b_k$; числа M_s и M_s' определяется изусловий $m_1 m_2 ... m_k = M_s m_s$, $M_s M_s' = 1 \bmod m_s$ Рассмотрим наше уравнение $M_1 = 35, M_2 = 28, M_3 = 20; M_1' = 3, M_2' = 2, M_3' = 6.$ $m_1 m_2 m_3 = 140;$ $x_0 = 35 * 3 * 1 + 28 * 2 * 3 + 20 * 6 * 2 = 513$ $x = 93$
4. Сформулировать алгоритм установки ЭЦП DSA. Дан текст с хэш значением равным 5. Выполните установку ЭЦП DSA. К полученным результатам примените протокол проверки подписи	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема DSA строится следующим образом: • сначала выбирается большое простое число p • выбирается простое число q которое является делителем $p-1$ • выбирается натуральноечисло t которое $0 < t < p$. Если число $t^{\frac{p-1}{q}} = 1 \bmod p$, то выбираем другое число t. В противном случае $g = t^{\frac{p-1}{q}} \bmod p$. • выбирается натуральноечисло x, которое является секретным ключом причем $1 < x < q$ • вычисляем $y = g^x \bmod p$ Установка подписи: • проверяем выполняется ли условие для хэш значение m текста M, что $0 < m < q$ • выбирается натуральноечисло k, $(0 < k < q)$. • вычисляем k^{-1} для которого выполняется условие $k * k^{-1} = 1 \bmod q$ • вычисляем два числа r и s по следующим правилам:

	$r = (g^k \bmod p) \bmod q$ и $s = k^{-1}(xr + m) \bmod q$ Если не выполняются условия $0 < r < q, 0 < s < q$ поменяйте входные параметры. Подписью является пара чисел (r, s) Проверка подписи Предположим, что к нам пришло сообщение M' с хэш значением m' и подписью (r', s') • если хотя бы одно из условий $0 < r' < q, 0 < s' < q$ не выполняется, то подпись считается недействительной • вычисляем $v = (s')^{-1} \bmod q$ • вычисляем: $z_1 = (m' v) \bmod q$ $z_2 = (r' v) \bmod q$ $u = (g^{z_1} y^{z_2}) \bmod p) \bmod q$ • проверяем условие $r' = u$. Если оно выполняется то подпись считается подлинной а сообщение –неизмененным. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA. Строим схему DSA • выбираем $p = 23, q = 11, t = 3$ • вычисляем $g = 3^2 \bmod 23 = 9$ • выбираем $x = 2$ • вычисляем $y = 9^2 \bmod 23 = 12$ Установка подписи: • выбираем $k = 4$ • вычисляем: $k^{-1} = 3$, $r = (9^4 \bmod 23) \bmod 11 = 6$, $s = (3 * (2 * 6 + 5)) \bmod 11 = 7$ Подписью является пара чисел $(6, 7)$ Проверка подписи Дано $m' = 5;\ r' = 6\ \ s' = 7.$ • условие $0 < 6 < 11,\ \ 0 < 7 < 11$ выполняется • вычисляем: $v = (s')^{-1} \bmod q = 7^{-1} \bmod 11 = 8$ $z_1 = (m' v) \bmod q = (5 * 8) \bmod 11 = 7$ $z_2 = (r' v) \bmod q = (6 * 8) \bmod 11 = 4$ $u = (g^{z_1} y^{z_2}) \bmod p) \bmod q = ((9^7 * 12^4) \bmod 23) \bmod 11 = 6$ Условие $r' = u$ выполнено, подпись подлинная.
5. Построить рюкзачную криптосистему и закодировать элементы множества, которые состоят из двоичных векторов (000,010,011,111)	Числовые значения могут отличаться от тех, которые приведены в данном решении Напомним описание рюкзачной криптосистемы. Создание криптосистемы: • выбираем сверхрастущий вектор $A = (a_1, \ldots, a_n)$ - это секретная информация • выбираем m и t такие что $m > \sum_{i=1}^{n} a_i$ и $НОД(m, t) = 1$ - это секретная информация • вычисляем t^{-1} такое что $t * t^{-1} = 1 \bmod m$ - это секретная информация • строим вектор $B = (b_1, \ldots, b_n)$, где $b_i = t a_i \bmod m$. Вектор B - это открытая

