Министерство науки и высшего образования Российской Федерации

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

Кафедра прикладных информационных технологий и программирования

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптография, криптоанализ и защита информации

01.03.02 «Прикладная математика и информатика»
(направленность (профиль): «Математическое моделирование и интеллектуальный анализ данных»)

Квалификация выпускника
Бакалавр

Форма обучения
Очная форма

Срок обучения: 4 года

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: 30-04-2025 09:43:19 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний в области криптографии, криптоанализа и основ информационной безопасности, а также навыков практической защиты информации в организациях.

Задачами учебной дисциплины являются:

– обеспечить знание обучающимися методов и средств криптографии и криптоанализа;
– выработать у обучающихся навыки работы с современными техническими и программно-аппаратными средствами защиты информации;
– научить обучающихся практически решать задачи защиты данных, программ и компьютерных систем.

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) 01.03.02 «Прикладная математика и информатика».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Базы данных;
– Информатика;
– Программирование;
– Архитектура вычислительных систем;
– Операционные системы;
– Инфокоммуникационные системы и сети;
– Проектная деятельность 1.

Учебная дисциплина дополняет знания и умения, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Проектная деятельность 2;
– Преддипломная практика.

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

Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1 Понимает принципы работы современных информационных технологий	– знать: основы защиты информации в современных информационных технологиях. – уметь: защищать информационные ресурсы и использованием разных сервисов и механизмов информационной безопасности.
		ОПК-4.3 Применяет современные информационные технологии и программные средства при решении прикладных задач	– знать: основы архитектуры компьютерных сетей. – уметь: использовать технические и программные средства для эшелонированной защиты компьютерной сети.

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

Семестр / курс		***ИТОГО***	***7 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость	*академ. час.*	***144***	*144*
	зачетных единиц	***4***	*4*
Лекции, *академ. час.*		***32***	*32*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***32***	*32*

в форме практической подготовки	***0***	*0*
Курсовая работа / проект, *академ. час.*	***0***	*0*
в форме практической подготовки	***0***	*0*
Консультации, *академ. час.*	***0***	*0*
в форме практической подготовки	***0***	*0*
Самостоятельная работа, *академ. час.*	***44***	*44*
в форме практической подготовки	***0***	*0*
Контроль, *академ. час.*	***36***	*36*
в форме практической подготовки	***0***	*0*

Содержание учебной дисциплины

Раздел 1 Базовые понятия информационной безопасности и защиты информационных систем;

Тема 1.1 Понятие информационной безопасности (определение информационной безопасности, основные составляющие информационной безопасности);

Тема 1.2 Основные угрозы информационной безопасности (основные определения и критерии классификации угроз, вредоносное программное обеспечение, каналы утечки информации);

Раздел 2 Криптография и криптоанализ;

Тема 2.1 Криптографические шифры (аутентичность сообщений, составные элементы шифра, классификация шифров);

Тема 2.2 Криптография с открытым ключом (симметричные и асимметричные шифры, управление криптографическими ключами, алгоритмы асимметричного шифрования);

Тема 2.3 Криптографические протоколы (основные понятия, разновидности протоколов, протоколы обмена ключами);

Тема 2.4 Криптоанализ (основные понятия, классификация криптоатак, методы криптоанализа);

Тема 2.5 Стеганография и защита программного кода (суть и цели стеганографии, направления использования, методы стеганографии, методы защиты программного кода);

Раздел 3 Сервисы безопасности;

Тема 3.1 Оценочные стандарты информационной безопасности (классификация стандартов, «Оранжевая книга», «Рекомендации X.800», стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»);

Тема 3.2 Уровни информационной безопасности (административный уровень, процедурный уровень, программно-технический уровень информационной безопасности);

Тема 3.3 Идентификация и аутентификация (основные понятия, виды идентификации, парольная и биометрическая аутентификация);

Тема 3.4 Управление доступом (логическое управление доступом, методы управления доступом, ролевое управление доступом, управление доступом в Java-среде);

Тема 3.5 Контроль целостности (функция хэширования, электронная цифровая подпись, протоколы контроля целостности);

