Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный индустриальный университет»

Кафедра автоматизации и информационных систем

УТВЕРЖДАЮ
Директор института
информационных технологий и
автоматизированных систем
_____ А.В. Зимин
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

09.03.02 «Информационные системы и технологии»
(направленность (профиль): «Разработка и эксплуатация
информационных систем и технологий»)

Квалификация выпускника
Бакалавр

Форма обучения
Заочная форма

Срок обучения: 4 года 6 месяцев

Год начала подготовки 2025

Новокузнецк
2025

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: daba56d7b892efca3bf5c04ed0251c98b19b099c
Владелец: Директор ИИТиАС Зимин Алексей Валерьевич
Действителен: с 15 января 2025 г. по 10 апреля 2026 г.
Дата и время: 13-05-2025 15:14:44 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:
- Изучение теоретических и прикладных аспектов информационной безопасности.;
- Знакомство с базовыми технологиями защиты информации в информационных системах.

Задачами учебной дисциплины являются:
- Изучение типовых механизмов обеспечения безопасности информационных систем.;
- Получение навыков использования криптографических средств защиты данных в приложениях.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам обязательной части **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:
- Математика;
- Информатика;
- Основы программирования;
- Технологии программирования.

Учебная дисциплина дополняет знания и умения, получаемые по одновременно изучаемым и последующим учебным дисциплинам:
- Проектирование информационно-управляющих систем;
- Программное обеспечение информационно-управляющих систем.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Общепрофессиональные компетенции

Наименование категории (группы) ОПК	Код и наименование ОПК	Код и наименование индикатора достижения ОПК	Планируемые результаты обучения
	ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и	ОПК-2.3 Применяет современные информационные технологии и программные средства при решении прикладных задач	– знать: Информационные технологии и программные средства обеспечения информационной безопасности. . – уметь: Проектировать многоуровневые системы защиты информации

	использовать их при решении задач профессиональной деятельности		.
	ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2 Понимает и использует принципы защиты информации и обеспечивает информационную безопасность	– знать: Методы, подходы и принципы защиты данных в информационных системах .. – уметь: Проектировать и реализовывать прикладные решения в области защиты данных..

4 Объем и содержание учебной дисциплины

Учебные занятия по учебной дисциплине проводятся в форме контактной работы и в форме самостоятельной работы обучающихся.

Контактная работа включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия, практикумы), промежуточную аттестацию обучающихся и иные формы взаимодействия обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации ООП на иных условиях, в том числе при проведении промежуточной аттестации обучающихся. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Объем учебной дисциплины

Сессия / курс		***ИТОГО***	***2 сессия / 4 курс***	***3 сессия / 4 курс***
Форма промежуточной аттестации				*экзамен*
Трудоёмкость	*академ. час.*	***144***	*36*	*108*
	зачетных единиц	***4***	*1*	*3*
Лекции, *академ. час.*		***2***	*2*	*0*
в форме практической подготовки		***0***	*0*	*0*
Лабораторные работы, *академ. час.*		***0***	*0*	*0*
в форме практической подготовки		***0***	*0*	*0*
Практические занятия, *академ. час.*		***2***	*0*	*2*
в форме практической подготовки		***0***	*0*	*0*
Курсовая работа / проект, *академ. час.*		***0***	*0*	*0*
в форме практической подготовки		***0***	*0*	*0*

Консультации, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Самостоятельная работа, *академ. час.*	***131***	*34*	*97*
в форме практической подготовки	***0***	*0*	*0*
Контроль, *академ. час.*	***9***	*0*	*9*
в форме практической подготовки	***0***	*0*	*0*

Содержание учебной дисциплины

Раздел 1 Информационная безопасность;

Тема 1.1 Термины и определения (понятия информационной безопасности, конфиденциальность, целостность, доступность, уязвимость, комплексная защита, риски).;

Тема 1.2 Типовые проблемы безопасности (типовые уязвимости информационных систем, phishing - атаки, spoofing атаки, poisoning - атаки, сетевой флуд, arp, ip spoofing (poisoning), отказ в обслуживании).;

Тема 1.3 Безопасность программного обеспечения (атаки на программное обеспечение, внедрение внешнего кода, атаки crosscripting и injection (SQL injection), переполнение буфера, атаки переполнения буфера, принципы безопасного программирования).;

Раздел 2 Элементы криптографии;

Тема 2.1 Введение в криптографию (история криптографии, логические и криптозащиты (защиты Кирхгофа), перестановочные, подстановочные шифры, примеры логических защит).;

Тема 2.2 Симметричная криптография (криптозащиты, блочные и поточные схемы шифрования, принципы реализации блочных и поточных защит с закрытым ключом, схема Фейстеля, алгоритмы Triple DES, Rijndael (AES)).;

Тема 2.3 Односторонние хэш функции (задачи хэширования данных, контрольные суммы, односторонние хэш функции, алгоритмы md5, sha1).;

Тема 2.4 Асимметричная криптография (идея открытого ключа, простые числа и преобразования, алгоритм RSA (Rivest, Shamir, Adelman), протокол Диффи - Хеллмана).;

Тема 2.5 Электронная цифровая подпись (идея электронной цифровой подписи, цифровые сертификаты, схемы с посредником, алгоритмы RSA, DSA в системах с цифровой подписью).;

Тема 2.6 Аутентификация и авторизация (системы аутентификации и авторизации, задачи, технологии, реализация подсистем аутентификации и авторизации).