	информация и используется, как ключ зашифрования. Шифрование Дано: вектор $B=(b_1,\dots,b_n)$ двоичныйвектор $X=(x_1,\dots,x_n)$ • шифр вычисляем $C=B*X$ Дешифрование Дано: вектор $A=(a_1,\dots,a_n)$ числа $C,t^{-1},m.$ • вычисляем $a=(C*t^{-1})\bmod m$ • решаем задачу о рюкзаке (A,a) Рассмотрим предложенное задание Создание криптосистемы: • выберем - это секретный ключ • вычислим $A=(1,3,5)\ m=11, t=5, t^{-1}=9$ Шифрование $B=(5,4,3)$ Дано: вектор двоичныевектора $x_1=(0,0,0)\ x_2=(0,1,0)$ $B=(5,4,3)$ получилишифр $(1,1,1)$ $c_1=0; c_2=4; c_3=7; c_4=12$

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
ОПК-4		
1	Владеть навыками: построение модели информационной безопасности	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	Владеть навыками: построение модели информационной безопасности	0 баллов – студент полностью не верно решил задачу 2 балла – студент полностью разобрался в решении задачи
3	Уметь: выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но была допущена вычислительная ошибка. 2 балла – студент полностью разобрался в решении задачи
4	Уметь: выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но была допущена вычислительная ошибка. 2 балла – студент полностью разобрался в решении задачи
5	Уметь: выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно рассмотрелодин протокол формирование или восстановление секрета. 2 балла – студент полностью разобрался в решении задачи
(проверка ОПК-3)		
1	*Уметь:* реализовывать некоторые криптографические	0 баллов – студент полностью

	алгоритмы. *Владеть навыками:*создавать ЭЦП.	неверно решил задачу 1 балл – студент верно решил одну подзадачу. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:*создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:*создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:*создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
5	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:*создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

Максимальное количество баллов по ОПК-4 -10 баллов

Максимальное количество баллов по ОПК-3 -10 баллов

Набранное количество баллов соответствует оценки за контрольную работу:

Рассмотрим формирование компетенций ОПК-4 и ОПК-3:

-менее 4 баллов компетенция не сформирована;

-от 4 до 6 баллов — пороговый уровень формирования компетенции;

- от 7 до 8 баллов —продвинутый уровень формирования компетенции;

- от 9 до 10 баллов —высокий уровень формирования компетенции.

Рассмотрим формирование оценки:

-менее 4 баллов по ОПК-4 или менее 4 баллов по ОПК-3 – оценка «неудовлетворительно»;

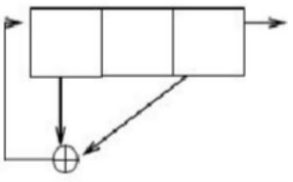
-от 4 до 6 баллов одна компетенция и от 4 до 8 баллов другая компетенция - оценка «удовлетворительно»;

-от 4 до 6 баллов одна компетенция и от 9 до 10 баллов другая компетенция или от 7 до 8 баллов одна компетенция и от 7 до 10 баллов другая компетенция - оценка «хорошо»;

-от 9 до 10 баллов одна компетенция и от 9 до 10 баллов другая компетенция - оценка «отлично».

Контрольная работа 2

(проверка ОПК-4)	
Задания	Ответы:
1.Постройте аффинную криптосистему, для русского алфавита. Закодируйте слово «золото»	Числовые значения могут отличаться от тех, которые приведены в данном решении Напомним, что аффинная криптосистема определяется тремя натуральными числами $a, b, m.$ Шифрование происходит заменой символа с

