Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота А. А.

Кафедра технологий обработки и защиты информации

23.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.45 Методы и средства криптографической защиты информации

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Анализ безопасности компьютерных систем

3. Квалификация (степень) выпускника:

Специалист

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Дрюченко Михаил Анатольевич, к.т.н., доцент

7. Рекомендована:

протокол №5 от 05.03.2024

8. Учебный год:

2027-2028

9. Цели и задачи учебной дисциплины:

изучение математических основ криптографической защиты информации, вопросов обеспечения конфиденциальности, целостности, аутентичности данных, использование криптографических средств для решения задач идентификации и аутентификации, изучение криптографических протоколов, рассмотрение вопросов моделирования случайных величин с заданным законом распределения, изучение принципов криптоанализа, получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи дисциплины:

- обучение студентов математическим основам криптографии, базовым принципам работы симметричных и асимметричных криптографических систем при использовании специализированных протоколов и программных средств шифрования данных;

- обучение студентов базовым принципам создания электронных подписей при решении задач аутентификации;

- овладение практическими навыками применения теоретических знаний для контроля целостности, шифрования конфиденциальной информации, решения задач идентифи-

кации и аутентификации.

10. Место учебной дисциплины в структуре ООП:

базовый блок дисциплины в обще-профессиональной части. Для успешного освоения дисциплины необходимы входные знания в области информатики, теории информации, математической статистики, цифровой обработки сигналов, навыки программирования.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1	Знает основные задачи, решаемые криптографическими методами	Знает основные задачи, решаемые криптографическими методами.
		ОПК-10.2	Знает математические модели шифров, подходы к оценке их стойкости	Знает математические модели шифров и криптографических систем, подходы к оценке их стойкости. Владеет практическими навыками разработки, тестирования и оценки стойкости криптографических алгоритмов.
		ОПК-10.3	Знает зарубежные и российские криптографические стандарты	Знает зарубежные и национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения. Владеет практическими навыками применения зарубежных и национальных стандартов Российской Федерации в области криптографической защиты информации при разработке ПО в области информационной безопасности.
		ОПК-10.4	Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами	Знает принципы работы симметричных и асимметричных криптографических систем, принципы генерации, хранения и использования криптографических ключей, принципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, современные стандарты шифрования, хеширования, электронной подписи. Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами, умеет устанавливать, настраивать и использовать на практике специализированные криптографические программные средства.
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информа-	ОПК-10.5	Умеет применять математические методы при исследовании криптографических алгоритмов	Знает математические основы симметричных и асимметричных криптографических систем. Умеет применять математические методы при исследовании криптографических алгоритмов, в том числе для

	ции, использовать средства криптографической защиты информации при решении задач профессиональной деятельности			оценки стойкости СКЗИ. Владеет практическими навыками тестирования и оценки стойкости программ, использующих СКЗИ.
		ОПК-10.6	Владеет навыками использования типовых криптографических алгоритмов	Владеет практическими навыками применения современных криптографических алгоритмов и протоколов, практическими навыками работы с известными криптографическими библиотеками.

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 7	Всего
Аудиторные занятия	68	68
Лекционные занятия	34	34
Практические занятия	0	0
Лабораторные занятия	34	34
Самостоятельная работа	40	40
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль	0	0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн- курса, ЭУМК
1. Лекции			
1.1	Введение. Теоретические аспекты криптографии	Исторические сведения и этапы развития криптографии. Предметная область криптографии. Математические основы криптографии. Моделирование случайных величин с заданным законом распределения. Датчики случайных чисел.	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
1.2	Криптографические методы и стандарты	Симметричные и асимметричные криптосистемы. Использование криптографических средств для решения задач идентификации и аутентификации. Электронная цифровая подпись (ЭЦП). Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных. Гаммирование. Криптография с использованием эллиптических кривых. Шифрование, обмен ключами, ЭЦП на основе эллиптических кривых. Квантовая криптография.	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
1.3	Криптоанализ	Виды криптоанализа. Базовые принципы работы криптоаналитических алгоритмов.	Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабора-

			торных работ.
2. Лабораторные работы			
2.1	Теоретические аспекты криптографии	1. Практическое изучение принципов работы датчиков псевдо-случайных числовых последовательностей. Реализация датчиков ПСЧП.	Размещены индивидуальные задания для выполнения лабораторных работ.
2.2	Криптографические методы и стандарты	2. Практическое изучение особенностей работы одного из методов построения блочных шифров – сети Фейстеля. Реализация сети Фейстеля заданной архитектуры. 3. Изучение различных режимов работы блочных алгоритмов симметричного шифрования. Модификация ранее реализованной сети Фейстеля для работы в режимах ECB, CBC, OFB. 4. Практическое изучение алгоритмов хеширования на основе блочных алгоритмов шифрования. Модификация ранее реализованного блочного алгоритма шифрования для создания алгоритма хеширования. 5. Практическое изучение алгоритмов асимметричного шифрования. Реализация алгоритма RSA. Практическое изучение возможностей и особенностей работы с известными криптографическими библиотеками (cryptopp). Настройка и компиляция модулей библиотеки, подключение к тестовому проекту и использование необходимых функций (выработки ключей на основе текстовых строк PBKDF2, хеширования SHA-1, симметричного шифрования AES и т.д.).	Размещены индивидуальные задания для выполнения лабораторных работ.
2.3	Криптоанализ	7. Практическое изучение принципов частотного криптоанализа. Реализация алгоритма для дешифровки закрытых текстов на русском и английском языках, созданных с использованием простейших шифров моноалфавитной подстановки.	Размещены индивидуальные задания для выполнения лабораторных работ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Теоретические аспекты криптографии	12		8	10	30
2	Криптографические методы и стандарты	14		20	20	54
3	Криптоанализ	8		6	10	24
		34	0	34	40	108

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие

- средства: рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при кон-

спектировании лекционного материала.

3) При проведении практических работ обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Рябко, Борис Яковлевич. Криптография и стеганография в информационных технологиях / Б.Я. Рябко, А.Н. Фионов, Ю.И. Шокин ; Рос. акад. наук, Сиб. отд-ние, Ин-т вычисл. технологий СО РАН .— Новосибирск : Наука, 2015 .— 239 с. : ил. — Библиогр.: с.232-236 .— ISBN 978-5-02-019206-5.
2	Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов .— 2-е изд. — Москва : Горячая линия - Телеком, 2013 .— 232 с. : ил., табл. — Библиогр.: с.225-229.
3	Корниенко, А.А. Криптографические методы защиты информации : учебное пособие / А.А. Корниенко, М.Л. Глухарев. – Санкт-Петербург : ПГУПС, [б. г.]. – Часть 1 – 2017. – 64 с. – ISBN 978-5-7641-1053-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111765 (дата обращения: 07.07.2023). – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
1	Круглов И.А. Введение в теоретико-числовые методы криптографии / И.А. Круглов [и др.]. – СПб: Лань, 2011. – 400 с.
2	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
3	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. – Самара : ПГУТИ, 2019. – 68 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/223319 (дата обращения: 07.07.2023). – Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024)

4	ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022 (срок предоставления с 12.01.2023 по 11.01.2024)
5	ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала, работа с учебно-методической литературой, подготовка отчетов по лабораторным работам.
Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован электронный курс, на котором размещены материалы к лекции и задания к лабораторным работам.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:

ПО ОС Windows v.7, 8, 10, Linux.

При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

18. Материально-техническое обеспечение дисциплины:

1) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19'', мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6'' FHD Lenovo V155-15API

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

3) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17'', мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-3 Теоретические аспекты криптографии. Криптографические методы и	ОПК-10	ОПК-10.1, ОПК-10.2, ОПК-10.3,	Контрольная работа по разделам дисциплины. Лабораторные работы 1-

	стандарты. Криптоанализ		ОПК-10.4, ОПК-10.5, ОПК-10.6	7. Тест по соответствующим разделам

Промежуточная аттестация

Форма контроля – зачет с оценкой

Оценочные средства для промежуточной аттестации

Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на практических занятиях

Контрольная работа по теоретической части курса

Лабораторные работы

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует таблице, приведенной ниже
3	Лабораторная работа	Содержит 7 заданий	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену (зачету с оценкой), в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену (зачету с оценкой).
4	КИМ промежуточной аттестации	Каждый контрольно- измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкала оценивания приведена ниже

Пример задания для выполнения лабораторной работы

Лабораторная работа № 2

«Блочное симметричное шифрование»

Цель работы

Практическое изучение особенностей работы одного из методов построения блочных шифров – сети Фейстеля.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы

Количество отведённых аудиторных часов - 4

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма при различных значениях параметров. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Реализовать процедуры шифрования и расшифровки информации с использованием сети Фейстеля заданной архитектуры (рисунок 1). Размер шифруемого блока 64 бита (*b*=6), размеры подблоков L и R по 32 бита. Секретный ключ K – случайная 64-битная последовательность. Раундовые ключи $K_i = (K >>> i*3)_{0..31}$, $i = \overline{0,n-1}$. Число раундов n изменяется от 2 до 12. Образующая функция $F(L_i, K_i) = (L_i <<< 9) \oplus (\sim((K_i >>> 11) \otimes L_i))$, $i = \overline{0,n-1}$. Исследовать влияние параметров сети на качество получаемых зашифрованных последовательностей.

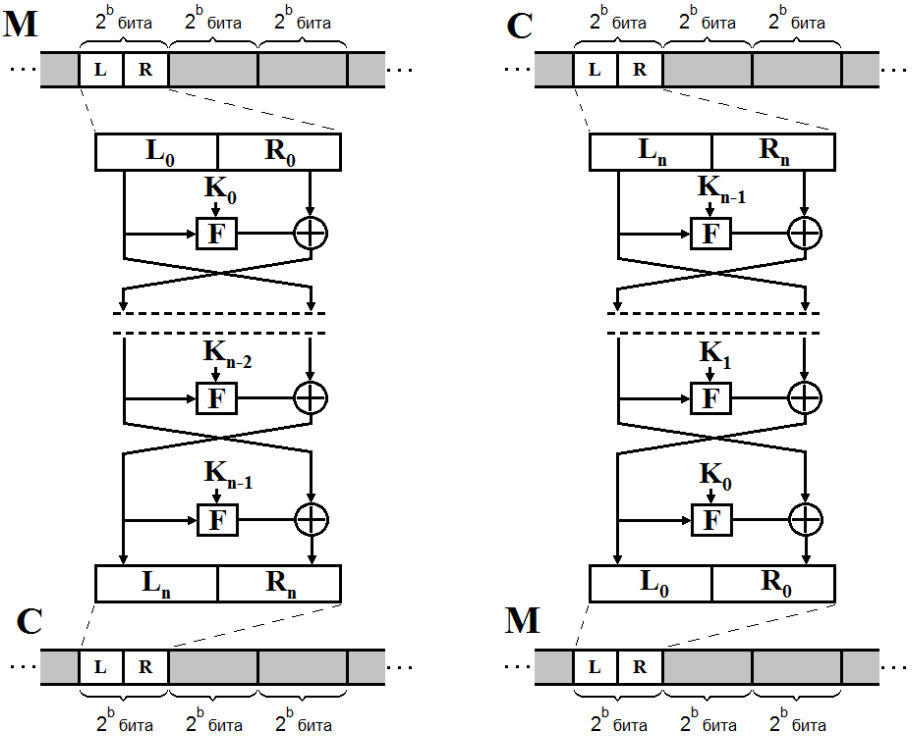

Рисунок 1

Примеры контрольных вопросов:

1. На примере своего варианта реализации практического задания пояснить свойства симметричности и обратимости сети Фейстеля.

2. Каким способом достигаются эффекты рассеивания и перемешивания?

Пример заданий теста по разделам дисциплины

1	Максимальная длина ключа в алгоритме Blowfish *а) 512 бит* *б) 128 бит* *в) 256 бит* *г) 448бит*	

2	Задачей дискретного логарифмирования является *а) нахождение степени, в которую следует возвести простое число для получения заданного целого числа* *б) нахождение степени, в которую следует возвести целое число для получения заданного целого числа* *в) разложение числа на простые сомножители*	
3	Какой из алгоритмов реализует асимметричное шифрование и м. использоваться для ЭП *а) 3DES* *б) Blowfish* *в) AES* *г) RSA*	
4	Хеш-функция должна обладать следующими свойствами *а) для любого данного значения хеш-кода h вычислительно невозможно найти M такое, что H (M) = h* *б) хеш-функция H должна применяться к блоку данных фиксированной длины* *в) хеш-функция H создает выход фиксированной длины* *г) хэш-функция H должна создавать выход произвольной длины* *д) для любого данного x вычислительно невозможно найти y ≠ x, что H(y) = H(x)* *е) для любого данного x вычислительно невозможно найти H (x)*	
…	…	

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине.

Задания закрытого типа

1. Шифр – это

а) состояние, выражающее процесс образования зашифрованных данных из открытых данных;

б) ключевое запоминающее устройство;

в) совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей;

г) значение исходных открытых параметров алгоритма криптографического преобразования

2. Для создания подписи следует использовать

а) свой закрытый ключ;

б) свой открытый ключ;

в) закрытый ключ получателя;

г) открытый ключ получателя

3. Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называются

а) блочными шифрами;

б) поточными шифрами;

в) двоичными аддитивными шифрами;

г) криптосистемами с ключом однократного применения

4. Алгоритм Диффи-Хеллмана основан на следующей математической задаче

а) факторизации числа;

б) нахождения простых чисел;

в) дискретного логарифмирования

5. Целостность – это

а) невозможность несанкционированного просмотра информации;

б) невозможность несанкционированного доступа к информации;
в) невозможность несанкционированного изменения информации

6. Функция, предназначенная для сжатия строки произвольной длины до нескольких десятков или сотен бит
а) ЭЦП;
б) логарифмическая функция;
в) функция Эйлера;
г) хеш-функция

7. Максимальная длина ключа в алгоритме Blowfish
а) 512 бит;
б) 128 бит;
в) 256 бит;
г) 448 бит

8. Размер общего ключа алгоритма 3DES (все ключи разные)
а) 56 бит;
б) 112 бит;
в) 168 бит;
г) 256 бит

9. Название криптосистем, в которых ключ шифрования и ключ дешифрования совпадают
а) симметричные;
б) асимметричные;
в) простые;
г) гибридные

10. Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем
а) идентификация;
б) авторизация;
в) аутентификация;
г) контроль целостности

11. Алгоритм Диффи-Хеллмана дает возможность
а) безопасно обменяться общим секретом при условии аутентификации сторон;
б) безопасно обменяться общим секретом;
в) зашифровать сообщение;
г) подписать сообщение

12. Порядок использования операций шифрования и расшифровки в алгоритме 3DES при создании зашифрованного сообщения
а) $C = E_{K1}[D_{K2}[E_{K1}[M]]]$, $K1 \neq K2$ $(E \rightarrow D \rightarrow E)$;
б) $C = D_{K1}[E_{K2}[D_{K1}[M]]]$, $K1 \neq K2$ $(D \rightarrow E \rightarrow D)$;
в) не имеет значения

13. Какой из алгоритмов реализует асимметричное шифрование и м. использоваться для ЭЦП
а) 3DES;
б) Blowfish;
в) AES;
г) RSA

14. Алгоритм RSA основан на следующей математической задаче
а) дискретного логарифмирования;
б) факторизации числа;
в) нахождения простых чисел

15. Другое название линейного поточного шифрования данных
а) перестановка;
б) гаммирование;
в) подстановка;
г) имитовставка

16. Разрядность шифруемых блоков данных в алгоритме RSA

а) больше разрядности ключа;
б) равна разрядности ключа;
в) меньше разрядности ключа;
г) произвольная

17. Хеш-функция должна обладать следующими свойствами (несколько ответов)

а) для любого данного значения хеш-кода h вычислительно сложно найти M такое, что H(M) = h;
б) хеш-функция H должна применяться к блоку данных фиксированной длины;
в) хеш-функция H создает выход фиксированной длины;
г) хеш-функция H должна создавать выход произвольной длины;
д) для любого данного x вычислительно сложно найти y ≠ x, что H(y) = H(x);
е) для любого данного x вычислительно сложно найти H (x)

18. Отличие самосинхронизирующихся поточных шифров от блочных

а) шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма;
б) шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности;
в) для шифрования и расшифровки используются разные ключи;
г) каждый блок открытого текста шифруется независимо от остальных блоков

19. Отличие синхронных поточных шифров от блочных

а) шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности;
б) для шифрования и расшифровки используются разные ключи;
в) каждый блок открытого текста шифруется независимо от остальных блоков;
г) шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма

20. Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что

а) в противном случае атакующий может взломать дискретный логарифм;

б) в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом;
в) в противном случае стороны не смогут вычислить общий секрет;

21. Режим шифрования, сохраняющий статистические особенности открытого текста

а) Cipher block chaining (CBC);
б) Cipher feed back (CFB);
в) Electronic code book (ECB)

22. Задачей дискретного логарифмирования является

а) нахождение степени, в которую следует возвести простое число для получения заданного целого числа;
б) нахождение степени, в которую следует возвести целое число для получения заданного целого числа;
в) разложение числа на простые сомножители

23. Электронная подпись – это

а) имитовставка;
б) информация, необходимая для шифрования и расшифровки сообщений;
в) способ преобразования исходного секретного сообщения с целью его защиты;
г) присоединяемый к сообщению блок данных, полученный с использованием криптографического преобразования

24. Функция, для которой легко найти прямое отображение и очень сложно найти обратное

а) нелинейная;
б) односторонняя;
в) линейная;
г) многозначная

25. Режим CBC используется для того, чтобы

а) одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки;
б) не было необходимости разбивать сообщение на целое число блоков достаточно большой длины;
в) увеличить скорость шифрования

26. Наука, изучающая математические методы нарушения конфиденциальности и целост-

ности информации

а) криптоанализ;
б) ктиптология;
в) криптография;
г) стегоанализ

27. Ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст

а) коллизия;
б) избыточность;
в) хеширование;
г) атака повтора

28. Протокол Нидхема-Шредера применяется для

а) шифрования;
б) аутентификации;
г) выработки электронной подписи

29. Метод построения блочных шифров, используемый в алгоритме AES

а) SP-сеть;
б) сеть Фейстеля

30. Разрядность ключа алгоритма шифрования ГОСТ Р 34.12-2015

а) 128 бит;
б) 192 бита;
в) 256 бит;
г) 320 бит

Задания открытого типа

1. Набор криптографических преобразований, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса.
2. Событие, в результате которого произошла или могла произойти утрата одного из свойств криптографического ключа, обеспечивающего безопасность криптосистемы
3. Механизм, генерирующий случайные величины для дальнейшего их использования в качестве инициализационного вектора ГПСЧ.
4. Устройство или алгоритм, который выдает последовательность статистически независимых и несмещенных бит.
5. Генераторы случайных чисел по способу получения чисел делятся на
6. Задача обращения функции g^x в некоторой конечной мультипликативной группе G называется.
7. Специальные таблицы поиска для обращения криптографических хеш-функций (использующие различные функции редукции).
8. Средство для обеспечения имитозащиты в протоколах аутентификации сообщений с доверяющими друг другу участниками – специальный набор символов, добавляемый к сообщению, предназначенный для обеспечения его целостности и аутентификации источника данных.
9. Перечислите известные алгоритмы диверсификации секретных ключей на основе строковых значений пароля (минимум 2 алгоритма).
10. Порядок использования ключей в асимметричных криптосистемах при шифровании и расшифровании данных. Шифрование на … ключе, расшифрование на … ключе.
11. Порядок использования ключей при создании и проверке электронной подписи (асимметричный вариант). Создание подписи на … ключе, проверка на … ключе.
12. Вид злоумышленных действий, при котором абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал.
13. Описание распределенного алгоритма, в процессе выполнения которого два (или более) участников последовательно выполняют определенные действия и обмениваются сообщениями.

Задания с развёрнутым ответом

1. Дайте определение электронной подписи. Нарисуйте обобщенную схему подписывания п проверки подписи. Распишите схему электронной подписи на основе алгоритма RSA (с двумя ключевыми парами).

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение электронной подписи. Корректную схему подписывания и проверки электронной подписи, а также корректную схему электронной подписи на основе алгоритма RSA.	3 балла
Обучающийся приводит полное и безошибочное определение электронной подписи. Приводит схему подписывания и проверки электронной подписи, а	2 балла

также схему электронной подписи на основе алгоритма RSA. Описание может содержать незначительные неточности.	
Представлено корректное определение электронной подписи. Схема подписывания и проверки электронной подписи может содержать незначительные неточности. Схема электронной подписи на основе алгоритма RSA не приведена или содержит существенные ошибки.	1 балл
Представлено неполное или содержащее грубые ошибки определение электронной подписи. Схема подписывания и проверки электронной подписи отсутствует или имеет существенные ошибки. Схема электронной подписи на основе алгоритма RSA не приведена или содержит существенные ошибки.	0 баллов

2. Опишите основные режимы выполнения алгоритмов блочного симметричного шифрования (ECB, CBC, CFB, OFB, CTR), приведите схемы их работы. Сформулируйте рекомендации по использованию каждого их режимов.

Критерии оценивания	Шкала оценок
Обучающийся приводит подробное описание режимов выполнения алгоритмов блочного симметричного шифрования, а также схемы их работы. Приводит корректные рекомендации по использованию каждого из режимов.	3 балла
Обучающийся приводит достаточно развернутое описание режимов выполнения алгоритмов блочного симметричного шифрования. Описание может содержать незначительные неточности. Приводит корректные рекомендации по использованию каждого из режимов.	2 балла
Представлено достаточно развернутое, но содержащее незначительные неточности описание режимов выполнения алгоритмов блочного симметричного шифрования. Отсутствуют схемы и рекомендации по использованию каждого из режимов.	1 балл
Представлено неполное или содержащее грубые ошибки описание режимов выполнения алгоритмов блочного симметричного шифрования. Отсутствуют схемы и рекомендации по использованию каждого из режимов.	0 баллов

3. Опишите принципы работы и приведите примеры генераторов псевдослучайных числовых последовательностей (ГПСЧП). Приведите не менее четырех статистических критериев, используемых для проверки выхода ГПСЧП на стохастичность.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое описание принципов работы ГПСЧП, приводит примеры генераторов. Рассматривает не менее четырех статистических критериев для проверки генерируемых псевдослучайных последовательностей на стохастичность.	3 балла
Обучающийся приводит достаточно развернутое описание принципов работы ГПСЧП, но не приводит примеры генераторов. Рассматривает не менее трех статистических критериев для проверки генерируемых псевдослучайных последовательностей на стохастичность.	2 балла
Представлено достаточно полное описание принципов работы ГПСЧП. Примеры генераторов отсутствуют. Рассмотрено менее трех тестов на стохастичность генерируемых последовательностей. В описании содержатся неточности.	1 балл
Представлено неполное или содержащее грубые ошибки описание принципов работы ГПСЧП. Примеры генераторов и тестов на стохастичность последовательностей отсутствуют.	0 баллов

4. Опишите принципы работы регистров сдвига с линейной (LFSR) и нелинейной обратной связью (NLFSR). Приведите примеры генераторов псевдослучайных двоичных последовательностей на основе сдвиговых регистров. Нарисуйте схему, реализующую линейный сдвиговый регистр, задаваемый полиномом $x^7 + x^4 + x^3 + 1$.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое описание принципов работы линейных и нелинейных регистров сдвига. Приводит примеры генераторов на основе сдвиговых регистров, а также корректную схему, реализующую линейный сдвиговый регистр, заданный полиномом.	3 балла
Обучающийся приводит достаточно развернутое описание принципов ра-	2 балла

боты линейных и нелинейных регистров сдвига. Приводит корректную схему, реализующую линейный сдвиговый регистр, заданный полиномом. Допускаются незначительные неточности, отсутствуют примеры генераторов.	
Представлено достаточно полное и корректное описание принципов работы линейных и нелинейных регистров сдвига. Отсутствуют примеры генераторов. Приведенная схема сдвигового регистра, соответствующая заданному полиному, содержит неточности.	1 балл
Представлены неполное или содержащее грубые ошибки описание принципов работы линейных и нелинейных регистров сдвига. Отсутствуют примеры генераторов. Отсутствует или приведена некорректная схема сдвигового регистра, соответствующая заданному полиному.	0 баллов

5. Дайте определение криптографической хеш-функции. Сформулируйте требования, предъявляемые к криптографическим хеш-функциям. Распишите схему Меркла-Дамгарда.

Критерии оценивания	Шкала оценок
Обучающийся приводит безошибочное определение криптографической хеш-функции. Приводит полные и корректные требования, предъявляемые к криптографическим хеш-функциям, корректную схему Меркла-Дамгарда.	3 балла
Обучающийся приводит безошибочное определение криптографической хеш-функции. Приводит полные требования, предъявляемые к криптографическим хеш-функциям, а также схему Меркла-Дамгарда. Описание может содержать незначительные неточности.	2 балла
Представлено корректное определение криптографической хеш-функции. Требования, предъявляемые к криптографическим хеш-функциям, приведены частично. Схема Меркла-Дамгарда содержит неточности.	1 балл
Представлено неполное или содержащее ошибки определение криптографической хеш-функции. Требования, предъявляемые к криптографическим хеш-функциям, приведены частично и содержат ошибки. Схема Меркла-Дамгарда не приведена или содержит существенные ошибки.	0 баллов

6. Распишите схему распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых.

Критерии оценивания	Шкала оценок
Обучающийся приводит корректные схемы распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых, а также развернутое их описание.	3 балла
Обучающийся приводит схемы распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых и краткое их описание. Описание может содержать незначительные неточности.	2 балла
Приведены обе схемы распределения ключей Диффи-Хеллмана, но в них содержатся неточности. Приведена только одна из схем распределения ключей Диффи-Хеллмана (классический вариант либо вариант на эллиптических кривых).	1 балл
Представлена одна их схем распределения ключей Диффи-Хеллмана (классический вариант либо вариант на эллиптических кривых). Схема содержит существенные ошибки.	0 баллов

7. Дайте определение криптографического протокола. Распишите схему работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение криптографического протокола. Приводит корректное описание этапов работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами.	3 балла
Обучающийся приводит полное и безошибочное определение криптографического протокола. Приводит описание основных этапов работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами. Описание может содержать незначительные неточности.	2 балла

Обучающийся приводит корректное определение криптографического протокола. Приводит только один из вариантов (симметричный или асимметричный) протокола Нидхема-Шредера. Описание может содержать неточности.	1 балл
Представлено неполное или некорректное определение криптографического протокола. Приведены неполные или некорректные описания вариантов протокола Нидхема-Шредера для аутентификации и обмена ключами.	0 баллов

8. Отпишите алгоритм шифрования Эль-Гамаля.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание алгоритма шифрования Эль-Гамаля.	3 балла
Обучающийся приводит развернутое описание алгоритма шифрования Эль-Гамаля, которое может содержать незначительные неточности.	2 балла
Обучающийся приводит недостаточно развернутое описание алгоритма шифрования Эль-Гамаля. Описание может содержать отдельные неточности.	1 балл
Представлено неполное или некорректное описание алгоритма шифрования Эль-Гамаля. Присутствуют грубые ошибки или неточности.	0 баллов

9. Опишите схему централизованного управления распределением открытых ключей.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание схемы централизованного управления распределением открытых ключей.	3 балла
Обучающийся приводит развернутое описание схемы централизованного управления распределением открытых ключей, которое может содержать незначительные неточности.	2 балла
Обучающийся приводит недостаточно развернутое описание схемы централизованного управления распределением открытых ключей. Описание может содержать отдельные неточности.	1 балл
Представлено неполное или некорректное описание схемы централизованного управления распределением открытых ключей. Присутствуют грубые ошибки или неточности.	0 баллов

10. Что такое хеш-функция и какова ее роль в криптографии?

Критерии оценивания	Шкала оценок
Обучающийся приводит безошибочное определение хеш-функции, а также развернутое описание ее роли в криптографии.	3 балла
Обучающийся приводит безошибочное определение хеш-функции, а также развернутое описание ее роли в криптографии. Ответ может содержать незначительные неточности.	2 балла
Обучающийся приводит корректное определение хеш-функции, отсутствует описание ее роли в криптографии.	1 балл
Представлено неполное или некорректное определение хеш-функции, отсутствует описание ее роли в криптографии, присутствуют грубые ошибки.	0 баллов

11. Отпишите алгоритм шифрования Эль-Гамаля.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание алгоритма шифрования Эль-Гамаля.	3 балла
Обучающийся приводит развернутое описание алгоритма шифрования Эль-Гамаля, которое может содержать незначительные неточности.	2 балла
Обучающийся приводит недостаточно развернутое описание алгоритма шифрования Эль-Гамаля. Описание может содержать отдельные неточности.	1 балл
Представлено неполное или некорректное описание алгоритма шифрования Эль-Гамаля. Присутствуют грубые ошибки или неточности.	0 баллов

12. Опишите основные этапы жизненного цикла криптографических ключей.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и полностью корректное описание основных этапов жизненного цикла криптографических ключей.	3 балла
Обучающийся приводит развернутое описание основных этапов жизненного цикла криптографических ключей. Описание может содержать незначительные неточности.	2 балла
Обучающийся приводит частичное описание жизненного цикла криптографических ключей.	1 балл
Представлено неполное или некорректное описание основных этапов жизненного цикла криптографических ключей. Присутствуют грубые ошибки или неточности.	0 баллов

13. Опишите принцип работы симметричных поточных шифров. Распишите обобщенные схемы работы синхронного и самосинхронизирующегося шифра, приведите рекомендации по их использованию в условиях возможного искажения зашифрованных данных.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное описание принципов работы симметричных поточных шифров. Приводятся корректные схемы работы синхронного и самосинхронизирующегося шифра, а также точные рекомендации по их использованию в условиях возможного искажения зашифрованных данных.	3 балла
Обучающийся приводит достаточно полное описание принципов работы симметричных поточных шифров. Приводятся схемы работы синхронного и самосинхронизирующегося шифра, а также точные рекомендации по их использованию в условиях возможного искажения зашифрованных данных. Описание может содержать незначительные неточности.	2 балла
Обучающийся приводит достаточно полное описание принципов работы симметричных поточных шифров. Приведены неполные, содержащие неточности, схемы работы синхронного и самосинхронизирующегося шифра. Отсутствуют рекомендации по их использованию в условиях возможного искажения зашифрованных данных.	1 балл
Представлено неполное или некорректное описание принципов работы симметричных поточных шифров, а также схемы работы синхронного и самосинхронизирующегося шифра. Присутствуют грубые ошибки или неточности.	0 баллов

14. Дайте определение линейного сдвигового регистра. Напишите реализацию регистра сдвига с линейной обратной связью (LFSR), задаваемого полиномом $x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$. Приведите два варианта реализации – LFSR Фибоначчи и LFSR Галуа. Язык программирования любой.

Критерии оценивания	Шкала оценок
Обучающийся приводит полные и безошибочное определение линейного сдвигового регистра, а также корректные и оптимальные реализации LFSR Фибоначчи и LFSR Галуа для регистра, описываемого заданным полиномом.	3 балла
Обучающийся приводит достаточно полное определение линейного сдвигового регистра, а также корректные, но, возможно, неоптимальные реализации LFSR Фибоначчи и LFSR Галуа для регистра, описываемого заданным полиномом. Описание может содержать незначительные неточности.	2 балла
Обучающийся приводит достаточно полное определение линейного сдвигового регистра. Приведена реализация лишь одного из вариантов LFSR Фибоначчи или Галуа. Описание может содержать незначительные неточности.	1 балл
Представлено неполное или некорректное определение линейного сдвигового регистра. Приведена реализация лишь одного из вариантов LFSR Фибоначчи или Галуа, содержащая существенные ошибки. Приведены реализации двух вариантов LFSR содержащие грубые ошибки или неточности.	0 баллов

15. Опишите компоненты и схему работы протокола аутентификации Kerberos. Сформулируйте основные преимущества данного протокола.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание схемы работы протокола аутентификации Kerberos. Корректно формулирует его преимущества.	3 балла
Обучающийся приводит достаточно развернутое описание схемы работы протокола аутентификации Kerberos. Корректно формулирует его преимущества. Описание может содержать незначительные неточности.	2 балла
Обучающийся приводит краткое, содержащее незначительные неточности, описание схемы работы протокола аутентификации Kerberos. Преимущества протокола не приводятся.	1 балл
Представлено неполное или некорректное описание схемы работы протокола аутентификации Kerberos. Преимущества протокола сформулированы некорректно или не приводятся.	0 баллов

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.
Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены в таблице, приведенной ниже.

Для оценивания результатов обучения на экзамене (зачете с оценкой) используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
2. умение проводить обоснование и представление основных теоретических и практических результатов;
3. умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторных заданий;
4. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
5. владение навыками программирования в рамках выполняемых лабораторных заданий.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций; повы-
- шенный (продвинутый) уровень сформированности компетенций; порого-
- вый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете с оценкой

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при	Повышенный уровень	Отлично

решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.		
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

Примерный перечень вопросов к зачету

№	Содержание
1	Алгоритмы симметричного шифрования
2	Криптосистемы с открытым ключом, однонаправленные функции
3	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
4	Прямая и арбитражная ЭП
5	Электронная подпись
6	Однонаправленные хэш-функции.
7	Алгоритм шифрования RSA
8	Схема распределения ключей Диффи-Хеллмана на основе эллиптических кривых.
9	Алгоритм шифрования DES, тройной DES
10	Алгоритм электронной подписи на основе эллиптических кривых ECDSA
11	Алгоритм шифрования Эль-Гамаля
12	Криптография с использованием эллиптических кривых
13	Алгоритм шифрования Blowfish
14	Квантовая криптография
15	Алгоритм хеширования MD5
16	Сеть Фейстеля
17	Система распределения ключей Диффи-Хеллмана
18	Нелинейные регистры сдвига с обратной связью
19	Гаммирование, линейный регистр сдвига с обратной связью
20	Программные датчики ПСП чисел

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий
обработки и защиты информации

_____ А.А. Сирота

__.__.2023

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.45 Методы и средства криптографической защиты информации

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
2. Система распределения ключей Диффи-Хеллмана

Преподаватель_____ М.А. Дрюченко