5 Перечень тем лекций

№ раздела / темы дисциплины	**Темы лекций**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 1.	Информационная безопасность		
Тема 1.1.	Термины и определения	0.2	

	(понятия информационной безопасности, конфиденциальность, целостность, доступность, уязвимость, комплексная защита, риски).		
Тема 1.2.	Типовые проблемы безопасности (типовые уязвимости информационных систем, phishing - атаки, spoofing атаки, poisoning - атаки, сетевой флуд, arp, ip spoofing (poisoning), отказ в обслуживании).	0.2	
Тема 1.3.	Безопасность программного обеспечения (атаки на программное обеспечение, внедрение внешнего кода, атаки crosscripting и injection (SQL injection), переполнение буфера, атаки переполнения буфера, принципы безопасного программирования).	0.2	
Раздел 2.	Элементы криптографии		
Тема 2.1.	Введение в криптографию (история криптографии, логические и криптозащиты (защиты Кирхгофа), перестановочные, подстановочные шифры, примеры логических защит).	0.1	
Тема 2.2.	Симметричная криптография (криптозащиты, блочные и поточные схемы шифрования, принципы реализации блочных и поточных защит с закрытым ключом, схема Фейстеля, алгоритмы Triple DES, Rijndael (AES)).	0.3	
Тема 2.3.	Односторонние хэш функции (задачи хэширования данных, контрольные суммы, односторонние хэш функции, алгоритмы md5, sha1).	0.3	
Тема 2.4.	Асимметричная криптография (идея открытого ключа, простые числа и преобразования, алгоритм RSA (Rivest, Shamir, Adelman), протокол Диффи - Хеллмана).	0.3	
Тема 2.5.	Электронная цифровая подпись (идея электронной цифровой подписи, цифровые сертификаты, схемы с	0.2	

	посредником, алгоритмы RSA, DSA в системах с цифровой подписью).		
Тема 2.6.	Аутентификация и авторизация (системы аутентификации и авторизации, задачи, технологии, реализация подсистем аутентификации и авторизации).	0.2	
Итого:		**2**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	**Темы практических занятий (семинаров)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 1.	Информационная безопасность		
Тема 1.1.	Термины и определения (понятия информационной безопасности, конфиденциальность, целостность, доступность, уязвимость, комплексная защита, риски).		
Тема 1.2.	Типовые проблемы безопасности (типовые уязвимости информационных систем, phishing - атаки, spoofing атаки, poisoning - атаки, сетевой флуд, arp, ip spoofing (poisoning), отказ в обслуживании).		
Тема 1.3.	Безопасность программного обеспечения (атаки на программное обеспечение, внедрение внешнего кода, атаки crosscripting и injection (SQL injection), переполнение буфера, атаки переполнения буфера, принципы безопасного программирования).		
Раздел 2.	Элементы криптографии		
Тема 2.1.	Введение в криптографию (история криптографии, логические и криптозащиты (защиты Кирхгофа), перестановочные, подстановочные шифры, примеры логических защит).		
Тема 2.2.	Симметричная криптография (криптозащиты, блочные и	1	

	поточные схемы шифрования, принципы реализации блочных и поточных защит с закрытым ключом, схема Фейстеля, алгоритмы Triple DES, Rijndael (AES)).		
Тема 2.3.	Односторонние хэш функции (задачи хэширования данных, контрольные суммы, односторонние хэш функции, алгоритмы md5, sha1).		
Тема 2.4.	Асимметричная криптография (идея открытого ключа, простые числа и преобразования, алгоритм RSA (Rivest, Shamir, Adelman), протокол Диффи - Хеллмана).	1	
Тема 2.5.	Электронная цифровая подпись (идея электронной цифровой подписи, цифровые сертификаты, схемы с посредником, алгоритмы RSA, DSA в системах с цифровой подписью).		
Тема 2.6.	Аутентификация и авторизация (системы аутентификации и авторизации, задачи, технологии, реализация подсистем аутентификации и авторизации).		
Итого:		**2**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	**Темы лабораторных работ**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	**Темы курсовых работ (проектов)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	**Виды самостоятельной работы**	**Трудоемкость, *академ.час***	
		всего	**в форме**