	порядковым номером на символ порядковыйномер которого вычисляется по формуле $f(x)=(ax+b)\bmod m$. Заметим, что на пару чисел a и m наложено условие взаимной простоты. Закодируйте слово «золото». Будем рассматривать $f(x)=(7x+5)\bmod 33$. Нам надо закодировать $(8,15,12,15,19,15)$. В результате получим $(28,11,23,11,6,11)$ или фраза «брьрлр»
2. Взломайте аффинную криптосистему $f(x)=(ax+b)\bmod m$, для русского алфавита. Известно, что в исходном тексте чаще всего встречаются символы с порядковыми номерами 10 и 14, а в шифрованном тексте с порядковыми номерами 8 и 17.	Нам надо решить систему $\begin{cases}10a+b=8 \bmod 33\\14a+b=17 \bmod 33\end{cases}$ или $\begin{cases}10a+b=17 \bmod 33\\14a+b=8 \bmod 33\end{cases}$ Ответ $a=27\ \ b=2$ или $a=6\ \ b=23$
3. Выполните операцию умножения байтов в поле $GF(2^8)$, которая используется в алгоритме AES. x^4+x+1 и x^4+x^2+1	Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$. Поскольку байты оперируют в поле $GF(2^8)$, то заданы операции сложения и умножения: • сложение - суть операция поразрядного XOR. • умножение- это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена $j(x)$ и использованием операции XOR при приведении подобных членов. В качестве неприводимого многочлена $j(x)=x^8+x^7+x^3+x+1$. Решение $(x^4+x+1)*(x^4+x^2+1)) \mod(x^8+x^4+x^3+x+1)=x^6+x^5+x^4+x^2.$
4. Закодируйте с помощью криптосистемы Хилла, для английского алфавита. Зашифровать слово «HELP»	Напомним криптосистему Хилла: Все арифметические операции выполняются по модулю $n=26$. Выбирается целое число d 3 2. Оно указывает размерность используемых матриц. Пусть теперь M - квадратная $d\ d$ матрица. Элементами матрицы M являются целые числа от 0 до 25. Отметим, что матрица M должна быть невырожденной.матрица M является секретным ключом. Шифрование происходит блоками по d символов, оно выполняется с помощью формулы $MP=C \bmod n$, где P - блок исходного текста, а C - блок шифра. Решение • Пустьбудет $M=\begin{pmatrix}3&3\\2&5\end{pmatrix}$ • $P_1=\begin{pmatrix}H\\E\end{pmatrix}=\begin{pmatrix}7\\4\end{pmatrix}$ и $P_2=\begin{pmatrix}L\\P\end{pmatrix}=\begin{pmatrix}11\\15\end{pmatrix}$ • Процессшифрования $MP_1=\begin{pmatrix}7\\8\end{pmatrix}=\begin{pmatrix}H\\I\end{pmatrix}=C_1$ и $MP_2=\begin{pmatrix}0\\19\end{pmatrix}=\begin{pmatrix}A\\T\end{pmatrix}=C_2$ В результате получим слово «HIAT»
(проверка ОПК-3)	
Задания	Ответы:
1.Постройте регистр сдвига с линейной обратной связью с ассоциированным многочленом x^2+x+1 и выпишем состояние регистра, если он был инициализирован вектором (111).	LFSR  Состояние регистра **итерация** / **состояние рег. стало** / Выход 0 — 111 1 — 011 — 1 2 — 101 — 1 3 — 010 — 1 4 — 001 — 0 5 — 100 — 1 вектор инициализации регистр сдвига $(1,1,1)$

		6	110	0
		7	111	0

2.Постройте 10 битную псевдослучайную последовательность с помощью RSA-генератора.

Числовые значения могут отличаться от тех, которые приведены в данном решении

Напомним, что RSA-генератор строится следующим образом:

- выбираем p и q - два больших простых числа примерно одинакового размера $p \neq q$;
- вычисляем число $n = pq$ и число $\varphi(n) = (p-1)(q-1)$;
- выбираем случайное натуральное число e, которое являются взаимно простыми с $\varphi(n)$;
- выбираем в качестве стартового числа генератора случайное натуральное число $x_0 \quad (1 < x_0 < n)$;
- искомой последовательностью бит длиной m будет являться последовательность

$RSA_{e,n,m}(x_0) = b_0 b_1 b_2 \ldots b_i \ldots b_{m-1}, \quad i = 0, \ldots, m-1,$ где b_i - младший бит числа x_i, $x_{i+1} = x_i^e \bmod n.$

Построим 10 битную псевдослучайную последовательность

- Пусть $p = 3,$ а $q = 11.$
- Вычислим $n = pq = 33$ и $\varphi(n) = (p-1)(q-1) = 20.$
- В качестве e возьмем число 3.
- В качестве стартового числа генератора $x_0 = 14.$
- В качестве элементов псевдослучайной последовательности будем брать младший бит в двоичной записи чисел $x_{i+1} = x_i^e \bmod n.$

В результате получили последовательность $RSA_{3,33,10}(14) = 0100010001$.