Тема 3.6 Экранирование и туннелирование (основы экранирования, архитектурная безопасность, межсетевые экраны).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Базовые понятия информационной безопасности и защиты информационных систем		
Тема 1.1.	Понятие информационной безопасности	2	
Тема 1.2.	Основные угрозы информационной безопасности	2	
Раздел 2.	Криптография и криптоанализ		
Тема 2.1.	Криптографические шифры	4	
Тема 2.2.	Криптография с открытым ключом	2	
Тема 2.3.	Криптографические протоколы	2	
Тема 2.4.	Криптоанализ	4	
Тема 2.5.	Стеганография и защита программного кода	2	
Раздел 3.	Сервисы безопасности		
Тема 3.1.	Оценочные стандарты информационной безопасности	2	
Тема 3.2.	Уровни информационной безопасности	2	
Тема 3.3.	Идентификация и аутентификация	2	
Тема 3.4.	Управление доступом	4	
Тема 3.5.	Контроль целостности	2	
Тема 3.6.	Экранирование и туннелирование	2	
Итого:		**32**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**

Раздел 1.	Организация технической защиты персональных данных	2	
Раздел 1.	Стандартные средства защиты персонального компьютера	4	
Раздел 1.	Защита документов офисного пакета	2	
Раздел 2.	Криптография. Шифры замены и перестановки	6	
Раздел 2.	Криптоанализ шифров замены и перестановки	8	
Раздел 3.	Построение инфраструктуры защищённых компьютерных сетей	10	
Итого:		**32**	**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. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	14	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию;	15	

	3. Прохождение тестирования.		
Раздел 3.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	15	
Контроль	*Подготовка к экзамену*	36	
Итого:		**80**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые разделы (темы) дисциплины	Контролируемые компетенции	Оценочные средства
Раздел 1.	ОПК-4	1. Наблюдение за работой на практическом занятии; 2. Тестовые задания
Раздел 2.	ОПК-4	1. Наблюдение за работой на практическом занятии; 2. Тестовые задания
Раздел 3.	ОПК-4	1. Наблюдение за работой на практическом занятии; 2. Тестовые задания
Экзамен.	ОПК-4	1. Экзамен на основе результатов текущего контроля

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 – индивидуальный или фронтальный устный опрос. В ходе проведения входного контроля обучающимся предлагается ответить на вопросы по материалу, изученному в процессе освоения ООП ВО.

Шкала оценивания устных ответов обучающихся

Критерии оценки:

– 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).

Оценку «зачтено» получает обучающийся, если он при собеседовании обнаруживает знание и понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, в том числе и самостоятельно составленные; при ответе на вопросы излагает материал последовательно и правильно, полно и аргументировано отвечает по содержанию задания; рационально использует время, отведенное на ответ.

Оценку «не зачтено» получает обучающийся, который не рационально использует время, отведенное на ответ; обнаруживает незнание ответа на соответствующий вопрос; допускает ошибки в формулировке определений и правил, искажающие их смысл; беспорядочно и неуверенно излагает материал. Оценка «не зачтено» отмечает такие недостатки в подготовке обучающегося, которые требуют проведения дополнительных индивидуальных консультаций.

Вопросы 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 – наблюдение за работой на практическом занятии; тестовые задания.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию результатов тестирования обучающихся

Тестирование проводится по изученным разделам (темам) учебной дисциплины для выявления уровня знаний и умений обучающегося, мотивирования обучающегося к активизации самостоятельной работы по усвоению учебного материала, выявления и устранения пробелов в знаниях, повышения дисциплины и организации учебной деятельности обучающегося.

Тестирование проводится в СУО «Moodle» в рамках часов, отведенных на самостоятельную работу обучающихся. Для тестирования используется 20 вопросов из базы типовых тестовых заданий по изученным разделам (темам) учебной дисциплины. Обучающийся выбирает один ответ из предложенных вариантов ответа. В случае выбора неправильного ответа обучающийся получает за данный вопрос 0 баллов; в случае правильного ответа – 1 балл.

Оценка формируется в соответствии с критериями таблицы:

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он ответил правильно на 80% - 100%тестовых заданий.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он ответил правильно на 70% - 79% тестовых заданий.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он ответил правильно на 60% - 69 %тестовых заданий.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, если он ответил правильно менее чем на 60% тестовых заданий.

12.2.2 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».

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: экзамен на основе результатов текущего контроля.

13.2 Оценивание обучающегося на экзамене

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он получил среднюю оценку «отлично» по 3-м результатам тестирования в период текущих аттестаций в семестре, выполнил правильно и полно все практические задания и самостоятельную работу.