			практической подготовки
Раздел 1.	1. Подготовка к практическому занятию; 2. Подготовка эссе; 3. Решение ситуационных задач.		
Тема 1.1.	1. Оформление отчета по этапам выполнения научного исследования; 2. Подготовка к практическому занятию.	14	
Тема 1.2.	1. Подготовка к практическому занятию; 2. Решение кейс-задач / кейсов.	14	
Тема 1.3.	1. Подготовка к практическому занятию; 2. Решение кейс-задач / кейсов.	14	
Раздел 2.	1. Оформление отчета по этапам выполнения научного исследования; 2. Подготовка к практическому занятию.		
Тема 2.1.	1. Подготовка к практическому занятию; 2. Решение кейс-задач / кейсов.	14	
Тема 2.2.	1. Подготовка к практическому занятию; 2. Решение кейс-задач / кейсов.	15	
Тема 2.3.	1. Выполнение контрольно-тренировочных упражнений; 2. Подготовка к практическому занятию.	15	
Тема 2.4.	1. Выполнение контрольно-тренировочных упражнений; 2. Подготовка к практическому занятию.	15	
Тема 2.5.	1. Подготовка к практическому занятию; 2. Решение кейс-задач / кейсов.	15	
Тема 2.6.	1. Подготовка к практическому занятию; 2. Решение кейс-задач / кейсов.	15	
Контроль	*Подготовка к экзамену*	9	
Итого:		**140**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые	**Контролируемые компетенции**	**Оценочные средства**

разделы (темы) дисциплины		
Раздел 1.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Наблюдение за работой на практическом занятии; 3. Ситуационные задачи; 4. Эссе
Тема 1.1.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Наблюдение за работой на практическом занятии
Тема 1.2.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Кейс-задачи / кейсы; 3. Наблюдение за работой на практическом занятии
Тема 1.3.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Кейс-задачи / кейсы; 3. Наблюдение за работой на практическом занятии
Раздел 2.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Наблюдение за работой на практическом занятии
Тема 2.1.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Кейс-задачи / кейсы; 3. Наблюдение за работой на практическом занятии
Тема 2.2.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Кейс-задачи / кейсы; 3. Наблюдение за работой на практическом занятии
Тема 2.3.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Контрольно-тренировочные упражнения; 3. Наблюдение за работой на практическом занятии
Тема 2.4.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Контрольно-тренировочные упражнения;

		3. Наблюдение за работой на практическом занятии
Тема 2.5.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Кейс-задачи / кейсы; 3. Наблюдение за работой на практическом занятии
Тема 2.6.	ОПК-2; ОПК-3	1. Вопросы для собеседования при защите отчета о практической работе; 2. Кейс-задачи / кейсы; 3. Наблюдение за работой на практическом занятии
Экзамен.	ОПК-2; ОПК-3	1. Вопросы к экзамену

11 Входной контроль

11.1 Цель входного контроля − определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания обучающегося используются как начальные значения в индивидуальном профиле академической успешности обучающегося.

11.2 Описание оценочных средств

Форма проведения входного контроля – тестирование.

Длительность тестирования – 30 минут.

Тестирование проводится в течение первых двух недель изучения учебной дисциплины в СУО «Moodle».

Для проведения тестирования используются тестовые задания для входного контроля (для ответа на 1 вопрос, как правило, выделяется 1 минута).

Шкала оценивания результатов тестирования

За каждый правильный ответ выставляется 1 балл. Максимальное количество – 20 баллов.

Оценка формируется в соответствии с критериями таблицы:

Процент результативности (правильных ответов)	Оценка
86 до 100	«отлично»
от 67до 85	«хорошо»
от 50 до 66	«удовлетворительно»
менее 50	«неудовлетворительно»

Основываясь на результатах тестирования, формируется индивидуальная траектория обучающегося (группы обучающихся), исходя из следующих соображений:

– 86 – 100 % – обучающийся готов к изучению учебной дисциплины без дополнительного повторения изученного ранее материала;

– 50 – 67 % – обучающийся в целом готов к изучению учебной дисциплины, требуется повторение отдельных вопросов(тем) изученного ранее материала, необходимого для успешного освоения учебной дисциплины;

– 49% и менее – обучающийся имеет слабую подготовку к изучению учебной дисциплины, необходимы корректирующие занятия и консультации.

Тестовые задания для входного контроля знаний обучающихся приведены в приложении.

12 Текущий контроль

12.1 Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению учебной дисциплины и позволяет оценить степень освоения изученного материала.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы по индивидуальной инициативе педагогического работника, в том числе посредством использования СУО «Moodle».

