

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»

Проректор по учебной работе

« 30 » 03

2022

Г.Ю. Нагорная



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Уровень образовательной программы бакалавриат

Направление подготовки 01.03.02 Прикладная математика и информатика

Направленность (профиль) Прикладная математика и информатика

Форма обучения очная

Срок освоения ОП 4 года

Институт Прикладной математики и информационных технологий

Кафедра разработчик РПД Математика

Выпускающая кафедра Математика

Начальник
учебно-методического управления

Семенова Л.У.

Директор института ПМ и ИТ

Тебுவ Д.Б.

Заведующий выпускающей кафедрой

Кочкаров А.М.

г. Черкесск, 2022 г.

СОДЕРЖАНИЕ

1. Цели освоения дисциплины.....	4
2. Место дисциплины в структуре образовательной программы	5
3. Планируемые результаты обучения по дисциплине.....	6
4. Структура и содержание дисциплины.....	8
4.1. Объем дисциплины и виды работы.....	8
4.2. Содержание дисциплины	9
4.2.1. Разделы (темы) дисциплины, виды деятельности и формы контроля.....	9
4.2.2. Лекционный курс	9
4.2.3. Лабораторный практикум	11
4.2.4. Практические занятия	12
4.3. Самостоятельная работа обучающегося.....	13
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	14
6. Образовательные технологии.....	16
7. Учебно-методическое и информационное обеспечение дисциплины.....	17
7.1. Перечень основной и дополнительной учебной литературы.....	17
7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»....	17
7.3. Информационные технологии	18
8. Материально-техническое обеспечение дисциплины	18
8.1. Требования к аудиториям (помещениям, местам) для проведения занятий.....	18
8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся.....	20
8.3. Требования к специализированному оборудованию.....	20
9. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.....	21
Приложение 1. Фонд оценочных средств.....	22
Приложение 2. Аннотация дисциплины.....	40
Рецензия на рабочую программу.....	41
Лист переутверждения рабочей программы дисциплины.....	42

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «**Защита информации**» является ознакомление обучающихся с основными организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами.

Задачи дисциплины:

- освоение обучающимися основных положений теории информационной безопасности в компьютерных системах;
- освоение обучающимися основных принципов и методов, применяемых при защите компьютерных систем.
- изучение правовых основ защиты информации в компьютерной системе;
- изучение организационно-технических, программно-аппаратных методов и средств защиты информации;
- изучение стандартов, моделей и методов шифрования информации, методы идентификации пользователей, методы защиты программ от вирусов;
- изучение криптографических методов защиты информации в компьютерных системах
- оценивать защищенность компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «**Защита информации**» относится к вариативной части Блока 1 Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. Ниже приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1	Объектно – ориентированное программирование	Преддипломная практика
2	Численные методы	

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 01.03.02 Прикладная математика и информатика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/индекс компетенции	Наименование компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:
1	2	3	4
1.	ОПК-5	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-5.1 Обладает базовыми знаниями в области алгоритмизации и программирования ОПК-5.2 Использует структурные особенности языков программирования и пакетов прикладных программ при реализации алгоритмов для решения прикладных задач ОПК-5.3 Разрабатывает компьютерные программы, пригодные для практического использования

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды работы

Вид учебной работы		Семестр	
		Всего часов	№ 8 (часы)
1		2	3
Аудиторная контактная работа (всего)		52	52
В том числе:			
Лекции (Л)		26	26
Практические занятия (ПЗ)		26	26
Лабораторные работы (ЛР)		-	-
Контактная внеаудиторная работа, в том числе		3,5	3,5
Индивидуальные и групповые консультации			
Самостоятельная работа обучающегося (СРО) (всего)		90	90
<i>Подготовка к практическим работам (ПР)</i>		40	40
<i>Работа с книжными и электронными источниками</i>		40	40
<i>Подготовка к промежуточному тестовому контролю</i>		10	10
Промежуточная аттестация	Зачет с оценкой, в том числе	ЗаО	ЗаО
	Прием зачета с оценкой, час	0,5	0,5
	СРО, час.		
ИТОГО: Общая трудоемкость	часов	144	144
	зач. ед.	4	4

4.2. Содержание дисциплины

4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля

№ п/п	Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР	ПЗ	СРО	все-го	
1	2	3	4	5	6	7	8
Семестр 8							
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	4		4	22	30	Контроль, контрольные вопросы
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	6		6	22	34	Текущий тестовый контроль, контрольные вопросы
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	6		6	22	34	Текущий тестовый контроль, контрольные вопросы
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	10		10	24	44	Текущий тестовый контроль, контрольные вопросы
5	Контактная внеаудиторная работа					1,5	индивидуальные и групповые консультации
	Промежуточная аттестация					0,5	ЗаО
Итого часов в 8 семестре:		26		26	90	144	
Всего:						144	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего Часов (ОФО)
1	2	3	4	5
Семестр 8				
1.	Раздел 1. Технологии защиты информации. Информационная безопасность.	1.1. Основные угрозы информации в компьютерных системах	Понятие безопасности. Информационные ресурсы. Взаимосвязь понятий информационной безопасности и защиты информации. Особенности защиты информации. Американские и европейские стандарты по защите информации.	4
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	2.1 Государственная политика в области безопасности компьютерных систем	Уязвимость информации. Понятие несанкционированного доступа к конфиденциальной информации. Дискреционная и мандатная политика безопасности. Правовые методы обеспечения информационной безопасности.	2
		2.2 Классификация технических средств защиты информации.	Физические средства защиты. Межсетевые экраны. Аутентификация пользователей на основе паролей и модели «рукопожатия». Аутентификация пользователей по биометрическим характеристикам, клавиатурному почерку и росписи мышью.	4
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	3.1 Элементы теории чисел	Взаимно простые числа. Сравнимость по модулю. Нахождение вычета некоторого числа по модулю. Кольцо вычетов. Арифметика часов. НОД. Функция Эйлера.	2
		3.2 Основные понятия криптологии. Методы шифрования	Шифрование. Симметричные и асимметричные криптосистемы. Абсолютно стойкий шифр. Хеширование. Криптографическая система DES и ее модификация. Криптографическая система ГОСТ 28147-89.	4
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1 Вредоносные программы	Классификация вредоносных программ. Загрузочные и файловые вирусы. Методы обнаружения и удаления ви-	4

			русов. Программные закладки и методы защиты от них.	
		4.2 Защита программных средств от несанкционированного использования и копирования	Принципы построения систем защиты от копирования. Методы защиты инсталляционных дисков от копирования. Методы настройки устанавливаемого программного обеспечения на характеристики компьютера. Методы противодействия исследованию алгоритма работы системы защиты	6
ИТОГО часов в 8 семестре:				26
Всего:				26

4.2.3. Практические занятия

№ п/п	Наименование раздела дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов (ОФО)
1	2	3	4	5
Семестр 8				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1 Теория чисел. Деление по модулю. Арифметика часов. Программирование алгоритма шифрования	Алгоритм шифрования открытого текста методом гаммирования. Листинг программы	2
			Шифрование методом Виженера. Программная реализация.	2
2	Раздел 2. Методы защиты информации от несанкционированного доступа	Электронная цифровая подпись. Вычисление ЭЦП.	Шифрование методом Диффи-Хелмана Программная реализация	6
3	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.	3.1 Симметричное шифрование	Шифрование методом блочной перестановки. Шифр Гронсфельда. Программная реализация	4
		3.2 Асимметричное шифрование	Использование двух ключей: открытый и закрытый. Шифр RSA. Программная реализация	2
4	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1 Методика использования антивирусных программ	Сайт лаборатории Касперского. Изучение интерфейса антивирусной программы «Антивирус Касперского». Проверка на вирус всех критических областей ПК.	10
ИТОГО часов в 8 семестре:				26

Всего:	26
---------------	-----------

4.3. Самостоятельная работа обучающегося

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего Часов (ОФО)
1	3	4	5	6
Семестр 8				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1	Работа с основной и дополнительной литературой. Чтение конспекта лекций. Подготовка к лабораторному практикуму.	22
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	2.1	Проработка лекций, работа с учебниками. Подготовка к лабораторному практикуму.	10
		2.2	Изучение конспекта лекций. Выполнения индивидуальных заданий по лабораторному практикуму.	12
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.	3.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по теме курсовой работы.	10
		3.2	Изучение конспекта лекций для выполнения практической и лабораторной работы	12
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1	Изучение конспекта лекций для выполнения практической и лабораторной работы.	12
		4.2	Изучение конспекта лекций. Выполнения индивидуальных заданий по лабораторному практикуму.	12
ИТОГО часов в 8 семестре:				90
Всего:				90

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

Обучающийся, готовясь к лекционному занятию, включает выполнение всех видов заданий размещенных в каждой лекции, т.е. задания выполняются еще до лекционного занятия по соответствующей теме. В ходе лекционных занятий, обучающийся должен вести конспектирование лекционного материала, обращать внимание на термины и определения, а также формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Обучающийся должен оставить в рабочих конспектах поля, на которых делает пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Обучающийся также должен задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой. Обучающийся должен уметь проводить текущей лекции с предшествующей лекцией.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

Лабораторные работы сопровождают и поддерживают лекционный курс.

Обучающийся должен подготовиться к выполнению лабораторных работ строго в соответствии с содержанием курса.

В начале каждого лабораторного занятия обучающийся должен ознакомиться с теоретическим материалом, необходимым для выполнения текущей лабораторной работы.

Подготовить ответы на контрольные вопросы, которые соответствуют теме лабораторной работы.

Каждая лабораторная работа содержит список индивидуальных заданий, на выполнение которых обучающийся должен быть готовым.

Полученные результаты выполнения лабораторной работы обучающийся должен уметь оформить и быть готовым к устной защите.

5.3. Методические указания для подготовки обучающихся к практическим занятиям

В ходе подготовки к практическим занятиям, обучающийся должен:

- изучить основную и дополнительную литературу, ознакомиться с новыми публикациями в периодических и электронных изданиях по теме практического занятия учебной программы;

- подготовиться к устному опросу, для этого подготовить ответы по всем учебным вопросам, выносимым на практическое занятие;

- подготовиться к выполнению текущего практического занятия, изучая соответствующую тему лекции;

- после прохождения каждого раздела, обучающийся, для целей закрепления пройденного материала проходит тесты;

- осуществляет самоконтроль качества подготовки к практическому занятию, осуществляя проверку своих знаний, отвечая на вопросы для самопроверки по соответствующей теме.

- обучающийся, при подготовке к практическому занятию может консультироваться с преподавателем через электронную почту и получать от него наводящие разъяснения.

5.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме дисциплины обучающимся предлагается перечень заданий для самостоятельной работы. К выполнению заданий для самостоятельной работы предъявляются следующие требо-

вания: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению. Обучающимся следует:

- руководствоваться графиком самостоятельной работы, определенным на кафедре;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать неясные вопросы на лабораторных и практических занятиях, а также получить информацию на консультациях.

5.4 Методические рекомендации прохождения тестирования

Подготовку к итоговому тестированию необходимо осуществлять поэтапно.

На первом этапе необходимо повторить основные положения всех тем, детально разбирая наиболее сложные моменты. Непонятные вопросы необходимо выписывать, чтобы по ним можно было проконсультироваться с преподавателем перед прохождением итогового тестирования. Подготовку по темам каждой дидактической единицы целесообразно производить отдельно. На этом этапе необходимо использовать материалы лекционного курса, материалы семинарских занятий, тестовые задания для текущего контроля знаний, а также презентации лекционного курса.

На втором этапе подготовки предлагается без повторения теоретического материала дать ответы тестовые задания для рубежного контроля знаний. Если ответы на какие-то вопросы вызвали затруднение, необходимо еще раз повторить соответствующий теоретический материал.

Наконец, третий этап подготовки необходимо осуществить непосредственно накануне теста. На данном этапе необходимо аккуратно просмотреть весь лекционный курс.

В случае, если результаты выполнения тестового задания оказались неудовлетворительными, необходимо зафиксировать темы, на вопросы по которым были даны неверные ответы, и еще раз углубленно повторить соответствующие темы в соответствии с указанными выше тремя этапами подготовки к тестированию.

5.5 Методические указания по подготовке к опросу (контрольные вопросы)

Самостоятельная работа обучающихся включает подготовку к опросу на практическом занятии. Опрос представляет собой форму текущего контроля успеваемости обучающегося по изучаемой дисциплине. При подготовке к опросу необходимо изучить материалы лекции, основную и дополнительную литературу, а также информацию с использованием Интернет-ресурсов по заявленной теме. Темы практических занятий, вопросы для обсуждения, а также контрольные вопросы даются в методических указаниях по соответствующим темам дисциплины. Обучающийся должен обратить внимание на основные термины и понятия по теме, на проблемные вопросы, подобрать дополнительную литературу для их освещения, составить тезисы выступления. Ответ обучающегося должен быть развернутым, аргументированным, логически выстроенным. При выставлении оценки учитывается правильность ответа по содержанию, самостоятельность суждений и выводов, умение анализировать и связывать теоретические положения с практикой.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4
Семестр 8			
1	1.1. Основные угрозы информации в компьютерных системах	Лекция–информация. Метод мозгового штурма	2
2	2.1 Государственная политика в области безопасности компьютерных систем	Лекция – информация. Презентация Метод мозгового штурма	2
4	2.2 Классификация технических средств защиты информации.	Лекция – информация. Презентация Метод мозгового штурма	2
5	3.1 Элементы теории чисел	Лекция – информация. Презентация Метод мозгового штурма	2
6	3.2 Основные понятия криптологии	Лекция – информация. Презентация	2
7	4.1 Антивирусные программы	Лекция – информация. Презентация	2
8	4.2 Политика безопасности в КС. Уровни доступа к информации для пользователей	Лекция – информация. Презентация	2
Итого часов в 8 семестре:			14
Всего:			14

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Алешников, С. И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых: учебное пособие / С. И. Алешников, Е. С. Алексеенко. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2010. — 158 с. — ISBN 978-5-9971-0073-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/23796.html>
2. Алешников, С. И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях: практическое пособие / С. И. Алешников, Е. В. Козьминых. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 с. — ISBN 5-88874-689-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/23851.html>
3. Алешников, С. И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых: практическое пособие / С. И. Алешников, Ю. Ф. Болтнев. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007. — 58 с. — ISBN 978-5-88874-803-9. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/23795.html>

Дополнительная литература

1. Гуров, В. В. Архитектура и организация ЭВМ / В. В. Гуров, В. О. Чуканов. — 2-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 183 с. — ISBN 5-9556-0040-X. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/73706.html>
2. Яроцкая, Е. В. Экономико-математические методы и моделирование: учебное пособие / Е. В. Яроцкая. — Саратов: Ай Пи Эр Медиа, 2018. — 227 с. — ISBN 978-5-4486-0074-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/69291.html>
3. Метелица, Н. Т. Вычислительные сети и защита информации: учебное пособие / Н. Т. Метелица. — Краснодар: Южный институт менеджмента, 2013. — 48 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/25962.html>
4. Краковский, Ю. М. Защита информации: учебное пособие / Ю. М. Краковский. — Ростов-на-Дону: Феникс, 2016. — 349 с. — ISBN 978-5-222-26911-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/59350.html>
5. Никифоров, С. Н. Защита информации. Защита от внешних вторжений: учебное пособие / С. Н. Никифоров. — Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 с. — ISBN 978-5-9227-0757-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/74381.html>

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Электронно-библиотечная система IPRbooks URL: [http:// www.iprbooks.ru/](http://www.iprbooks.ru/) ООО «Ай Пи Эр Медиа». Доступ к ЭБС IPRbooks Договор №6906/20 от 01.07.2020г Подключение с 01.07.2020г. по 01.07.2021г
2. Электронно-библиотечная система IPRbooks URL: [http:// www.iprbooks.ru/](http://www.iprbooks.ru/) ООО «Ай Пи Эр Медиа». Доступ к ЭБС IPRbooks Договор №8117/21П от 11.06.2021г Подключение с 01.07.2021г до 01.07.2022г.

7.3. Информационные технологии, лицензионное программное обеспечение

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Microsoft Azure Dev Tools for Teaching 1. Windows 7, 8, 8.1, 10 2. Visual Studio 2008, 2010, 2013,2019 5. Visio 2007, 2010, 2013 6. Project 2008, 2010, 2013 7. Access 2007, 2010, 2013 и т. д.	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022г. (продление подписки)
MS Office 2003, 2007, 2010, 2013	Сведения об Open Office: 63143487, 63321452, 64026734, 6416302, 64344172, 64394739, 64468661, 64489816, 64537893, 64563149, 64990070, 65615073 Лицензия бессрочная
Антивирус Dr.Web Desktop Security Suite	Лицензионный сертификат Серийный № 8 DVG-V96F-H8S7-NRBC Срок действия: с 20.10.2022 до 22.10.2023г.
Цифровой образовательный ресурс IPRsmart	Лицензионный договор №10423/23П от 30.06.2023 г. Срок действия: с 01.07.2023 г. до 01.07.2024г.

Свободное программное обеспечение: WinDJView, Sumatra PDF,7-Zip

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к аудиториям (помещениям, местам) для проведения занятий

1. Учебная аудитория для проведения занятий лекционного типа

Ауд.243

Специализированная мебель:

Кафедра настольная - 1 шт., доска меловая - 1 шт., стулья – 65 шт., парты - 34шт.

Технические средства обучения, служащие для предоставления учебной информации большой аудитории:

Экран на штативе – 1 шт.

Проектор – 1 шт.

Ноутбук – 1 шт

2. Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнение курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Ауд.251

Специализированная мебель:

Стол преподавательский - 1 шт., компьютерные столы - 10шт., парты -7шт., стулья - 24шт., доска меловая - 1шт.

Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:

Персональный компьютер – 10 шт.

Экран настенный рулонный – 1 шт.

3. Лаборатория компьютерной графики

Ауд.251 Специализированная мебель:

Стол преподавательский - 1 шт., компьютерные столы - 10шт., парты -7шт., стулья - 24шт., доска меловая - 1шт.

Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:

Персональный компьютер – 10 шт.

Экран настенный рулонный – 1 шт.

8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся

Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде, и т.п.

8.3. Требования к специализированному оборудованию нет

9. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается (в случае необходимости) адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья комплектуется фонд основной учебной литературой, адаптированной к ограничению электронных образовательных ресурсов, доступ к которым организован в БИЦ Академии. В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ Защита информации

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Защита информации в компьютерных системах

Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ОПК-5	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

2. Этапы формирования компетенции в процессе освоения дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающимися.

Этапность формирования компетенций прямо связана с местом дисциплины в образовательной программе.

Разделы (темы) дисциплины	Формируемые компетенции (коды)
	ОПК-5
Раздел 1. Технология защиты информации. Информационная безопасность.	
1.1. Основные угрозы информации в компьютерных системах	+
Раздел 2. Методы защиты информации от несанкционированного доступа	
2.1 Государственная политика в области безопасности компьютерных систем	+
2.2 Классификация технических средств защиты информации	+
Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	
3.1 Элементы теории чисел	+
3.2 Основные понятия криптологии	+
Раздел 4. Защита компьютерных систем от вредоносных программ	
4.1 Вредоносные программы	+
4.2 Защита программных средств от несанкционированного использования и копирования.	+

3. Показатели, критерии и средства оценивания компетенций, формируемых в процессе изучения дисциплины

ОПК-5

Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Индикаторы достижения компетенции	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовлетв	удовлетв	хорошо	отлично	Текущий контроль	Промежуточная аттестация
ОПК-5.1 Обладает базовыми знаниями в области алгоритмизации и программирования	Допускает существенные ошибки в знаниях стандартных пакетов прикладных программ для решения практических задач защиты информации, отлаживать и тестировать программы по алгоритмам шифрования; пробелы в знаниях элементов теории чисел.	Демонстрирует некоторые способности в знаниях стандартных пакетов прикладных программ для решения практических задач защиты информации, отлаживать и тестировать программы по алгоритмам шифрования, а также криптографическим методам и средств обеспечения информационной безопасности.	Демонстрирует способность в знаниях стандартных пакетов прикладных программ для решения практических задач защиты информации, отлаживать и тестировать программы по алгоритмам шифрования, а также криптографическим методам и средств обеспечения информационной безопасности	Демонстрирует профессиональную способность к языкам программирования, для целей автоматизации шифрования информации; методов кодирования; знания о государственной политике в области безопасности компьютерных систем; знания элементов теории чисел, составляющие математическую основу криптографических	Текущий тестовый контроль, контрольные вопросы	Зачет с оценкой
ОПК-5.2 Использует структурные особенности языков программирования и пакетов прикладных программ при реализации алгоритмов для решения прикладных задач	Допускает частично освоенное умение пользоваться стандартными программами для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять крип-	Демонстрирует в целом удовлетворительные, но не систематизированные умения пользоваться стандартными программами для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять	Демонстрирует в целом хорошие, но содержащие отдельные пробелы в использовании стандартных программ для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифро-	Демонстрирует умения в использовании стандартных программ для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять элементы теории чисел для задач криптографических	Текущий тестовый контроль, контрольные вопросы	Зачет с оценкой

	тографические методы и средства обеспечения информационной безопасности.	криптографические методы и средства обеспечения информационной безопасности; использовать элементы теории чисел для моделирования задач защиты информации.	вания; применять элементы теории чисел для моделирования задач криптографии.	методов и средств обеспечения информационной безопасности.		
ОПК-5.3 Разрабатывает компьютерные программы, пригодные для практического использования	Фрагментарно владеет некоторыми пакетами стандартных программ для решения задач защиты информации; не владеет интернет технологиями для организации защиты информации, не владеет возможностями математической основы криптографии теории чисел.	Владеет отдельными навыками работы со стандартными программами для решения задач защиты информации; технологиями отладки и тестирования программ по алгоритмам шифрования; элементов теории чисел для моделирования задач защиты информации.	Демонстрирует в целом успешные знания по стандартным программам для решения практических задач защиты информации; технологии отладки и тестирования программ по алгоритмам шифрования; по криптографическим методам и средствам обеспечения информационной безопасности.	Демонстрирует профессиональные навыки работы в специализированных пакетах программ для решения практических задач защиты информации; владеет технологиями отладки и тестирования программ по алгоритмам шифрования; владеет способностью применять элементы теории чисел для решения задач криптографии.	Текущий тестовый контроль, контрольные вопросы	Зачет с оценкой

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к зачету с оценкой

по дисциплине Защита информации

1. Проблема защиты информации и подходы к ее решению.
2. Основные понятия защиты информации.
3. Угрозы безопасности и каналы утечки информации.
4. Классификация методов и средств защиты информации. Специфика программных средств. Правовое обеспечение защиты информации.
5. Способы нарушения защищенности информации и защиты от него в компьютерных системах.
6. Организация базы учетных записей пользователей в ОС Windows
7. Способы аутентификации пользователей.
8. Аутентификация пользователей на основе паролей и модели «рукопожатия».
9. Программно-аппаратная защита от локального несанкционированного доступа.
10. Аутентификация пользователей на основе их биометрических характеристик.
11. Протоколы прямой аутентификации.
12. Протоколы не прямой аутентификации.
13. Виртуальные частные сети.
14. Разграничение прав пользователей в ОС Windows.
15. Дискреционное, мандатное и ролевое разграничение доступа к объектам.
16. Подсистема безопасности ОС Windows.
17. Разграничение доступа к объектам в ОС Windows.
18. Средства защиты информации в глобальных компьютерных сетях.
19. Стандарты оценки безопасности компьютерных систем
20. Элементы теории чисел.
21. Способы симметричного шифрования. Абсолютно стойкий шифр.
22. Генерация, хранение и распространение ключей.
23. Криптографическая система DES и ее модификации.
24. Криптографическая система ГОСТ 28147-89.
25. Применение и обзор современных симметричных криптосистем.
26. Принципы построения, свойства и применение асимметричных криптосистем.
27. Криптографическая система RSA.
28. Криптографические системы Диффи-Хеллмана, Эль-Гамала
29. Электронная цифровая подпись и ее применение. Функции хеширования.
30. Принципы построения систем защиты от копирования.
31. Защита установочных дисков и установленного программного обеспечения.
32. Защита программных средств от изучения.
33. Вредоносные программы, их признаки и классификация.
34. Программные закладки и защита от них.
35. Методы обнаружения и удаления вредоносных программ

Контрольные вопросы к разделам

по дисциплине Защита информации

Раздел 1. Технология защиты информации. Информационная безопасность.

1. В каких формах может быть представлена информация?
2. Что относится к информации ограниченного доступа?
3. Что понимается под защитой информации?
4. Что относится к основным характеристикам защищаемой информации?
5. Что такое угроза безопасности информации? Каковы основные виды угроз?
6. Какие существуют каналы утечки конфиденциальной информации?
10. Почему проблема защиты информации не может быть решена с помощью только формальных методов и средств?
11. В чем сущность организационной защиты информации?
12. Каковы уровни правового обеспечения информационной безопасности?
13. Какие законодательные акты составляют основу российского информационного права?
14. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?

Раздел 2. Методы защиты информации от несанкционированного доступа

1. Какие существуют способы несанкционированного доступа к информации в компьютерных системах?
2. Какие способы аутентификации пользователей могут применяться в компьютерных системах?
3. В чем заключаются основные недостатки парольной аутентификации и как она может быть усилена?
4. В чем сущность, достоинства и недостатки аутентификации на основе модели «рукопожатия»?
5. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?
6. В чем специфика аутентификации пользователей на основе их клавиатурного почерка и росписи мышью?
7. Какие элементы аппаратного обеспечения могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем?
10. Почему с помощью только программных средств нельзя обеспечить необходимую степень защищенности от локального несанкционированного доступа к информации в компьютерных системах?
13. Какие применяются разновидности межсетевых экранов?
14. Что такое VPN и для чего они предназначены?
15. Каковы общие недостатки всех межсетевых экранов?
16. В чем сущность, достоинства и недостатки дискреционного управления доступом к объектам КС?

Раздел 3. Криптографические методы и средства обеспечения информационной безопасности

1. Что называется вычетом целого числа по некоторому модулю?
2. Почему операции над вычетами находят широкое применение в криптографии?
3. В чем разница между симметричными и асимметричными криптографическими системами?
4. Какие основные способы применяются при создании алгоритмов симметричной криптографии?
5. В чем разница между потоковыми и блочными шифрами?
6. Какие симметричные криптосистемы используются сегодня?
7. В каких режимах может использоваться криптосистема DES?
8. Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста?
9. В каких режимах может использоваться криптосистема ГОСТ 28147-89? Как в ней обеспечивается аутентичность и целостность шифротекстов.
10. Что лежит в основе асимметричной криптографии?
11. В чем особенности и основные сферы применения асимметричных криптосистем?
12. На чем основана криптостойкость систем RSA и Эль-Гамала?
13. Что такое электронная цифровая подпись, как она получается и проверяется?
14. Какова роль в системах ЭЦП функций хеширования?
15. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?
16. Какие функции CryptoAPI используются для получения и проверки электронной цифровой подписи?
17. Каков порядок вызова функций CryptoAPI при получении ЭЦП?

Раздел 4. Защита компьютерных систем от вредоносных программ

1. Какие программы относят к разряду вредоносных?
2. Что такое компьютерный вирус?
3. Какие существуют виды компьютерных вирусов?
4. В чем разница между загрузочными и файловыми вирусами?
5. Как происходит заражение и функционирование загрузочных вирусов?
6. Какие типы файлов могут заражаться файловыми вирусами?
7. Как происходит заражение программных файлов?
8. Почему файлы документов могут содержать вирусы?
9. Как обеспечивается автоматическое получение управления макровирусами?
10. Как включить встроенную защиту от вирусов в макросах в программах Microsoft Office? В чем недостатки этой защиты?
11. Какие существуют основные каналы заражения вирусами объектов компьютерной системы?
12. Какие существуют методы автоматического обнаружения и удаления вирусов? В чем их достоинства и недостатки?
13. В чем заключается профилактика заражения компьютерными вирусами?
14. Какие виды программных закладок существуют?
15. Как может происходить проникновение программной закладки в компьютерную систему?
16. Как осуществляется взаимодействие внедренной в КС программной закладки и нарушителя?
17. Какие существуют методы защиты от программных закладок? Что такое изолированная программная среда?
18. Что называется защитой программных продуктов от несанкционированного копирова-

ния?

19. На каких принципах должна основываться разработка системы защиты от копирования?

20. Какие требования предъявляются к системам защиты от копирования?

21. Из каких основных компонентов состоит типовая система защиты от копирования?

22. Какие характеристики компьютера могут использоваться для настройки защищаемого программного продукта?

23. В чем заключается достоинства и недостатки программно-аппаратной защиты от копирования на основе электронных ключей?

Тестовые задания

по дисциплине Защита информации

Раздел 1. Технология защиты информации. Информационная безопасность.

1. Формы представления информации в плане защиты информации

1. Цифровая, документированная, графическая
2. Программная, алгоритмическая, телекоммуникационная
3. Электронная, реквизитная, текстовая
4. Речевая, документированная, телекоммуникационная

2. Документированной называется информация

1. Представленная на материальных носителях вместе с идентифицирующими ее реквизитами
2. Представленная в виде кодов и сохраненная на лазерных дисках объемом 1,5 Мб.
3. Представленная только на жестких магнитных дисках вместе с идентифицирующими ее реквизитами
4. Закодированная и защищенная паролем, и представленная на носителях вместе с идентифицирующими ее реквизитами

3. К информации ограниченного доступа относится

1. Служебные сведения, не подлежащие распространению в сети интернет
2. Конфиденциальная информация, хранящаяся в государственных архивах данных
3. Информация, запрашиваемая гражданами в органах государственной власти
4. Государственная тайна и конфиденциальная информация.

4. Под защитой информации понимается

1. Комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности
2. Комплекс мероприятий, направленных на обеспечение целостности информации
3. Комплекс мероприятий, направленных на обеспечение хранения информации
4. Комплекс мероприятий, направленных на ввод, хранения, обработки и передачи данных

5. К основным характеристикам защищаемой информации относится

1. Кодированность, корректность, целостность
2. Государственность, служебность, доступность
3. Конфиденциальность, целостность и доступность
4. Целостность, защищенность и доступность

6. Угроза безопасности информации это

1. Событие или действие, которое может вызвать изменение функционирования компьютерных систем, связанное с нарушением защищенности обрабатываемой в ней информации
2. Действие, которое может вызвать искажение обрабатываемой информации
3. Событие, которое может послужить потере конфиденциальной информации
4. Событие или действие, которое может вызвать изменение функционирования физического канала связи в компьютерных системах, по которому передается защищаемая информация

7. ПЭМИН это когда

1. Потеря информации происходит через специальные каналы утечки информации
2. Утечка информации происходит через подслушивающие аппараты

3. Утечка информации происходит через сотрудников управления
4. Утечка информации происходит через перехваты электромагнитных излучений и наводок

8. Уровни правового обеспечения информационной безопасности

1. Международные договоры, подзаконные акты, государственные стандарты, локальные нормативные акты
2. Международные договоры, Федеральные законы, государственные стандарты, Указы Президента РФ
3. Подзаконные акты, государственные стандарты, Постановления Правительства РФ
4. Локальные нормативные акты, письма Арбитражного Суда РФ, международные договоры

8. Инженерно-технические средства защиты информации

1. Механические, электрические, электронные устройства, аппаратные средства компьютерных систем, папки и файлы
2. Физические объекты, механические, электрические, электронные устройства, элементы конструкции зданий, охрана
3. Электронные устройства, элементы конструкции зданий, охрана, персонал, противопожарная защита
4. Физические объекты, механические, электрические, электронные устройства, элементы конструкции зданий, средства пожаротушения

9. Комплексная система защиты информации это

1. Это совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в КС.
2. Это совокупность объединенных единым целевым назначением средств, для обеспечения защиты информации в КС.
3. Это совокупность правил, законов и писем, в которых прописаны методы и средства обеспечивающих необходимую эффективность защиты информации в КС.
4. Это свод правил утвержденных законодательно в целях организации эффективной защиты информации в КС

Раздел 2. Методы защиты информации от несанкционированного доступа

10. Основные способы защиты от несанкционированного доступа к информации в компьютерных системах

1. Идентификация, авторизация, шифрование
2. Аутентификация, авторизация, шифрование
3. Шифрование, аутентификация, электронная цифровая подпись
4. Электронная цифровая подпись, авторизация, шифрование

10. Основные недостатки парольной аутентификации

1. Сложно обеспечить реальную уникальность и сложность каждого вновь выбираемого пользователем пароля
2. Возможность перехвата пароля в открытом виде или его подбора по хеш-значению
3. Возможность получения или смены пароля в результате обмана
4. Все вышеперечисленные недостатки

11. Сущность модели «рукопожатия»

1. Способ аутентификации пользователя и применяется при удаленной аутентификации
2. Секретное правило преобразования информации
3. Запрос-ответ, парольная аутентификация
4. Все вышеперечисленные являются сущностью модели «рукопожатия»

12. Биометрические характеристики пользователей, которые могут применяться для их аутентификации

1. Отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза
2. Рисунок сетчатки глаза, геометрическая форма и размеры лица
3. Тембр голоса, геометрическая форма и размеры уха
4. Все выше перечисленные биометрические характеристики

13. Характерные особенности аутентификации пользователей на основе их клавиатурного почерка и росписи мышью?

1. Стабильность их характеристик для всех пользователей независимо от возраста и эмоционально- психологического состояния
2. Нестабильность их характеристик у одного и того же пользователя, связанными с улучшением навыков по работе с клавиатурой и мышью или наоборот из-за старения организма, а также с изменениями связанными с эмоциональным состоянием пользователя.
3. Нарушение навыков по работе с клавиатурой и мышью или наоборот из-за старения организма, а также с изменениями связанными с эмоциональным состоянием пользователя.
4. Нестабильность их характеристик у одного и того же пользователя, связанными с улучшением их психологического состояния

14. Элементы аппаратного обеспечения, которые могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем

1. Магнитные диски, пластиковые карты с магнитной полосой, Touch Memory, карты со штрих-кодом, смарт-карты, маркеры eToken (USB-брелки)
2. Магнитные диски, пластиковые карты, iButton, карты со штрих-кодом, смарт-карты, USB-брелки
3. Магнитные диски, пластиковые карты с магнитной полосой, карты со штрих-кодом, карты с памятью, смарт-карты, маркеры eToken
4. 2. Магнитные диски, пластиковые карты, Touch Memory, карты со штрих-кодом, смарт-карты с паролем, USB-брелки с памятью

15. Touch Memory представляет собой

1. Миниатюрную батарейку с определенным диаметром и толщиной, имеющий один сигнальный контакт и один контакт заземления
2. Миниатюрную батарейку с определенным диаметром 16мм и толщиной в пределах от 3 до 6 мм, имеющий один сигнальный контакт и один контакт заземления
3. Миниатюрную батарейку с определенным диаметром 15 мм и толщиной в пределах от 4 до 6 мм, имеющий один сигнальный контакт и один контакт заземления
4. Миниатюрную батарейку с ПЗУ и ОЗУ со встроенным элементом питания

16. Двухфакторная аутентификация это

1. метод идентификации пользователя в каком-либо сервисе при помощи запроса всевозможных аутентификационных данных
2. система доступа, основанная на двух «ключках»: одним владеет сам пользователь, например, это телефон, на который приходит SMS с кодом, другой – это его обычные логин и пароль
3. процедура прохождения алгоритма аутентификации строго в два этапа
4. один из способов защиты информации от несанкционированного доступа, требующий помимо основного пароля и биометрические данные пользователя

17. В основе работы протокола S/Key лежит?

1. протокол PAP для аутентификации пользователей на основе встроенной базы данных одноразовых паролей

2. протокол PAP, который не может существовать без S/Key
3. лежит процедура аутентификации по биометрическим характеристикам
4. протокол, определяющий пользователя при помощи специальных аппаратных средств (смарт-карты, USB-токенов и т.д.)

18. Протокол CHAP основан

1. на модели «рукопожатия»
2. на модели специальных аппаратных средств
3. на модели «клиент»-«сервер»
4. генерации случайных чисел с целью определения ID-сервера

19. Протокол Kerberos предназначен для

1. обеспечения конфиденциальности передаваемой по сети информации, используя при этом функции шифрования, а также технологию выдачи мандатов
2. однопользовательских рабочих станций, для целей безопасной передачи информации по локальной сети
3. для аутентификации субъекта объектом через специальные ключи шифрования
4. централизованного администрирования учетных записей пользователей работающих в сети интернет

20. Применяемые разновидности межсетевых экранов

1. фильтрующие маршрутизаторы
2. шлюзы сеансового уровня
3. шлюзы прикладного уровня
4. все вышеперечисленные

21. VPN предназначены?

1. для создания всевозможных межсетевых экранов
2. виртуальные частные сети для скрытия топологии внутренних сетей организаций, обменивающихся информацией по сети интернет, и защиты трафика между ними.
3. виртуальные частные сети для выделения числа защищаемых подсетей и выделения специального криптомаршрутизатора для безопасной передачи данных по сети интернет
4. виртуальные частные сети для открытия топологии внутренних сетей организаций, обменивающихся информацией по сети интернет, и защиты трафика между ними с использованием криптомаршрутизатора

22. В чем достоинства и недостатки использования пароля программы BIOS Setup?

1. все пользователи получают разные пароли, сложность замены пароля если он забыт, слабая защищенность, технические пароли позволяют загрузить операционную систему неавторизованным пользователям
2. все пользователи получают одинаковые пароли, простора замены пароля если он забыт, слабая защищенность, технические пароли позволяют загрузить операционную систему неавторизованным пользователям
3. все пользователи получают разные пароли, сложность замены пароля если он забыт, слабая защищенность, технические пароли не позволяют загрузить операционную систему неавторизованным пользователям
4. все пользователи получают общий пароль, сложность замены пароля если он забыт, слабая защищенность, технические пароли позволяют загрузить операционную систему неавторизованным пользователям

25. Пароли пользователей в открытых версиях операционной системы Windows сохраняются в файле с расширением

1. *.pwl

2. *.scr
3. *.sys
4. *.pvl

26. Редактор системных правил Windows называется и предназначен

1. edit и предназначен для редактирования реестра ОС
2. poledit и предназначается для ввода определенных ограничений на права конкретного пользователя или всех пользователей системы
3. editor и предназначается для ввода запрета на выполнение программ в режиме эмуляции DOS
4. poleditor и предназначен для ввода определенных ограничений на настройку панели управления ОС

27. Операционные системы Windows 9x/ME/XP Home Edition не могут считаться защищенными

1. в силу того, что перед началом проектирования версий ОС эта цель изначально не ставилась
2. в силу широкого распространения отдельно от ОС программно-аппаратных средств защиты информации
3. в силу широкого применения отдельно функционирующих программ по защите информации
4. в силу отсутствия специальных программ по защите ОС

Формируемая компетенция ПК-3

28. Достоинства дискреционного управления доступом к объектам КС

1. простота идентификации, возможность описания пользователем доступ к своим ресурсам
2. детализированность и назначение прав доступа
3. простота реализации доступом к объектам КС и гибкость
4. простота администрирования и гибкость

29. Достоинства мандатного управления доступом к объектам КС

1. простота построения общей схемы доступа и простота администрирования, высокая надежность работы с КС
2. гибкость программной реализации и простота администрирования
3. назначение прав доступа без разграничения пользователей всех уровней
4. правило доступа к объекту осуществляется через специальные модели матрицы доступа

Раздел 3. Криптографические методы и средства обеспечения информационной безопасности

30. Целые числа a и b сравнимы по модулю n (целому числу, неравному нулю)

1. если выполняется условие $a = b + kn$, для некоторого целого числа k
2. если не выполняется условие $a = b + kn$, для некоторого целого числа k
3. если выполняется условие $a = b \{div n\}$ для некоторого целого числа k
4. если не выполняется условие $a = b \{div n\}$ для некоторого целого числа k

31. Что называется вычетом целого числа a по некоторому модулю n ?

1. Если $b \geq 0$, $a = b \{mod n\}$ и $|b| < n$, то b называют вычетом числа a по модулю n .
2. Если $b \leq 0$, $a = b \{mod n\}$ и $|b| < n$, то b называют вычетом числа a по модулю n .
3. Если $b = 1$, $a = b \{mod n\}$ и $|b| < n$, то b называют вычетом числа a по модулю n .
4. Если $b \geq 0$, $a = b \{div n\}$ и $|b| < n$, то b называют вычетом числа a по модулю n .

32. В чем разница между симметричными и асимметричными криптографическими системами?

1. Симметричные криптосистемы применяют один ключ и для шифрования и расшифрования, а асимметричные – разные ключи
2. Симметричные криптосистемы применяют разные ключи, а асимметричные - один ключ и для шифрования и расшифрования
3. Симметричные криптосистемы применяют один ключ и для шифрования и расшифрования и он является несекретным, а асимметричные – разные ключи, которые являются секретными
4. Симметричные криптосистемы применяют один ключ и для шифрования и расшифрования, а асимметричные – разные ключи являющиеся в свою очередь открытыми и закрытыми

33. Какие основные способы применяются при создании алгоритмов симметричной криптографии?

1. перестановки, сочетание и гаммирование
2. перестановки, подстановки и гаммирование
3. перестановки, замещение и гаммирование
4. перемещение, замещение и гаммирование

Формируемая компетенция ПК-3

34. Разница между потоковыми и блочными шифрами состоит в том, что

1. В блочных шифрах присутствует проблема неполных блоков, а в потоковых такой проблемы нет.
2. шифры в потоковом режиме являются несимметричными, а блочные – симметричными шифрами
3. В блочных шифрах присутствует проблема неполных блоков, которые дополняются несколькими битами, а в потоковых такой проблемы нет.
4. потоковый шифр иногда приводит к криптографической потере стойкости, а блочный при этом содержит проблему неполного блока

35. Идеальным (по К. Шеннону) шифром может считаться

1. шифр с ключом шифрования, который вырабатывается по какому-то алгоритму и длина шифруемого открытого текста при этом не должна превышать ключа шифрования
2. шифр с ключом шифрования, который вырабатывается совершенно случайным образом и длина шифруемого открытого текста не должна превышать ключа шифрования
3. шифр с абсолютно стойким ключом шифрования и длина шифруемого открытого текста не должна превышать ключа шифрования
4. шифр с идеальным стойким ключом шифрования и длина шифруемого открытого текста может превышать ключа шифрования

36. В каких режимах может использоваться криптосистема DES?

1. ECB, DBF, CFB, OFB
2. ECB, DBF, CFB, DFB
3. ECB, CBC, CFB, OFB
4. KCB, CBC, CFB, OFB

37. Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста?

1. CBC
2. CFB
3. OFB
4. ECB

38. В каких режимах может использоваться криптосистема ГОСТ 28147-89? Как в ней обеспечивается аутентичность и целостность шифротекстов?

1. сложная замена, гаммирование, гаммирование с прямой связью, генерация ключа имитовставки
2. простая замена, гаммирование, гаммирование с прямой связью, генерация имитовставки длиной 32 бита
3. простая замена, гаммирование, гаммирование без обратной связи, генерация имитовставки
4. простая замена, гаммирование, гаммирование с обратной связью, генерация имитовставки

39. К асимметричным криптографическим системам относятся

1. RSA, Диффи-Хелмана, Эль-Гамала
2. Хофмана, Шеннона, Эль-Гамала
3. Шеннона, Эль-Гамала, Диффи-Хелмана
4. Хофмана, RSA, Эль-Гамала

40. Роль функции хеширования в системах ЭЦП

1. обеспечить защиту от угроз безопасности электронных документов
2. обеспечить защиту от угроз безопасности электронных документов передаваемых по сетям интернет
3. обеспечить криптостойкость на основе эллиптических кривых
4. обеспечить высокую чувствительность к любым изменениям в документе

41. Провайдеры криптографического обслуживания предоставляют услуги

1. шифрования, расшифрования, получения и проверки электронной цифровой подписи, генерация, хранение и распределение ключей шифрования
2. шифрования, расшифрования, получения и проверки электронной цифровой подписи, хранение и распределение ключей расшифрования
3. шифрования, расшифрования, получение и проверка электронной цифровой подписи, хранение и распределение ключей блочного шифрования
4. шифрования, расшифрования, получение и проверка электронной цифровой подписи, хранение и распределение ключей симметричного и несимметричного шифрования в битах

42. На каких принципах строится взаимодействие прикладной программы и криптопровайдера?

1. имеет прямой доступ к изготовлению и хранению ключей, определяет детали выполнения криптографических операций, не обрабатывает данные для аутентификации пользователя
2. не имеет прямого доступа к изготовлению и хранению ключей, определяет детали выполнения криптографических операций, обрабатывает данные для аутентификации пользователя
3. не имеет прямого доступа к изготовлению и хранению ключей, не определяет детали выполнения криптографических операций, обрабатывает данные для аутентификации пользователя
4. не имеет прямого доступа к изготовлению и хранению ключей, не определяет детали выполнения криптографических операций, не обрабатывает данные для аутентификации пользователя

Раздел 4. Защита компьютерных систем от вредоносных программ

43. В операционной системе обеспечиваются аутентичность и целостность криптопровайдера

1. электронной цифровой подписью
2. специальным алгоритмом запроса
3. хеш-значением
4. ключами симметричного шифрования

44. По способу распространения в КС подразделяются на:

1. паразитические, компаньоны, комбинированные
2. ссылочные, перезаписывающие, загрузочные
3. файловые, загрузочные, комбинированные
4. ссылки, файловые, загрузочные

45. По способу заражения других объектов подразделяются на:

1. резидентные, нерезидентные
2. резидентные, загрузочные
3. нерезидентные, ссылочные
4. резидентные, файловые

3

46. По деструктивным возможностям вирусы подразделяются

1. безвредные, неопасные, опасные, очень опасные
2. безвредные, опасные, неопасные, резидентные
3. безвредные, призраки, неопасные, резидентные
4. безвредные, опасные, спутники, резидентные

47. По особенностям реализуемого алгоритма

1. вирусы-шпионы, паразитические, вирусы-призраки
2. вирусы-спутники, вирусы-призраки, резидентные
3. вирусы-спутники, опасные, резидентные
4. вирусы-спутники, паразитические, вирусы-призраки

48. Вредоносные программы – это

1. троянские утилиты и сетевые черви
2. программы, наносящие вред данным и программам, находящимся на компьютере
3. антивирусные программы
4. программы, наносящие вред пользователю, работающему на зараженном компьютере

49. Вирус внедряется в исполняемые файлы и при их запуске активизируется

1. загрузочный вирус
2. макровирус
3. файловый вирус
4. сетевой червь

Комплект заданий для практической работы

по дисциплине Защита информации

Раздел 1. Технология защиты информации. Информационная безопасность.

Практическая работа № 1

Тема: Теория чисел. Деление по модулю. Арифметика часов.

Программирование алгоритма шифрования

Цель: Изучить алгоритм шифрования методом гаммирования

Краткое содержание:

1. Алгоритм шифрования открытого текста методом гаммирования. Листинг программы
2. Ознакомиться с алгоритмом шифрования
3. Автоматизировать на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы

Практическая работа № 2

Тема: Шифрование методом одноалфавитной подстановки. Программная реализация.

Цель: Изучить алгоритм шифрования методом одноалфавитной подстановки.

Краткое содержание:

2. Ознакомиться с алгоритмом шифрования одноалфавитной подстановки.
3. Автоматизировать на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы

Практическая работа № 3

Тема: Настройка программного генератора паролей

Цель: Научиться создавать в системе Lazarus генератор паролей

Краткое содержание:

1. Создание генератора паролей в среде Lazarus.
2. Представить листинг программы
3. Шифрование текстового файла методом Вижинера.
4. Написать программу шифрования и дешифрования текстового файла методом Вижинера на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи
- изучение задания к практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы.

Раздел 2. Методы защиты информации от несанкционированного доступа

Практическая работа № 4

Тема: Криптографические системы

Цель: Изучение алгоритма Эль-Гамала.

Краткое содержание:

1. Алгоритм Эль-Гамала. