

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

25.01.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.1.28 Методы и средства защиты компьютерной информации

(код и наименование дисциплины по учебному плану)

Направление подготовки
(специальность)

09.03.04 Программная инженерия

Квалификация выпускника

Бакалавр

(бакалавр/магистр/специалист)

Направленность

Разработка программных систем

Курс 3
Семестр 6

Распределение учебного времени

Трудоемкость по учебному плану	216 / 6	часов/зачетных единиц
Лекции	32	часов
Лабораторные работы	32	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	64	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	116	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	6	семестр
Зачет	-	семестр
БРК, ДЗ	-	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 09.03.04 Программная инженерия

Программу составили:

заведующий кафедрой с ученой степенью кандидата наук	ИиСП	СОГЛАСОВАНО	А.В. Бородин
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информатики и системного программирования

25.01.2023	протокол №	1
(дата)		

Заведующий кафедрой	СОГЛАСОВАНО	А.В. Бородин
		(И.О. Фамилия)

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)
кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	А.В. Бородин
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит
выпускающая кафедра

	СОГЛАСОВАНО	А.А. Кречетов
		(И.О. Фамилия)

Эксперт(ы): Егошин Алексей Борисович, ген. директор ООО "Цитрус"

Рабочая программа проверена и зарегистрирована в УМЦ 01.03.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационн ой и библиографиче ской культуры с применением информационн о-коммуникацион ных технологий и с учетом основных требований информационн ой безопасности	ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знания: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. умения: навыки:
	ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знания: умения: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. навыки:
	ОПК-3.3 Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	знания: умения: навыки: Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

2. ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	ОПК-7.1. Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий	знания: Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий. умения: навыки:
	ОПК-7.2 Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ	знания: умения: Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ. навыки:
	ОПК-7.3 Имеет навыки программирования, отладки и тестирования прототипов программно-технических	знания: умения: навыки: Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач.

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Основы программирования (ОПК-3), Алгоритмы и структуры данных (ОПК-3), Теория вычислительных процессов (ОПК-7)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих практиках: Преддипломная практика (ОПК-3), Преддипломная практика (ОПК-7); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-3), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-7)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии,

реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические и лабораторные занятия, процедуры самообучения

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция, проблемная лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Криптографические методы и средства защиты компьютерной информации	116	ОПК-3, ОПК-7
Лекция. Лекция №1. Понятие модели угроз. Классификация моделей угроз. Дисциплина МиСЗКИ как ответ на разрешимые формальные модели угроз. Традиционные нотации дисциплины. Отражение нотаций в УК РФ.	2	
Лекция. Лекция №2. Концепция симметричной криптографии. КС Цезаря: механическая нотация. КС Вижинера: нотация в терминах одномодульной системы вычетов. Виды ключей. Понятие криптоанализа. Атака на шифр Цезаря-Вижинера с короткопериодическим ключом. Результат К. Шеннона (1947).	2	
Лекция. Лекция №3. Генераторы случайных равномерно распределенных чисел. Физические датчики энтропии. Системотехнические принципы генерации равномерно распределенных чисел.	2	
Лекция. Лекция №4. ПСЧ и практически стойкие КС. Понятие практической стойкости. ГПСЧ: история, ЛКДПСЧ, выбор параметров ЛКДПСЧ.	4	
Лекция. Лекция №5. Асимметричные КС: идеи, свойства. Криптосистема RSA: принципы, генерация ключей, стойкость. Варианты использования. Идея ЭП.	4	
Лекция. Лекция №6. Понятие криптографической хеш-функции.	2	
Лекция. Лекция №7. Криптографические протоколы. Основной тезис. Классический метод перебора. Верификация криптографических протоколов. Пример: протокол аналогового голосования. Пример полной реализации механизма ЭП.	2	
Лабораторная работа. Лабораторная работа №1. Реализация модели симметричной КС на основе схемы "граблей" Цезаря с небольшим количеством "зубьев" и атака на нее методом сужения.	12	
Лабораторная работа. Лабораторная работа №2. Реализация модели симметричной КС на основе использования ЛК-ключа и реализация корреляционной атаки на нее.	12	
Лабораторная работа. Лабораторная работа №3. реализация криптографической хеш-функции в соответствии с заданием.	8	

Задания для самостоятельной работы, в том числе выполнение История криптографии.		
Статья К. Шеннона 1947 г.		
Современные генераторы энтропии.		
Возникновение постквантовой криптографии.	66	
Некриптографические методы и средства защиты компьютерной информации	64	ОПК-3, ОПК-7
Лекция. Лекция №8. Субъектно-объектный подход к анализу ВС. Теорема об отсутствии доверенных субъектов в ВС с архитектурой фон Неймана. Понятие доверенной аппаратной компоненты.	8	
Лекция. Лекция №9. Знакомство с концепцией и технологий TRM.	6	
Задания для самостоятельной работы, в том числе выполнение Изделия серии КРИПТОН.		
Изделие АККОРД АМДЗ.		
Технология TRM.	50	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

Занятия лекционного типа дают систематизированные знания по дисциплине, концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации.

Подготовка к занятиям семинарского типа включает ознакомление с планом лабораторного занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой дисциплины.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины, оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины включает выполнение лабораторных работ.

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе.

Формой промежуточной аттестации по дисциплине является экзамен.

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Баричев, Сергей Геннадьевич. Основы современной криптографии [Текст] : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. 3-е изд., стер. Москва: Горячая линия - Телеком, 2020. - 175 с. ISBN 978-5-9912-0182-7. Экземпляры: всего 24.	24
2.	Глухов, М. М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] / Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Санкт-Петербург: Лань, 2022. - 400 с. ISBN 978-5-8114-1116-0.	https://e.lanbook.com/book/210746
3.	Рацеев, С. М. Математические методы защиты информации. [Электронный ресурс] / Рацеев С. М. Санкт-Петербург: Лань, 2023. - 544 с. ISBN 978-5-8114-8589-5.	https://e.lanbook.com/book/326153
4.	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / Прохорова О. В. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с. ISBN 978-5-507-46010-6.	https://e.lanbook.com/book/293009
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	429 (III)	ПК RAMEC GALE/i7-3770/B75M2x4DDR3/GTX650/500S АТА3/монит.LCD PHILIPS 23,6" клав.,мышь (8), Принтер HP LaserJet Professional P1102 (1),	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office

		Проектор VIEWSONIC PJD6550LW белый (1), Комплект учебной мебели (1)	Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
2.	430 (III)	ПК RAMEC GALE/i7-3770/B75M2x4DDR3/GTX650/500S АТА3/монит.LCD PHILIPS 23,6" клав.,мышь (8), Проектор VIEWSONIC PJD6550LW белый (1), Шкаф телекоммуникационный напольный ЦМО ШТК-М (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
3.	521 (I)	Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
4.	522 (I)	Анализатор спектра NS-30A (1), Антенна M102 в компл. с кабелем ВЧ TNCm-SMAm (1), Блок питания лаборат. НУ 3003 D-3 (1), Внешний HDD WD 2TB 3.0 , 3.5"USB (1), Внешний накопитель 1 Seagate Original USB 3.0 4 Tb (1), Внешний накопитель флешка USB TRANSCEND Jetflash 780 64 Gb (1), Гигабитный управляемый коммутатор на 16 портов (1), Измеритель CN -801 HP (1),	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio

	<p>Кондиционер AEG ACS-09HR (1), Многофункциональный измерительный прибор (1), Монитор 20 "Beng FP 202W (2), Монитор LCD Samsung 17" SM 713N (1), МФУ Canon i-SENSYS MF 4018 (1), МФУ 1 Лазерный Canon i-Sensys MF226 (1), Набор ВЧ переходников (1), Ноутбук Dell Latitude E6520 Intel Core I5 Processor 2520M 15,6" (2), Ноутбук TOSHIBA Satellite L655-1H2-RU (1), Паяльная станция AOYUE 968 (1), Переключатель ZX80-DR230 (1), Персональный компьютер 3 Atlant A2X4/4G(3)/512Mb/монитор Pyama 2209/3Y (1), ПК RAMEC GALE LCD LG 23"/Intel i5 4590/MSI B85M-E45/2x4DDR3/GT740 2Gb/500Gb/клав,мышь (28), Преобразователь SP-200-24-AC-DC в кожу 199x99x50мм (1), Приемопередающая программно-конфигурируемая радиоплатформа G32 (1), Принтер Canon LBP 2900 лазерный с кабелем (1), Проектор мультимедийный Hitachi CP-EX250 (1), Проектор мультимедийный Hitachi CP-EX251N (1), Сист. блок Pen D 945 3.4 DDR 2 1024*2/FDD 3.5/250 Gb/DVD-RW/кл+мышь+коврик (1), Системный блок CPU Intel Core i7-6700/ASRod Z-170/32 Gb/GTX 1070/200 Gb/Wi-Fi +клав, мышь (1), Станок сверлильный 350 Вт (1), Универсальная приёмопередающая платформа для проектирования СВЧ-систем компл.mgx92 (1), Усилитель LZY-22 (1), Усилитель ZHL-3A-S (1), Комплект учебной мебели (1)</p>	Enterprise, Комплект ПО для решения основных пользовательских задач
--	---	---

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

!DISC=Методы и средства защиты компьютерной информации

!TYPE=2

!TASK1

Установление подлинности сторон это:

!TRUE

аутентификация

!FALSE

идентификация

!FALSE

шифрование

!FALSE

атака

!TASK2

Криптографический алгоритм, в котором ключи, используемые для шифрования и дешифрования сообщений, одинаковы, называют:

!TRUE

симметричным

!FALSE

асимметричным

!FALSE

синхронным

!FALSE

асинхронным

!TASK3

В большинстве симметричных алгоритмов применяют:

!TRUE

1 ключ

!FALSE

2 ключа

!FALSE

3 ключа

!FALSE

4 ключа

!TASK4

К симметричным схемам шифрования относятся:

!TRUE

схема Вижинера

!FALSE

RSA

!FALSE

DSA

!FALSE

шифр Эль-Гамала

!TASK5

Наилучшими для использования в симметричных схемах шифрования являются случайные ключи, построенные на основе:

!TRUE

шумоподобных последовательностей

!FALSE

регулярных последовательностей

!FALSE

помехоустойчивых кодов

!FALSE

эффективных кодов

!TASK6

Текст, который требуется зашифровать, называется:

!TRUE

открытым

!FALSE

закрытым

!FALSE

тайным

!FALSE

секретным

!TASK7

Семейство обратимых преобразований открытого текста в шифротекст называется:

!TRUE

шифр

!FALSE

ключ

!FALSE

пароль

!FALSE

код

!TASK8

Нормальное применение криптографического преобразования открытого текста, в результате которого образуется шифротекст, называется:

!TRUE

шифрование

!FALSE

дешифрование

!FALSE

кодирование

!FALSE

Декодирование

!TASK9

Процесс нормального применения криптографического алгоритма, итогом которого будет преобразование шифротекста в открытый текст, называется:

!TRUE

дешифрование

!FALSE

декодирование

!FALSE

кодирование

!FALSE

шифрование

!TASK10

Совершенно секретной системой является

!TRUE

криптосистема Вернама

!FALSE

криптосистема RSA

!FALSE

криптосистема на эллиптической кривой

!FALSE

блочная криптосистема

!TASK11

Наука, которая занимается поиском и исследованием математических методов преобразования информации с целью ее защиты, называется:

!TRUE

криптография

!FALSE

криптоанализ

!FALSE

шифрование

!FALSE

дешифрование

!TASK12

Процесс исследования возможности расшифровывания информации без знания ключей называется:

!TRUE

криптоанализ

!FALSE

криптография

!FALSE

дешифровка

!FALSE

расшифровка

!TASK13

Конечное множество используемых для кодирования информации знаков это:

!TRUE

Алфавит

!FALSE

Латиница

!FALSE

Символика

!FALSE

Нет правильного ответа

!TASK14

Упорядоченный набор из элементов алфавита это:

!TRUE

Текст

!FALSE

Шрифт

!FALSE

Стенограмма

!FALSE

Экспликация

!TASK15

Процесс преобразования исходного текста, который носит также название открытого текста, в шифротекст, называемый также криптограммой, это:

!TRUE

Шифрование

!FALSE

Зашифровка

!FALSE

Кодирование

!FALSE

Декодирование

!TASK16

Обратный шифрованию процесс, когда на основе ключа зашифрованный текст преобразуется в исходный, называется:

!TRUE

Дешифрование

!FALSE

Шифрование

!FALSE

Раскодирование

!FALSE

Декодирование

!TASK17

Информация, необходимая для шифрования и дешифрования текстов:

!TRUE

Ключ

!FALSE

Знак

!FALSE

Контроль

!FALSE

Секрет

!TASK18

Обычно представляет собой последовательный ряд букв алфавита:

!TRUE

ключ

!FALSE

секретный канал

!FALSE

открытый канал

!FALSE

шрифт

!TASK19

Криптографическая система называется криптосистемой _____, если ее стойкость основывается на сохранении в секрете алгоритмов шифрования и дешифрования.

!TRUE

ограниченного использования

!FALSE

общего использования

!FALSE

криптосистемой с секретным ключом

!FALSE

криптосистемой с открытым ключом

!TASK20

В честь какого исторического персонажа названа одна из известных криптографических систем:

!TRUE

Юлия Цезаря

!FALSE

Октавиана Августа

!FALSE

Марка Антония

!FALSE

Марка Цицерона

!TASK21

Криптографическая система называется криптосистемой _____, если ее стойкость основывается не на секретности алгоритмов шифрования и дешифрования, а на секретности ключа.

!TRUE

общего использования

!FALSE

ограниченного использования

!FALSE

криптосистемой с секретным ключом

!FALSE

криптосистемой с открытым ключом

!TASK22

Одним из требований обеспечения стойкости общей криптографической системы является:

!TRUE

огромное количество возможных ключей

!FALSE

небольшое количество возможных ключей

!FALSE

два возможных ключа

!FALSE

один возможный ключ

!TASK23

Большое число ключей в общем случае _____ стойкости

криптосистемы.

!TRUE

не обеспечивает

!FALSE

обеспечивает

!FALSE

обеспечивает, если используется правильный ключ

!FALSE

обеспечивает, если открытый текст отвечает специальным требованиям

!TASK24

Криптографическая система называется _____, если в ней любые две стороны, перед тем, как связаться друг с другом, должны заранее договориться между собой об использовании в дальнейшем некоторой секретной части информации, которая и называется секретным ключом.

!TRUE

криптосистемой с секретным ключом

!FALSE

криптосистемой с открытым ключом

!FALSE

общего использования

!FALSE

ограниченного использования

!TASK25

Одним из создателей первой практической реализации криптосистемы с открытым ключом был:

!TRUE

Леонард Адлеман

!FALSE

Клод Шеннон

!FALSE

Уитфрид Диффи

!FALSE

Мартин Хеллман

!TASK26

Одним из создателей первой практической реализации криптосистемы с открытым ключом был:

!TRUE

Эди Шамир

!FALSE

Уитфрид Диффи

!FALSE

Мартин Хеллман

!FALSE

Клод Шеннон

!TASK27

Одним из создателей первой практической реализации криптосистемы с открытым ключом был:

!TRUE

Рональд Ривест

!FALSE

Уитфрид Диффи

!FALSE

Клод Шеннон

!FALSE

Мартин Хеллман

!TASK28

Этот термин относится к процессам системы обработки информации, содержанием которых является генерация и распределение ключей между пользователями.

!TRUE

управление ключами

!FALSE

электронная (цифровая) подпись

!FALSE

криптографическая хеш-функция

!FALSE

дайджест сообщения

!TASK29

Как называется присоединяемый к тексту результат его криптографического преобразования, который позволяет при получении этой совокупности другим пользователем проверить авторство и подлинность сообщения.

!TRUE

Электронной (цифровой) подписью

!FALSE

Шифросистемой с открытым ключом

!FALSE

Шифросистемой с секретным ключом

!FALSE

Симметричной шифросистемой

!TASK30

Каждое положительное целое число, большее единицы, может быть представлено в виде:

!TRUE

произведения степеней простых чисел

!FALSE

произведения простых чисел

!FALSE

произведения четных чисел

!FALSE

произведения нечетных чисел

!TASK31

Одна из теорем Евклида гласит, что множество $\{2, 3, 5, 7, 11, 13, \dots\}$ всех простых чисел

!TRUE

бесконечно

!FALSE

конечно

!FALSE

имеет мощность континуума

!FALSE

нет такой теоремы

!TASK32

_____ – это способность противостоять попыткам хорошо оснащенного современной техникой и знаниями криптоаналитика в попытках: дешифровать перехваченный шифротекст, раскрыть ключи шифрования и/или тайно нарушить целостность и подлинность информации.

!TRUE

Стойкость

!FALSE

Сила

!FALSE

Крепость

!FALSE

Постоянство

!TASK33

_____ представляет собой сумму по модулю два произведений неинвертированных переменных, а также, если необходимо, константы 1.

!TRUE

Полином Жегалкина

!FALSE

Полином Чебышева

!FALSE

Полином Цернике

!FALSE

Полином Лежандра

!TASK34

Полином с коэффициентами вида 0 и 1 - это полином:

!TRUE

Жегалкина

!FALSE

Лежандра

!FALSE

Эрмита

!FALSE

Цернике

!TASK35

Криптосистема RSA основана на:

!TRUE

проблеме факторизации больших чисел;

!FALSE

проблеме решения задачи дискретного логарифмирования;

!FALSE

проблеме генерации больших простых чисел;

!FALSE

проблеме поиска примитивного элемента в циклической группе.

!TASK36

Криптосистема Эль-Гамала основана на:

!TRUE

проблеме решения задачи дискретного логарифмирования;

!FALSE

проблеме факторизации больших чисел;

!FALSE

проблеме генерации больших простых чисел;

!FALSE

проблеме поиска примитивного элемента в циклической группе.

!TASK37

Эффективным алгоритмом для нахождения наибольшего общего делителя двух целых чисел является:

!TRUE

алгоритм Евклида

!FALSE

алгоритм Эратостена

!FALSE

алгоритм Пифагора

!FALSE

алгоритм Франсуа Виета

!TASK38

Эффективным алгоритмом для нахождения целого числа, мультипликативно обратного данному целому по модулю, является:

!TRUE

Расширенный алгоритм Евклида

!FALSE

Расширенный алгоритм Эратостена

!FALSE

Расширенный алгоритм Пифагора

!FALSE

Расширенный алгоритм Франсуа Виета

!TASK39

_____ – это время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция размера задачи или количества входных данных.

!TRUE

Временная сложность

!FALSE

Время воспроизведения алгоритма

!FALSE

Время верификации алгоритма

!FALSE

Время работы алгоритма в рамках конкретной реализации для конкретного вычислителя

!TASK40

_____ алгоритма измеряется временной и емкостной сложностями алгоритма, в зависимости от размера входных данных.

!TRUE

Вычислительная сложность

!FALSE

Временная сложность

!FALSE

Измерительная сложность

!FALSE

Колмогоровская сложность

!TASK41

_____ алгоритма – это емкость необходимой машинной памяти.

!TRUE

Емкостная сложность

!FALSE

Вычислительная сложность

!FALSE

Временная сложность

!FALSE

Колмогоровская сложность

!TASK42

_____ называют исходное сообщение, которое должен защищать криптограф.

!TRUE

Открытым текстом

!FALSE

Закрытым текстом

!FALSE

Кодированным текстом

!FALSE

Имитовставкой

!TASK43

_____ – это множество обратимых преобразований открытого текста, проводимых с целью его защиты.

!TRUE

Шифр

!FALSE

Код

!FALSE

Символ

!FALSE

Ключ

!TASK44

Процесс применения обратимого преобразования шифросистемы к открытому тексту называется шифрованием или зашифровыванием, а результат этого преобразования –

!TRUE

шифротекстом

!FALSE

расшифровыванием

!FALSE

дешифрованием

!FALSE

кодом

!TASK45

Процесс применения обратимого преобразования шифросистемы к открытому тексту называется шифрованием или зашифровыванием, а результат этого преобразования –

!TRUE

криптограммой

!FALSE

расшифровыванием

!FALSE

дешифрованием

!FALSE

кодом

!TASK46

Процесс обратного преобразования шифротекста в открытый текст называется

!TRUE

расшифровыванием

!FALSE

декодированием

!FALSE

кодообозначениями

!FALSE

раскрытием

!TASK47

Обычные криптосистемы с секретным ключом называют

!TRUE

симметричными криптосистемами.

!FALSE

асимметричными криптосистемами

!FALSE

2-ключевыми криптосистемами

!FALSE

Криптосистемами с открытым ключом

!TASK48

Если криптоаналитик не может уточнять распределение вероятностей возможных открытых текстов по имеющемуся у него шифротексту, даже если он обладает всеми необходимыми для этого средствами, то криптосистема называется:

!TRUE

теоретически стойкой

!FALSE

практически стойкой

!FALSE

среднестойкой

!FALSE

непоколебимой

!TASK49

Задачи, которые не могут быть систематически решены за полиномиальное время, называют:

!TRUE

Трудными

!FALSE

Решаемыми

!FALSE

Легкими

!FALSE

Некорректными

!TASK50

Задачи, которые решаются за полиномиальное время, называются:

!TRUE

решаемыми

!FALSE

нерешаемыми

!FALSE

трудными

!FALSE

неразрешимыми

!TASK51

Согласно теореме Евклида:

!TRUE

Множество простых чисел бесконечно

!FALSE

Множество простых чисел конечно

!FALSE

Все простые числа сведены в единую таблицу Евклида

!FALSE

Единая таблица простых чисел пока до конца не заполнена

!TASK52

Классы эквивалентности, на которые отношение сравнимости по модулю n разбивает множество целых чисел, называют:

!TRUE

классами вычетов по модулю n

!FALSE

классами множества целых чисел

!FALSE

классами сравнимости по модулю n

!FALSE

модульными классами

!TASK53

Функцию, которая отображает строку символов произвольного размера в строку символов фиксированного размера называют:

!TRUE

хеш-функцией

!FALSE

хаш-функцией

!FALSE

зип-функцией

!FALSE

рар- функцией

!TASK54

Потенциальная опасность нарушения одного или нескольких свойств системы защиты называется:

!TRUE

угрозой

!FALSE

намерением

!FALSE

шантажом

!FALSE

подкупом

!TASK55

_____ описывает процесс зашифровывания и осуществляет

зависящее от ключа отображение последовательностей блоков текста (сообщения) открытого в последовательности блоков текста (сообщения) шифрованного.

!TRUE

Функция зашифровывания

!FALSE

Функция криптографическая

!FALSE

Функция односторонняя

!FALSE

Необратимая функция

!TASK56

Функция, описывающая процесс расшифровывания и осуществляющая отображение, обратное к функции зашифровывания, называется:

!TRUE

Функция расшифровывания

!FALSE

Функция равновероятная

!FALSE

Функция односторонняя

!FALSE

Необратимая функция

!TASK57

Функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины называется:

!TRUE

Хеш-функцией

!FALSE

Хеш-значением

!FALSE

Криптографической хеш-функцией

!FALSE

Хитрой функцией

!TASK58

Процесс доверенной загрузки – это,

!TRUE

Когда каждый этап загрузки системы передает управление следующему этапу только после проверки целостности программного обеспечения, функционирующего на следующем этапе.

!FALSE

Когда все программное обеспечение, используемое в ходе загрузки, лицензионное.

!FALSE

Когда все программное обеспечение, используемое в ходе загрузки, получено из доверенных источников.

!FALSE

Когда используется лицензионная операционная система.

!TASK59

Разрешимая формальная модель угроз это:

!TRUE

Формальная модель угроз, для которой существует конечный алгоритм, который за конечное время дает ответ на вопрос «Реализовалась данная угроза или нет?»

!FALSE

Формальная модель угроз, для которой не существует конечного алгоритма, который за конечное время дает ответ на вопрос «Реализовалась данная угроза или нет?»

!FALSE

Формальная модель угроз, для которой существует конечный алгоритм, который за конечное время не дает ответа на вопрос «Реализовалась данная угроза или нет?»

!FALSE

Формальная модель угроз, для которой существует бесконечный алгоритм, который за конечное время дает ответ на вопрос «Реализовалась данная угроза или нет?»

!TASK60

Неразрешимая формальная модель угроз это:

!TRUE

Формальная модель угроз, для которой либо не существует конечного алгоритма, который дает ответ на вопрос «Реализовалась данная угроза или нет?», либо такой конечный алгоритм существует, однако он не способен за конечное время ответить на этот вопрос.

!FALSE

Формальная модель угроз, для которой существует бесконечный алгоритм, который за конечное время дает ответ на вопрос «Реализовалась данная угроза или нет?»

!FALSE

Формальная модель угроз, для которой не существует конечного алгоритма, который за конечное время дает ответ на вопрос «Реализовалась данная угроза или нет?»

!FALSE

Формальная модель угроз, для которой существует конечный алгоритм, который за конечное время не дает ответа на вопрос «Реализовалась данная угроза или нет?»

!END

Перечень вопросов для проведения промежуточной аттестации

1. Понятие модели угроз. Классификация моделей угроз.
2. Классификационные признаки моделей угроз, рассматриваемых в курсе «Методы и средства защиты информации».
3. Модель угроз «Несанкционированный доступ к передаваемой через открытый канал информации». Криптографические методы противодействия данной угрозе.
4. Модель угроз «Навязывание ложной информации третьей стороной в открытом канале передачи данных». Криптографические методы противодействия данной угрозе.
5. Модель угроз «Искажение передаваемой в открытом канале информации». Понятие семантической избыточности информации. Роль семантической избыточности информации в

противодействию данной угрозе.

6. Модель угроз «Искажение передаваемой в открытом канале информации». Криптографические методы противодействия данной угрозе. Классификация методов. Пример.
7. Понятие симметричной криптографической системы. Преимущества и недостатки.
8. Понятие асимметричной криптографической системы. Преимущества и недостатки. Пример.
9. Понятие криптографической хеш-функции.
10. Комбинированные криптографические системы. Причины появления. Принципы организации.
11. Модель угроз «Искажение передаваемой в открытом канале информации». Методы противодействия данной угрозе, основанные на симметричной криптографии.
12. Модель угроз «Искажение передаваемой в открытом канале информации». Методы противодействия данной угрозе, основанные на асимметричной криптографии.
13. Модель угроз «Искажение передаваемой в открытом канале информации». Методы противодействия данной угрозе, основанные на использовании криптографических хеш-функций.
14. Понятие электронной цифровой подписи. Основы и принципы.
15. Простейшие протоколы обеспечения многократной электронной цифровой подписи. Пример применения.
16. Проблема генерации ключей. Генезис проблемы: от засекреченной детерминанты к абсолютно случайной ключевой последовательности на примере симметричной криптографической системы Цезаря.
17. Короткопериодические ключевые последовательности. Анализ стойкости.
18. Длиннопериодические ключевые последовательности. Датчики псевдослучайных чисел и их роль для создания длиннопериодических ключевых последовательностей. Анализ стойкости длиннопериодических ключевых последовательностей.
19. Линейный конгруэнтный датчик псевдослучайных чисел. Классификация. Мультипликативный и смешанный конгруэнтный методы. Условия выбора мультипликативного конгруэнтного метода.
20. Линейный конгруэнтный датчик псевдослучайных чисел. Выбор модуля.
21. Линейный конгруэнтный датчик псевдослучайных чисел. Выбор множителя.
22. Линейный конгруэнтный датчик псевдослучайных чисел. Выбор параметров для компьютеров с десятичной архитектурой.
23. Линейный конгруэнтный датчик псевдослучайных чисел. Дерево принятия решений по выбору параметров.
24. Системы гарантированной секретности. Теоретические основы.
25. Понятие Фон Неймановской архитектуры вычислительной системы. Базовые принципы. Проблема получения случайных чисел в рамках данной архитектуры. Основной вывод.
26. Физические принципы генерации случайности. Связь с одним из базовых принципов Фон

Нэймановской архитектуры вычислительных систем. Преимущества и недостатки каждого из рассмотренных принципов.

27. Системотехнические основы построения датчиков случайных чисел. Аналоговый тракт. Причины выбора тех или иных системотехнических решений.
28. Системотехнические основы построения датчиков случайных чисел. Принципы аналого-цифрового преобразования. Причины выбора данного принципа аналого-цифрового преобразования.
29. Математическая основа аналого-цифрового преобразования принадлежности.
30. Статистический контроль выходных последовательностей случайных чисел. Связь с проблемой фликкер-шума.
31. Понятие криптоанализа. Основная посылка криптоанализа.
32. Криптоанализ простейших симметричных криптографических систем с короткопериодическим ключом.
33. Криптоанализ простейших симметричных криптографических систем с псевдослучайным ключом.
34. Понятие криптографического протокола
35. Свойства корректности протокольной основы криптографического протокола
36. Классический метод перебора анализа протоколов
37. Методы анализа криптографических протоколов
38. Анализ и синтез стойких криптографических протоколов на примере протокола секретного аналогового голосования
39. Модели угроз «Нарушение целостности программного обеспечения внутри периметра защиты». Формализация. Субъектно-объектный подход.
40. Аксиомы субъектно-объектного подхода к анализу безопасности информационных систем. Понятие субъекта, объекта и доступа, другие связанные понятия.
41. Классификация доступов в вычислительной системе. Пример.
42. Теорема о неразрешимости множества доверенных субъектов в вычислительной системе Фон Нэймановской архитектуры. Связь с одним из базовых принципов Фон Нэймановской архитектуры. Понятие доверенной аппаратной компоненты.
43. Жизненный цикл вычислительной системы от включения до выключения энергоснабжения на примере IBM PC AT совместимого компьютера. Место доверенной аппаратной компоненты.
44. Укрупненная логическая архитектура дисковых накопителей большой емкости в операционных системах компании Microsoft для IBM PC AT совместимых компьютеров.
45. Области возможного проявления деятельности разрушающих программных воздействий в пространстве состояний жизненного цикла вычислительной системы на примере IBM PC AT совместимого компьютера.
46. Аппаратный модуль доверенной загрузки АККОРД-АМДЗ. Назначение.
47. Аппаратный модуль доверенной загрузки АККОРД-АМДЗ. Принцип работы.

48. Примеры аппаратных решений для создания изолированных программных сред.