Формы проведения текущего контроля – вопросы для собеседования при защите отчета о практической работе; кейс-задачи / кейсы; контрольно-тренировочные упражнения; наблюдение за работой на практическом занятии; ситуационные задачи; эссе.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию решения ситуационных задач

Критерии оценки	Баллы
Умение анализировать ситуацию и находить оптимальное количество решений.	0,5
Умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для уточнения ситуации.	0,5
Умение моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат.	0,5
Умение принять правильное решение на основе анализа ситуации.	0,5
Умение четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения.	0,5
Умение критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.	0,5
Адекватность и соответствие ответов обучающегося современным тенденциям рынка, конструктивность.	0,5
Креативность, нестандартность предлагаемых решений.	0,5

Критерии оценки	Баллы
Количество альтернативных вариантов решения задачи (версионность мышления).	0,5
Наличие необходимых умений, их выраженность (в зависимости от требований).	0,5

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

12.2.2 Рекомендации по оцениванию эссе

Эссе – это самостоятельная письменная работа. Цель написания эссе состоит в развитии умений самостоятельного творческого подхода к пониманию и осмыслению проблем научного знания, возможности его прикладного использования, а также умений письменного изложения собственных мыслей и отношения к различным явлениям.

Наименование критерия оценки эссе	Всего баллов по критерию	Детализация оценивания
1 Полнота раскрытия темы и проблематика	до 15	1.1 Соответствие теме – **до 5**. 1.2 Выделена ключевая проблема – **до 5**. 1.3 Наличие творческого подхода к изложению материала – **до 5**.
2 Широта эрудиции, знания в исследуемой области	до 10	2.1 Использованы термины и определения, соответствующие интерпретации проблемы – **до 5**, в т.ч.: верно указаны все термины и определения по теме – 5, смысл терминов и определений передан не совсем точно – 3; термины и определения даны принципиально неверно – 0. 2.2 Приведены соответствующие теме и проблеме примеры – **до 5**: из обыденного опыта – 1, из учебной литературы – 2, из научных исследований – до 5.
3 Информи-рованность, знание последних событий в стране и в мире	до 5	3.1 Автор рассматривает последние события в стране и в мире: только как указание актуальности – 1, для раскрытия содержания проблемы – **до 3.** 3.2 Автор приводит оценки последним событиям в стране и в мире с точки зрения разных теоретических позиций, разных выделенных им аспектов проблемы – **до 2**.
4 Логичность и связность изложения, грамотность	до 10	4.1 Грамотный письменный язык – **до 2.** 4.2 Выделены основные структурные элементы эссе (введение с обоснованием постановки проблемы и актуальности; раскрытие содержания проблемы, варианты решений; выводы автора) – **до 5**. 4.3 Непротиворечивость, последовательность посылок, суждений и выводов – **до 3**.
5 Обоснованность выводов	до 10	5.1 Выводы автора сформулированы в явном виде – **до 2**. 5.2 В выводах суммируются ранее высказанные оценки, различения, решения проблемы – **до 5**. 5.3 Выводы содержат оригинальные суждения автора – **до 3**.

Максимальная оценка за эссе – 50 баллов. В зависимости от количества набранных обучающимся баллов за эссе оценка ставится по следующей градационной сетке:

Количество набранных баллов	Оценка
43 – 50 баллов	отлично
33 – 42 баллов	хорошо
26 – 32 баллов	удовлетворительно
0 – 25 баллов	неудовлетворительно

12.2.3 Рекомендации по оцениванию в процессе наблюдения за работой на практическом занятии

Наблюдение за работой на практическом занятии – важнейший компонент контроля деятельности обучающихся и качества их обучения.

Критерии оценки в процессе наблюдения за работой на практическом занятии:

– самостоятельность выполнения задания и работы с методическими указаниями (учитывается работа в течение занятия, быстрота и способность нахождения в методических указаниях нужной информации);

– правильность выполнения работы (учитывается последовательность выполняемых действий, умение работать с инструментами и/или средствами вычислительной техники);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения работы с учетом индивидуальных особенностей обучающихся);

– активность обучающегося при выполнении практической работы (учитывается индивидуальная работа и работа в группе).

Критерии оценки по результатам наблюдения за работой на практическом занятии

Наименование параметра оценки	Максимальное количество баллов
Самостоятельно выполняет задания; умеет работать с методическими указаниями.	2,5
Указанные в методических указаниях действия выполняет в правильной последовательности; умеет работать с инструментами и/или средствами вычислительной техники.	1,25
Рационально использует время, отведенное на задание; проявляет активность при выполнении практической работы.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

12.2.4 Рекомендации по оцениванию выполнения контрольно-тренировочных упражнений

12.2.5 Рекомендации по оцениванию ответов на вопросы в процессе собеседования при защите отчета о практической работе

Подготовку к защите отчета о практической работе обучающиеся осуществляют в рамках самостоятельной работы. Вопросы для подготовки к защите отчета о практической работе представлены в методических указаниях к практическим занятиям.

Критерии оценки устных ответов на вопросы при защите отчета о практической работе:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– сознательность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– сопровождение ответа примерами (учитывается умение грамотно и с пользой применять фактический материал для подкрепления теоретического при устном ответе);

– рациональность использования времени, отведенного на ответ (не одобряется затянутость выполнения задания, устного ответа во времени, с учетом индивидуальных особенностей обучающихся).

Критерии оценки устных ответов обучающихся на вопросы при защите отчета о практической работе

Наименование параметра оценки	Максимальное количество баллов
Излагает материал последовательно и правильно; полно и аргументировано отвечает по содержанию задания.	2,5
Обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, в том числе и самостоятельно составленные.	1,25
Рационально использует время, отведенное на ответ; устный ответ не затянут во времени.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

12.2.6 Рекомендации по оцениванию решения кейс-задач

Критерии оценки	Баллы
Умение анализировать ситуацию и находить оптимальное количество решений.	0,5
Умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для уточнения ситуации.	0,5

Критерии оценки	Баллы
Умение моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат.	0,5
Умение принять правильное решение на основе анализа ситуации.	0,5
Умение четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения.	0,5
Умение критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.	0,5
Адекватность и соответствие ответов обучающегося современным тенденциям рынка, конструктивность.	0,5
Креативность, нестандартность предлагаемых решений.	0,5
Количество альтернативных вариантов решения задачи (версионность мышления).	0,5
Наличие необходимых умений, их выраженность (в зависимости от требований).	0,5

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины приведены в приложении.

13 Промежуточная аттестация

13.1 Оценочные материалы для промежуточной аттестации обучающихся по учебной дисциплине предназначены для оценки степени достижения запланированных результатов обучения по завершению изучения учебной дисциплины в установленной учебным планом форме и позволяют определить качество усвоения изученного материала.

Итоговой формой контроля сформированности компетенций у обучающихся по учебной дисциплине является: экзамен.

Оценочные материалы для промежуточной аттестации обучающихся включают: вопросы к экзамену.

13.2 Оценивание обучающегося на экзамене

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, обладает приемами выполнения практических задач по формированию компетенций.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его,

Оценка	Требования к знаниям
	не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, обладает необходимыми умениями и приемами их выполнения.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по данной учебной дисциплине.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – Москва: Издательство Юрайт, 2025. – 277 с. – URL: https://urait.ru/book/informacionnaya-bezopasnost-567672 (дата обращения: 12.05.2025);

2 Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2025. – 357 с. – URL: https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-560516 (дата обращения: 12.05.2025);

3 Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2025. – 352 с. – URL: https://urait.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-580669 (дата обращения: 12.05.2025).

б) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru. – URL: https://libr.sibsiu.ru;

2 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для авторизир. пользователей. – URL: https://library.sibsiu.ru/LibrELibraryFullText.asp;

3 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, [200 –]. – URL: http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

4 ЛАНЬ : электронно-библиотечная система : [коллекция «Единая профессиональная база знаний для технических вузов - Издательство Лань" ЭБС»] / ООО «Издательство ЛАНЬ». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

5 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

6 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: https://biblioclub.ru. – Режим доступа: для авторизир. пользователей. – URL: http://www.biblioclub.ru;

7 Электронная библиотека УМЦ ЖДТ : [коллекция «Эксплуатация железных дорог»] / ФГБУ ДПО «Учебно-методический центр по образованию на железнодорожном транспорте». – Москва, [2013 –]. – URL: https://umczdt.ru/books/. – Режим доступа: для авторизир. пользователей;

8 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

9 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: http://eivis.ru. – Режим доступа: по подписке.

в) лицензионное и свободно распространяемое программное обеспечение:

– 7-Zip;
– Adobe Acrobat Reader;
– Astra Linux Special Edition;
– Kaspersky Endpoint Security;
– Microsoft Office;
– Microsoft Windows;
– OnlyOffice;
– Р7-Офис.

г) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

15 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории, оснащенные оборудованием, компьютерной техникой, и техническими средствами обучения, в том числе:
- учебную аудиторию для проведения занятий лекционного типа, оборудованную учебной доской, экраном и мультимедийным проектором;
- учебную аудиторию для проведения занятий семинарского типа (практических занятий), оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, научно-техническую библиотеку СибГИУ;
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, научно-техническую библиотеку СибГИУ.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Составитель(и):

ассистент Орлова Ирина Сергеевна (кафедра автоматизации и информационных систем).

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии».

Согласована:
Начальник РЦС С
/ начальник Регионального центра
сопровождения Сибирь
ООО «ЕвразТехника ИС»  Е. В. Кириенко

Приложение

Тестовые задания для входного контроля знаний обучающихся

Выберите один правильный ответ.

1 Наиболее распространенной на практике моделью данных является:

а) иерархическая;

б) сетевая;

в) графовая;

г) реляционная.

2 К распространенным сетевым топологиям локальных сетей относится:

а) шинная топология;

б) иерархическая звезда;

в) кольцо;

г) многогранник.

3 Для работы с реляционной СУБД используются технологии:

а) SIEQUEL;

б) SQL;

в) ASM;

г) DSL.

4 Наиболее распространенной технологией обработки информации в распределенных сетях является:

а) файл – поток;

б) файл – сервер;

в) клиент – сервер;

г) модель – представление.

1. К иерархическим моделям хранения информации можно отнести:

а) формат html;

б) формат xmms;

в) формат xml;

г) формат gdb.

2. К устройствам передачи данных канального уровня относятся:

а) концентратор;

б) коммутатор;

в) маршрутизатор;

г) мост.

3. К устройствам передачи данных сетевого уровня относятся:

а) концентратор;

б) коммутатор;

в) маршрутизатор;

г) мост.

4. Модель взаимодействия открытых систем ISO OSI использует следующее количество уровней:

а) 4;

б) 5;

в) 6;
г) 7;
д) 9.

5. Для передачи гипертекстовых данных в сети Internet применяется протокол:

а) rmi;
б) dmi;
в) http;
г) vrml;
д) ftp.

6. Для выборки отдельных записей из таблицы базы данных используется оператор:

а) invoke;
б) select;
в) call;
г) open.

7. Уникальный идентификатор отдельного узла в сети Internet задается:

а) ip-адресом;
б) ip-адресом и маской подсети;
в) аппаратным MAC адресом;
г) уникальным vlan адресом.

8. Перенаправление трафика между сетями:

а) является задачей коммутации;
б) является задачей трансформации;
в) является задачей маршрутизации;
г) является задачей переадресации.

9. Объединение нескольких каналов передачи данных в один:

а) коммутирование;
б) мультиплексирование;
в) комбинирование;
г) форсирование.

10. Цифровой сигнал основан на использовании:

а) непрерывного сигнала;
б) использует 4 уровня сигнала;
в) использует 3 уровня сигнала;
г) использует 2 уровня сигнала.

11. К протоколам передачи данных транспортного уровня можно отнести:

а) smtp;
б) pop3;
в) imap;
г) udp.

12. Для динамического распределения ip-адресов в сети Internet используется протокол:

а) wins;
б) dns;
в) dhcp;

13. В чем заключается преимущество цифрового сигнала над аналоговым:

а) более высокая помехозащищенность;
б) более высокое быстродействие;
в) надежность кодирования информации;
г) точность представления данных.

14. Каковы функции канального уровня передачи данных:

а) привязка к аппаратному адресу физической передающей среды;
б) логическая адресация узлов в сети;
в) маршрутизация;
г) динамическая адаптация.

15. Какие задачи решает протокол ftp:

а) динамическая адресация;
б) передача файлов;
в) маршрутизация почты;
г) доставка почты.

16. Назовите типовые задачи информационной сети:

а) хранение и обработка данных;
б) хранение и передача данных;
в) перенаправление трафика между промежуточными узлами.

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины

Тема 1.1 Термины и определения.

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1 Дайте определение понятию информационная безопасность.
2 Что такое конфиденциальность данных.
3 Что такое целостность данных.
4 Чем отличается понятие целостности и конфиденциальности данных.
5 Что подразумевается под доступностью данных?
6 Какая информационная система является уязвимой.
7 Приведите примеры уязвимостей операционных систем.

8 Что подразумевается под термином «атака информационной системы».

9 Каковы причины возникновения инцидентов информационной безопасности.

10. Поясните основные понятия и определения информационной безопасности.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 1.2. Типовые проблемы безопасности

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

1 Дайте определение понятию «уязвимость информационной системы»

2 Дайте определение понятию «атака информационной системы».

3 Приведите пример классификации типовых уязвимостей информационных систем.

4 Что такое типовая уязвимость информационной системы.

5 Phishing – атаки на ИТ-системы. Приведите примеры.

6 Poisoning – атаки. Приведите примеры.

7 Spoofing – атаки. Приведите примеры.

8 Атаки отказа в обслуживании и распределенного отказа в обслуживании.

9 Атаки на протокол arp. Arp spoofing, arp poisoning.

10. Атаки на протокол ip. Ip spoofing, ip poisoning.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 1.3. Безопасность программного обеспечения

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

17. Что такое безопасность программного обеспечения. Поясните.

18. Проблемы безопасности программного обеспечения. Поясните.

19. Каковы типовые проблемы безопасности программного обеспечения. Из-за чего они возникают?

20. Атаки на стек. Атаки срыва стека. Поясните суть.

21. Атаки на буфер. Переполнение буфера. Поясните суть.

22. Атаки внедрением кода. Приведите примеры.

23. Атаки на SQL – сценарии. SQL-injection. Приведите примеры.
24. Атаки reverse – engeneering. Приведите примеры.
3 Инструментарий обнаружения уязвимостей ПО.
4 Инструменты SoftIce, OllyDbg.
10. Механизмы защиты программного обеспечения.
10 Механизмы противодействия атакам на программное обеспечение.
11 Механизмы защиты исходного кода.
12 Упаковщики и обфускаторы исходного кода.
13 Принципы безопасного программирования.
14 Принципы защиты программного обеспечения.
15 Защита данных.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 2.1. Введение в криптографию

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

10 История криптографии.
11 Защита Цезаря.
12 Понятие логической защиты. Поясните отличие логических и криптозащит.
13 Логические защиты. Многоалфавитная замена. Поясните идею.
14 Логические защиты. Таблицы подстановок, перестановок. Поясните идею.
15 Разработайте и приведите пример логической защиты.
16 Криптозащиты.
17 Защиты Кирхгофа.
18 Недостатки логических защит.
19 Практическая применимость логических защит.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 2.2. Симметричная криптография

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

25. Общая идея симметричного алгоритма. Закрытый ключ.
26. Придумайте симметричный алгоритм, использующий закрытый ключ.

27. Понятия закрытого ключа, вектора инициализации. Приведите примеры алгоритмов, использующих вектор инициализации.

28. Опишите понятие «раунд шифрования». Приведите примеры вычислений, использующих или не использующих раунды шифрование. Что такое развертывание ключа?

29. В чем заключается идея схемы Фейстеля?

30. Как функционирует криптозащита на основе сети Фейстеля.

31. Стандарт DES. Опишите в общих чертах принцип действия.

32. Стандарт Triple Des. Опишите стандарт в общих чертах.

33. Алгоритм Idea Филиппа Циммермана.

34. Алгоритм Rijndael. Преимущества схемы Rijndael.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 2.3. Односторонние хэш функции

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

5 Задача определения контрольной суммы. Приведите примеры.

6 Задача хэширования данных. Приведите примеры.

7 Задача аутентификации и авторизации. Приведите примеры.

8 Суть алгоритмов одностороннего хэширования.

9 Смысл алгоритмов одностороннего хэширования.

10 Алгоритм MD5. Поясните принцип действия.

11 Алгоритм SHA1. Поясните принцип действия.

12 Атаки на односторонние хэш - функции. Поясните в общих чертах принцип действия.

13 Принципы взлома односторонних хэш функций.

14 Недостатки односторонних – хэш функций.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 2.4. Асимметричная криптография

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

16 Общая идея асимметричной криптографии.

17 Системы с секретом. Сложность вычислений секрета.

18 Понятие вычислительной сложности алгоритма.

19 Схема Клиффорда Кокса.

20 Смысл преобразований Клиффорда Кокса.

21 Схема Диффи-Хеллмана.

22 Протокол Диффи-Хеллмана.

23 Алгоритм RSA. Принцип генерации ключевой пары в RSA.

24 Принцип открытого шифрования RSA. Приведите примеры.

25 Недостатки практического использования современных реализаций RSA.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 2.5. Электронная цифровая подпись

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

20 Проблемы электронной цифровой подписи.

21 Почему системы с электронной цифровой подписью не работают.

22 Использование RSA в схемах с цифровой подписью. Поясните.

23 Схемы без посредника в механизмах с ЭЦП. Поясните.

24 Схемы с посредником в механизмах с ЭЦП. Поясните.

25 Стандарт DSS.

26 Применение стандарта электронной цифровой подписи в современных платежных системах. Расскажите.

27 Поясните работу асимметричной схемы на примере ЭЦП.

28 Расскажите в чем на ваш взгляд, заключаются недостатки ЭЦП.

29 Недостатки практического использования современных реализаций ЭЦП.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

Тема 2.6. Аутентификация и авторизация

1 Устный опрос на лекции

Перечень вопросов для устного опроса:

35. Отличие аутентификации и авторизации.
36. Подходы к аутентификации.
37. Механизмы аутентификации.
38. Парольные защиты. Принципы парольных защит.
39. Поясните основные этапы реализации механизмов аутентификации.

2 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

3 Тестирование по результатам освоения лекционного материала и самостоятельной работы

Тестирование проводится для определения степени усвоения материалов лекций, а также выполнения самостоятельной работы в рамках часов, отведенных на самостоятельную работу обучающихся, в СУО «Moodle».

Примерный перечень вопросов для тестирования:

15 Преобразование открытого текста сообщения в закрытый называется:

- процедура шифрования;
- алгоритм шифрования;
- обеспечение аутентификации;
- цифровая запись.

16 Входные параметры процесса шифрования (несколько верных ответов):

- зашифрованный текст;
- ключ;
- открытый текст;
- алгоритм.

17 Какие из сервисов реализуются при использовании криптографических преобразований (несколько верных ответов):

- контроль целостности;
- аутентификация;
- шифрование;
- алгоритм.

18 Что позволяет предотвратить использование криптографических преобразований:

- отказ от информации;
- обеспечение аутентификации;
- утечку информации;
- использование алгоритмов асимметричного шифрования.

19 Знание ключа позволяет:

- использовать криптографические сервисы безопасности;
- обеспечить аутентификацию;
- предотвратить утечку информации;
- выполнить обратное преобразование.

20 Что в криптографии понимается под термином «элементарное опробование»:

- операция над двумя разрядными двоичными числами;
- проверка ключа на целостность;
- сопоставление двух паролей;

- передача ключа по какому-либо каналу связи.