3. Создайте комбинирующий генератор, состоящий из двух регистров сдвига с линейной обратной связью.

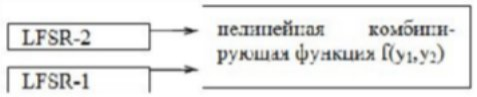
Первый регистр с ассоциированным многочленом $x^6 + x + 1,$ он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра $y_1.$

Второй регистр с ассоциированным многочленом $x^5 + x + 1$ он был инициализирован вектором $(1,1,1)$. Выход регистра $y_2.$

В качестве комбинирующей функции возьмем $f(y_1, y_2) = y_1 y_2$

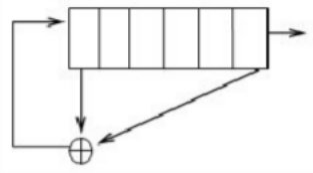
Постройте 7 битную псевдослучайную последовательность

Напомним, что комбинирующий генератор проиллюстрировать следующей схемой



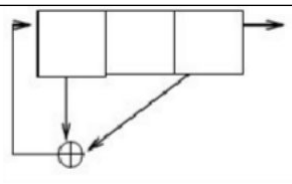
Решение

- Первыйрегистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	$y_1.$	итерация	состояние рег. стало	$y_1.$
0	111111		4	101011	1
1	011111	1	5	010101	1
2	101111	1	6	101010	1
3	010111	1	7	110101	0

- Второй регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_2.	итерация	состояние рег. стало	y_2.
0	111		4	001	0
1	011	1	5	100	1
2	101	1	6	110	0
3	010	1	7	111	0

В результате получимпоследовательность 1110100

4. Создайте сжимающий генератор, состоящий из двух регистров сдвига с линейной обратной связью.
Первый регистр с ассоциированным многочленом $x^6 + x + 1$, он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра b_i.
Второй регистр с ассоциированным многочленом $x^5 + x + 1$ он был инициализирован вектором $(1,1,1)$. Выход регистра c_i.
Постройте 6 битную псевдослучайную последовательность

Напомним, что сжимающий генератор описывается следующей образом:
Используется 2 регистра с линейной обратной связью. Тактовые импульсы поступают на оба LFSR. Предположим, что

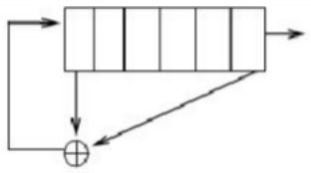
$b = b_0 b_1 b_2 K$ последовательность с выхода LFSR1.

$c = c_0 c_1 c_2 K$ - последовательность с выхода LFSR2,

Тогда результирующая последовательность $z = z_0 z_1 z_2 K$ включает в себя те биты b_i, для которых соответствующие биты $c_i = 1$. Остальные биты последовательности b игнорируются.

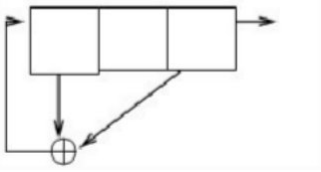
Решение

• Первыйрегистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	b_i	итерация	состояние рег. стало	b_i
0	111111		5	010101	1
1	011111	1	6	101010	1
2	101111	1	7	110101	0
3	010111	1	8	011010	1
4	101011	1	9	001101	0

• Второй регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало		итерация	состояние рег. стало	
0	111		5	100	1
1	011	1	6	110	0
2	101	1	7	111	0
3	010	1	8	011	1
4	001	0	9	101	1

В результате получимпоследовательность 111110

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
ОПК-4		
1	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил одну вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи
3	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
ОПК-3		
1	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью

		разобрался в решении задачи

Максимальное количество баллов по ОПК-4 -8 баллов
Максимальное количество баллов по ОПК-3 -8 баллов
Набранное количество баллов соответствует оценки за контрольную работу:
Рассмотрим формирование компетенций ОПК-4 и ОПК-3:

-менее 4 баллов компетенция не сформирована;
-от 4 до 5 баллов — пороговый уровень формирования компетенции;
- от 6 до 7 баллов — продвинутый уровень формирования компетенции;
- 8 баллов — высокий уровень формирования компетенции.

Рассмотрим формирование оценки:

-менее 4 баллов по ОПК-4 или менее 4 баллов по ОПК-3 – оценка «неудовлетворительно»;
-от 4 до 5 баллов одна компетенция и от 4 до 7 баллов другая компетенция - оценка «удовлетворительно»;
-от 4 до 5 баллов одна компетенция и 8 баллов другая компетенция или от 6 до 7 баллов одна компетенция и от 6 до 8 баллов другая компетенция - оценка «хорошо»;
-8 баллов одна компетенция и 8 баллов другая компетенция - оценка «отлично».

Тест для самопроверки по результатам освоения дисциплины.

(проверка ОПК-3)

Вопрос 1Вычислите $НОД(315,123)$

Выберите ответ
1) 3.
2) 6
3) 12

Вопрос 2Найдите xдля которого выполняется $\begin{cases} x = 1 \bmod 5 \\ x = 2 \bmod 7 \end{cases}$

Выберите ответ
1) 3.
2) 16
3) 12

Вопрос 3Алгоритмы шифрования с открытым ключом – это система

Выберите ответ
1) в которых ключ расшифрования трудно найти даже при известном ключе шифрования
2) в которых ключ расшифрования легко находится по ключу шифрования
3) в которых ключ расшифрования совпадает с ключом шифрования

Вопрос 4Закодируйте вектор $X = (0,1,1)$с помощью рюкзачной криптосистемы, которая является криптосистемой с открытым ключом.

Дано секретный ключ рюкзачной криптосистемы:

- вектор $A = (1,3,5)$, которыйявляетсязакрытым;
- число $m = 11$, котороеявляетсямодулем;
- число $t = 5$,котороеявляетсямножителем.

Выберите ответ
1) 7.
2) 16
3) 12

Вопрос 5Зашифруйтечисло 5 криптосистемой RSA,если задано

- простые числа $p = 3$ и $q = 7$;
- ключ шифрования (открытый ключ) $e = 5$.

Выберите ответ
1) 17
2) 2
3) 25

Вопрос 6В какой криптосистеме алгоритм шифрования блока X задается формулой $C = X^e \bmod n$, где

- n - это число, которое получается из формулы $n = p*q$ здесь p и q простые числа;
- e - это открытый ключ шифрования, который удовлетворяет условию $НОД(e, j(n)) = 1$, где $j(n) = (p - 1)*(q - 1)$.

1) Криптосистема RSA
2) Криптосистема RC6
3) криптосистема AES

Вопрос 7Постройте 6 битную псевдослучайную последовательность RSA. Дано:

- Пусть $p = 3$, а $q = 7$.
- В качестве e возьмем число 5.
- В качестве стартового числа генератора $x_0 = 5$.
- В качестве элементов псевдослучайной последовательности будем брать младший бит в двоичной записи чисел x_{i+1}

1) В результатеполучилипоследовательность $RSA_{21}(5) = 111111$.
2) В результатеполучилипоследовательность $RSA_{21}(5) = 111110$.
3) В результатеполучилипоследовательность $RSA_{21}(5) = 100101$.

Вопрос 7КриптосистемаRSA - это.

1) Криптосистема открытого ключа (ассиметричная криптосистема)
2) Симметричная криптосистема
3) Криптосистема вида квадрат

Правильныеответы

Вопрос №	Вариант ответа		**Вопрос №**	Вариант ответа
1	1		**5**	1
2	2		**6**	1
3	1		**7**	1
4	1		**8**	1

Каждый правильный ответ оценивается в 1 балл.

Набранное количество баллов 8 соответствует формированию проверяемой компетенции на высоком уровне, 6-7 баллов – на продвинутом уровне, 4-5 баллов – на пороговом уровне, менее 4 баллов – ниже порогового уровня.

Список заданий к зачету

На зачете проверяется сформированность знаний, умений и навыков в соответствии с компетенциямиОПК-4 (вопросы 1–8) и ОПК-3 (вопросы 9–16).

Зачет проводится в устной форме и выставляется по итогам ответов, данных студентом на два вопроса из списка. Список вопросов к зачету заранее доступен для студентов.

1. Определение информации, данных, знаний. Определение безопасности. Несанкционированный доступ.
2. Информационные системы. Доступность, целостность, конфиденциальность. Основные понятия об угрозах.
3. Каналы утечки информации, их классификация.
4. Каналы утечки информации технических средств обработки, хранения и передачи информации.Каналы утечки речевой информации. Каналы утечки информации при её передаче по каналам связи.

5. Технические каналы утечки видовой информации. Каналы утечки информации, создаваемые атаками извне и внутри корпоративных систем ИКТ

6. Модели разграничения доступа по принципу предоставления прав. Модели дискретного доступа. Вероятностные модели.

7. Информационные модели. Модель мандатного доступа. Модель Бела-Лападулы, игровая модель. Матрица доступов.

8. Аутентикация, авторизация, пароли, токены, "рукопожатие". Протоколы аутентификации без передачи секретной информации, одноразовые ключи.

9. Доказательство с нулевым знанием.

10. Асимметричные шифры, шифры с открытым ключом.

11. Электронные цифровые подписи. Трудоемкость дешифрования. Рюкзачная криптосистема.

12. Алгоритм RSA.

13. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Алгоритм Эль-Гамаля. Алгоритм Рабина.

14. Введение в защиту ПО. Угрозы безопасности ПО. Примеры уязвимостей ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО.

15. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО. Компьютерные вирусы и антивирусные программы.

16. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800

Описание процедуры выставления оценивания сформированности компетенций(для ответа на теоретический вопрос)

Результат определяется оценками «отлично» (высокий уровень), «хорошо» (продвинутый уровень), «удовлетворительно» (пороговый уровень), «неудовлетворительно» (компетенция не сформирована).

Для оценивания ответов (по каждой компетенции):

Оценка «отлично»:

- студент ответил на вопрос правильно и полно.

Оценка «хорошо»:

- студент ответил на вопрос правильно, но недостаточно полно (не менее 70% от полного).

Оценка «удовлетворительно»:

- студент ответил на вопрос с 1 ошибкой или 1-2 недочетами и неполно (не менее 70% от полного ответа).

Оценка «неудовлетворительно»:

- студент ответил на вопрос неправильно (больше 1 ошибки или 2 недочетов) или неполно (менее 70% от полного).

Критерии оценивания

Оценка **«зачтено»** выставляется студенту, который:

- прочно усвоил предусмотренный программный материал;
- правильно, аргументировано ответил на все вопросы, с приведением примеров;
- показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов.

Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельных и контрольной работы, систематическая активная работа на практических занятиях.

Оценка **«не зачтено»** Выставляется студенту, который не справился с 50% вопросов и заданий, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем. Целостного представления о взаимосвязях, компонентах дисциплины у студента нет.

Список заданий к экзамену

На экзамене проверяется сформированность знаний, умений и навыков в соответствии с компетенциямиОПК-4 (вопросы 1–9) и ОПК-3 (вопросы 10–21).

Экзамен проводится в устной форме и выставляется по итогам ответов, данных студентом на два теоретических и один практический вопрос. Список теоретических вопросов к экзамену заранее доступен для студентов. В билете присутствует один практический вопрос, аналогичный рассмотренным в курсе.

Список вопросов к экзамену:

1. Определение информации, данных, знаний. Определение безопасности. Несанкционированный доступ.
2. Информационные системы. Доступность, целостность, конфиденциальность. Основные понятия об угрозах
3. Модели разграничения доступа по принципу предоставления прав. Модели дискретного доступа. Вероятностные модели.
4. Информационные модели. Модель мандатного доступа. Модель Бела-Лападулы, игровая модель. Матрица доступов.
5. Критерий адекватности защиты. Оранжева книга. Документы Гостехкомиссии РФ. Информационная безопасность распределенных систем. Рекомендации X.800 .
6. Юридические вопросы информационной безопасности
7. Угрозы безопасности ПО. Примеры уязвимостей ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО.
8. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО. Компьютерные вирусы и антивирусные программы
9. Шифрование. Трудоемкость дешифрования. Симметричные шифры. Схема Фейстеля, SP-сеть. Режимы шифрования. Некоторые исторические алгоритмы (алгоритмы Цезаря, Вижнера).
10. Алгоритмы AES, Гост 28147-89, DES,
11. Serpent, Mars,IDEA
12. Каналы утечки информации технических средств обработки, хранения и передачи информации. Каналы утечки речевой информации.
13. Каналы утечки информации при её передаче по каналам связи. Технические каналы утечки видовой информации. Каналы утечки информации, создаваемые атаками извне и внутри корпоративных систем ИКТ
14. Асимметричные шифры, шифры с открытым ключом.Идея открытых ключей и преимущества их. Алгоритм Рабина. Алгоритм RSA. Алгоритм Эль-Гамаля
15. Электронные цифровые подписи. ЭЦП RSA, ЭЦП DSA, ЭЦП Гост
16. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Решить $y = a^x \bmod p$
17. Генераторы случайных и псевдослучайных чисел, их использование при аутентификации. Криптографические ГПСЧ, их свойства.
18. Генератор LFSR, и его модификации. Взлом LFSR.
19. Виды поточных шифров. Алгоритмы A5, RC4, Flash, Wake
20. Аутентикация, авторизация, пароли.
21. Хэш-функции MD5, SHA1.

Описание процедуры выставления оценивания сформированности компетенций (для ответа на теоретический вопрос)

Результат определяется оценками «отлично» (высокий уровень), «хорошо» (продвинутый уровень), «удовлетворительно» (пороговый уровень), «неудовлетворительно» (компетенция не сформирована).

Для оценивания ответов (по каждой компетенции):

Оценка «отлично»:

- студент ответил на вопрос правильно и полно.

Оценка «хорошо»:

- студент ответил на вопрос правильно, но недостаточно полно (не менее 70% от полного).

Оценка «удовлетворительно»:

- студент ответил на вопрос с 1 ошибкой или 1-2 недочетами и неполно (не менее 70% от полного ответа).

Оценка «неудовлетворительно»:

- студент ответил на вопрос неправильно (больше 1 ошибки или 2 недочетов) или неполно (менее 70% от полного).

Критерии оценивания экзамена:

«2» - плохо:

Теоретический вопрос: студент не раскрыл теоретический вопрос, на заданные экзаменаторами вопросы не смог дать удовлетворительный ответ.

Практический вопрос: студент не понял смысла текста (задачи), не смог выполнить задания. На заданные экзаменатором вопросы ответил неудовлетворительно, не продемонстрировал сформированность требующихся для выполнения заданий знаний и умений. Или студент понял отдельные детали текста, но не его основной смысл, задания выполнил неправильно, на заданные экзаменатором вопросы ответил неудовлетворительно, не продемонстрировал сформированность требующихся для выполнения заданий умений.

«3» - удовлетворительно:

Теоретический вопрос: студент смог с помощью дополнительных вопросов воспроизвести основные положения темы, но не сумел привести соответствующие примеры или аргументы, подтверждающие те или иные положения.

Практический вопрос: студент понял смысл текста (задачи), но смог выполнить задание лишь после дополнительных вопросов, предложенных экзаменатором. При этом на поставленные экзаменатором вопросы не вполне ответил правильно и полно, но подтвердил ответами понимание вопросов и продемонстрировал отдельные требующиеся для выполнения заданий знания и умения.

«4» - хорошо:

Теоретический вопрос: студент (не допуская ошибок) правильно изложил теоретический вопрос, но недостаточно полно или допустил незначительные неточности, не искажающие суть понятий, теоретических положений, правовых и моральных норм. Примеры, приведенные учеником, воспроизводили материал учебников. На заданные экзаменатором уточняющие вопросы ответил правильно.

Практический вопрос: студент понял смысл текста (задачи), предложенные задания выполнил правильно, но недостаточно полно. На заданные экзаменатором вопросы ответил правильно. Проявил необходимый уровень всех требующихся для выполнения заданий знаний и умений.

«5» - отлично:

Теоретический вопрос: студент полно и правильно изложил теоретический вопрос, привел собственные примеры, правильно раскрывающие те или иные положения, сделал обоснованный вывод;

Практический вопрос: студент понял смысл текста (задачи), полно и правильно выполнил предложенные задания, проявил высокий уровень всех требующихся для выполнения заданий знаний и умений.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенцийна различных этапах их формирования, описание шкалы оценивания

2.1. Шкала оцениваниясформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующейтрехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков,полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

3. Методические рекомендации преподавателюпо процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1Критерии оценивания степени овладения знаниями, умениями,навыкамии (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знаниебазовыхтеорий,концепцийинаправлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) врамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироватьсявбазовых теориях,концепцияхинаправлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные,глубокиеиполныезнанияповсемразделам дисциплины;
- точное использование терминологии данной области знаний,стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решениинаучных и профессиональных задач;

- способность самостоятельно и творчески решать сложные задачи (проблемы) врамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельнаяработанапрактических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачтено», «незачтено») определяетсярабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформировананиже, чем на пороговом уровне.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформировананиже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины «Информационная безопасность»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине **«Информационная безопасность»** являются лекции и практические занятия. Для успешного освоения дисциплины очень важно рассмотрение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий.

Задачи разбираются на лекциях и лабораторных занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, лабораторных занятиях или из учебной литературы. Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задания, аналогичные разобранным на лекциях и лабораторных занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач. Для проверки и контроля усвоения теоретического материала, периодически проводятся контрольные работы.

Освоить вопросы, излагаемые в процессе изучения дисциплины «Математические методы защиты информации» самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала и большим объемом курса. Поэтому посещение всех аудиторных занятий является совершенно необходимым. Без упорных и регулярных занятий в течение семестра сдать экзамен по итогам изучения дисциплины студенту практически невозможно.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы особенно рекомендуется использовать учебную литературу.

Также для подбора учебной литературы рекомендуется использовать широкий спектр интернет-ресурсов:

1. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru) - электронная библиотека, обеспечивающая доступ к наиболее востребованным материалам-первоисточникам, учебной, научной и художественной литературе ведущих издательств (*регистрация в электронной библиотеке – только в сети университета. После регистрации работа с системой возможна с любой точки доступа в Internet.).

2.Информационная система "Единое окно доступа к образовательным ресурсам" (http://window.edu.ru/library).

Целью создания информационной системы "Единое окно доступа к образовательным ресурсам" (ИС "Единое окно ") является обеспечение свободного доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования.

Информационная система "Единое окно доступа к образовательным ресурсам" создана по заказу Федерального агентства по образованию в 2005-2008 гг. Головной разработчик проекта - Федеральное государственное автономное учреждение Государственный научно-исследовательский институт информационных технологий и телекоммуникаций (ФГАУ ГНИИ ИТТ "Информика") www.informika.ru.

ИС "Единое окно" объединяет в единое информационное пространство электронные ресурсы свободного доступа для всех уровней образования в России. Разделы этой системы:

- Электронная библиотека– является крупнейшим в российском сегменте Интернета хранилищем полнотекстовых версий учебных, учебно-методических и научных материалов с открытым доступом. Библиотека содержит более 30 000 материалов, источниками которых являются более трехсот российских вузов и других образовательных и научных учреждений. Основу наполнения библиотеки составляют электронные версии учебно-методических материалов, подготовленные в вузах, прошедшие рецензирование и рекомендованные к использованию советами факультетов, учебно-методическими комиссиями и другими вузовскими структурами, осуществляющими контроль учебно-методической деятельности.

-Интегральный каталог образовательных интернет-ресурсов содержит представленные в стандартизованной форме метаданные внешних ресурсов, а также содержит описания полнотекстовых публикаций электронной библиотеки. Общий объем каталога превышает 56 000 метаописаний (из них около 25 000 - внешние ресурсы). Расширенный поиск в "Каталоге" осуществляется по названию, автору, аннотации, ключевым словам с возможной фильтрацией по тематике, предмету, типу материала, уровню образования и аудитории.

- Избранное. В разделе представлены подборки наиболее содержательных и полезных, по мнению редакции, интернет-ресурсов для общего и профессионального образования.

-Библиотеки вузов. Разделсодержит подборки сайтов вузовских библиотек, электронных каталогов библиотек вузов и полнотекстовых электронных библиотек вузов.

Для самостоятельного подбора литературыв библиотеке ЯрГУ рекомендуется использовать:

1. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php)дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб.и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.

2. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

3. Электронная картотека «Книгообеспеченность» (http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.