Оценка	Требования к знаниям
хорошо	Оценка «хорошо» выставляется обучающемуся, если он получил среднюю оценку «хорошо» по 3-м результатам тестирования в период текущих аттестаций в семестре, выполнил правильно и полно все практические задания.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он получил среднюю оценку «удовлетворительно» по 3-м результатам тестирования в период текущих аттестаций в семестре, выполнил правильно и полно все практические задания практические задания и самостоятельную работу.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, если он получил оценку «неудовлетворительно» хотя бы по 1-му результату тестирования в период текущих аттестаций в семестре и не выполнил все практические задания практические задания и самостоятельную работу.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. – URL: https://urait.ru/bcode/536902 (дата обращения: 24.04.2025);

2 Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — ISBN 978-5-534-02574-3. – URL: https://urait.ru/bcode/536453 (дата обращения: 24.04.2025);

3 Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. – URL: https://urait.ru/bcode/537247 (дата обращения: 24.04.2025);

4 Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. – URL: https://urait.ru/bcode/544029 (дата обращения: 24.04.2025).

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

8 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:

– Astra Linux Special Edition;
– LibreOffice;
– Microsoft Office;
– Microsoft Windows;
– VirtualBox;
– 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), оснащенную компьютерной техникой и периферийным оборудованием;
- 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) 01.03.02 «Прикладная математика и информатика».

Составитель(и):

доцент Пермякова Елена Павловна (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Согласован:

Генеральный директор

ООО «Агит-плюс» Рыжих А.Ю.

Приложение

Вопросы для входного контроля знаний обучающихся

1. Что такое многосвязный интерфейс?
2. Что называется каналом связи?
3. Как называется путь, соединяющий два смежных узла сети?
4. Какая из перечисленных топологий в основном применяется в глобальных сетях?
5. Какой тип сетевого кабеля является наиболее помехозащищённым?
6. Какой тип интерфейса использует операционная система Windows?
7. Из каких частей состоит диалог между пользователем и приложением?
8. Какие составляющие включает пользовательский интерфейс?

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

1 Тестовые задания

Раздел 1 Базовые понятия информационной безопасности и защиты информационных систем

1. Какая из категорий является важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию»?

а) конфиденциальность

б) доступность
в) целостность
2. Следствием чего в большинстве случаев является угроза?

а) следствием наличия уязвимых мест
б) следствием наличия злоумышленников
в) следствием наличия окон опасности
г) следствием наличия источников угроз

3. Какие из вредоносных программ способны самостоятельно распространять свои копии?

а) вирусы
б) черви
в) спам
г) рекламные программы
д) программы дозвона

4. Для чего обычно предназначена «логическая бомба»?

а) для удаления вредоносного ПО из системы
б) для внедрения вредоносной программы
в) для контроля над атакуемой системой
г) для агрессивного потребления ресурсов
д) для предотвращения заражения компьютера вредоносным ПО

5. Мероприятия по защите чего вы будете разрабатывать при переупорядочении, краже, дублировании данных, возникших в вашей системе?

а) динамической целостности
б) статической целостности
в) прямой доступности
г) структурной целостности
д) достоверности данных

6. При защите чего вы примените помехоподавляющие фильтры?

а) сетей питания и каналов связи для безопасности передаваемых сигналов
б) персональных компьютеров для безопасности персональных ресурсов
в) корпоративных компьютеров для безопасности корпоративной информации

7. В вашей системе зафиксировано выполнение действий под видом лица, обладающего полномочиями, для доступа к данным? Вы предпримите ответные действия как на:

а) маскарад
б) злоупотребление полномочиями
в) подмену ролей
г) фальсификацию

Раздел 2 Криптография и криптоанализ

1. Какие виды ключей применяются в асимметричных методах шифрования?

а) секретный ключ для шифрования
б) секретный ключ для расшифрования
в) не секретный ключ для шифрования
г) не секретный ключ для расшифрования

2. В каких методах шифрования используется два ключа?

а) в асимметричных
б) в симметричных
в) во всех

3. Выберите существенный недостаток асимметричных методов шифрования.

а) низкое быстродействие
б) ненадёжность
в) большая сложность
г) большое количество ошибок
д) неустойчивость к взлому шифра

4. Что такое «составной ключ»?

а) секретный ключ, разделённый на 2 части, которые хранятся отдельно
б) ключ, состоящий из секретной и несекретной частей
в) ключ, разделённый на части, которые хранятся совместно, но используются раздельно

5. Чем ограничены таблицы Виженера по строкам и столбцам?

а) ничем, они могут любого размера

б) количеством символов используемого алфавита
в) количеством символов исходного текста

6. Выберите правильное расположение букв ключа и исходного слова при использовании таблицы Виженера.

а) буквы ключа расположены в верхней строке таблицы, буквы открытого текста – в первом столбце таблицы
б) буквы ключа расположены в первом столбце таблицы, буквы открытого текста – в верхней строке таблицы
в) буквы ключа и открытого текста расположены в верхней строке таблицы
г) буквы ключа и открытого текста расположены в первом столбце таблицы

7. На каком наблюдении основан тест Казиски, используемый при криптоанализе шифра Виженера?

а) два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном длине ключевого слова, будут по-разному зашифрованы
б) два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном длине ключевого слова, будут одинаково зашифрованы
в) два разных отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном длине ключевого слова, будут одинаково зашифрованы
г) два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, равном длине ключевого слова, будут одинаково зашифрованы

8. Что при криптоанализе шифра Виженера позволяет определить индекс совпадений?

а) длину ключевого слова
б) ключевое слово
в) расшифрованный текст

9. Вам необходимо придумать «составной ключ» для шифрования сообщений. Вы сделаете:

а) секретный ключ, разделённый на две части, которые хранятся отдельно
б) ключ, состоящий из секретной и несекретной частей, которые хранятся отдельно

в) не секретный ключ, разделённый на несколько частей, которые хранятся отдельно

Раздел 3 Сервисы безопасности

1. К какому уровню безопасности относится управление персоналом?

а) к административному
б) к процедурному
в) к программно-техническому

2. В группу каких сервисов попадает большинство сервисов безопасности?

а) локализующие
б) превентивные
в) меры обнаружения нарушений
г) меры по выявлению нарушителя

3. Словосочетание «проверка подлинности» используется как синоним?

а) идентификации
б) аутентификации
в) псевдонимности
г) аудита

4. Какой из видов аутентификации является самым слабым средством проверки подлинности?

а) биометрическая аутентификация
б) парольная аутентификация
в) SMS-аутентификация
г) аутентификация по электронной подписи

5. Почему за приемлемое время специально организовать так называемую «коллизию» при хэшировании невозможно?

а) потому что хэш-функция – односторонняя
б) потому что хэш-функция – двусторонняя
в) потому что хэш-функция – обратимая

6. Вы – администратор сети. Как при ролевом управлении доступом вы определите роль пользователя в системе?

а) в соответствии с технической структурой организации
б) в соответствии с функциональной структурой организации
в) в соответствии с организационной структурой организации

7. Выберите, что как системный администратор вы должны осуществлять в рамках такого направления поддержания работоспособности, как «поддержка программного обеспечения»?

а) контроль за тем, какое программное обеспечение установлено
б) контроль за изменениями, вносимыми в программную конфигурацию
в) контроль за физическими носителями информации (флэшками, HDD-дисками и др.)
г) контроль за отсутствием неавторизованного изменения программ и прав доступа к ним

8. При каком виде деятельности по поддержанию работоспособности сотрудник получает исключительный доступ к системе, и на практике очень трудно контролировать, какие действия он совершает?

а) управление носителями
б) регламентные работы
в) конфигурационное управление
г) документирование
д) резервное копирование

9. Согласно какому принципу вы как администратор ИС будете следовать при распределении роле и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс?

а) принципу минимизации привилегий
б) принципу разделения обязанностей
в) принципу максимизации ответственности
г) всем перечисленным принципам

2 Выполнение практических работ

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

Примеры заданий на практические работы.

Раздел 1 Базовые понятия информационной безопасности и защиты информационных систем

1. Определить сертифицированные средства защиты персональных данных (ПДн) для заданных субъектов ПДн и типов информационных систем.
2. Практически изучить стандартные средства защиты персонального компьютера.
3. Практически изучить средства защиты документов офисного пакета.

Раздел 2 Криптография и криптоанализ

1. Зашифруйте исходное сообщение методами: перестановки, перестановки по ключу, двойной перестановки, «магического квадрата», Цезаря, Трисемуса и Виженера.
2. Сделайте криптоанализ шифротекстов, полученных методами: перестановки, двойной перестановки, «магического квадрата».
3. Сделайте частотный анализ шифротекста.
4. Сделайте криптоанализ шифров Виженера без заданного ключа.

Раздел 3 Сервисы безопасности

1. Сэмулируйте компьютерную сеть.
2. Произведите настройку DHCP-сервера.
3. Произведите объединение двух сетей.
4. Произведите настройку Web-сервера.
5. Изучите технологии виртуальных локальных сетей VLAN.
6. Произведите настройку NAT и RIP протокола.

3. Оценивание обучающегося на экзамене

Промежуточная аттестация производится на основе текущего контроля успеваемости при условии выполнения всех заданий в семестре, предусмотренных фондом оценочных средств по дисциплине.