21 Чем определяется уровень надежности применяемых криптографических преобразований:

- значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;
- сложностью комбинации символов, выбранных случайным образом;
- использованием большого числа ключей для шифрования;
- отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

22 Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:

- идентификация и аутентификация пользователей и субъектов доступа;
- управление доступом;
- обеспечение постоянного числа пользователей сети;
- обеспечения целостности;
- регистрация и учет.

23 Что называется имитовставкой:

- это блок данных, переменной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты;
- это блок данных фиксированной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты.

24 Как иначе называется симметричное шифрование:

- шифрование с закрытым ключом;
- шифрование методом Бейтса;
- шифрование с открытым ключом;
- шифрование с переменным ключом.

25 Какой алгоритм не используется при симметричном шифровании:

26 поточное шифрование;

27 побитовое шифрование;

28 блочное шифрование;

29 алгоритм Эль-Гамаля.

26 Какой из режимов алгоритма DES используется для построения шифров гаммирования?

- электронная кодовая книга;
- сцепление блоков шифра;
- обратная связь по шифротексту;

- обратная связь по выходу.

27 Какова длина блока алгоритма шифрования DES:

- 16 бит;
- 56 бит;
- 64 бита;
- 5 байт.

28 Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:

- Ю;
- 14;
- 16;
- 20.

29 Что является преимуществом симметричного шифрования:

- скорость выполнения криптографических преобразований;
- легкость внесения изменений в алгоритм шифрования;
- секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
- применение в системах аутентификации (электронная подпись).

30 Какой размер ключа в отечественном стандарте симметричного шифрования:

- 56 бит;
- 124 бит;
- 256 бит.

31 Какие из режимов шифрования данных не включает в себя отечественный стандарт симметричного шифрования:

- режим гаммирования;
- режим простой замены;
- режим обратной связи по шифротексту;
- режим гаммирования с обратной связью.

32 Использует ли отечественный стандарт симметричного шифрования дополнительный ключ:

- да;
- нет.

33 Какое из этих утверждений является верным:

- у S-блоков ГОСТ 4-битовые входы и выходы;
- у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы;
- у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы.

34 Используется ли в отечественном стандарте симметричного шифрования процедура генерации подключей из ключей, как в DES:

- да, но эта процедура сравнительно проста;
- не используется;
- используется аналогичная по сложности процедура.

4 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

5 Вопросы к экзамену для промежуточной аттестации

30 Общая идея симметричного алгоритма. Закрытый ключ.

31 Придумайте симметричный алгоритм, использующий закрытый ключ.

32 Понятия закрытого ключа, вектора инициализации. Приведите примеры алгоритмов, использующих вектор инициализации.

33 Опишите понятие «раунд шифрования». Приведите примеры вычислений, использующих или не использующих раунды шифрование. Что такое развертывание ключа?

34 В чем заключается идея схемы Фейстеля?

35 Как функционирует криптозащита на основе сети Фейстеля.

36 Стандарт DES. Опишите в общих чертах принцип действия.

37 Стандарт Triple Des. Опишите стандарт в общих чертах.

38 Алгоритм Idea Филиппа Циммермана.

39 Алгоритм Rijndael. Преимущества схемы Rijndael.

40 Задача определения контрольной суммы. Приведите примеры.

41 Задача хэширования данных. Приведите примеры.

42 Задача аутентификации и авторизации. Приведите примеры.

43 Суть алгоритмов одностороннего хэширования.

44 Смысл алгоритмов одностороннего хэширования.

45 Алгоритм MD5. Поясните принцип действия.

46 Алгоритм SHA1. Поясните принцип действия.

47 Атаки на односторонние хэш - функции. Поясните в общих чертах принцип действия.

48 Принципы взлома односторонних хэш функций.

49 Недостатки односторонних – хэш функций.

50 Общая идея асимметричной криптографии.

51 Системы с секретом. Сложность вычислений секрета.

52 Понятие вычислительной сложности алгоритма.

53 Схема Клиффорда Кокса.

54 Смысл преобразований Клиффорда Кокса.

55 Схема Диффи-Хеллмана.

56 Протокол Диффи-Хеллмана.

57 Алгоритм RSA. Принцип генерации ключевой пары в RSA.

58 Принцип открытого шифрования RSA. Приведите примеры.

59 Недостатки практического использования современных реализаций RSA.

60 История криптографии.

61 Защита Цезаря.

62 Понятие логической защиты. Поясните отличие логических и криптозащит.

63 Логические защиты. Многоалфавитная замена. Поясните идею.

64 Логические защиты. Таблицы подстановок, перестановок. Поясните идею.

65 Разработайте и приведите пример логической защиты.

66 Криптозащиты.

67 Защиты Кирхгофа.

68 Недостатки логических защит.

69 Практическая применимость логических защит.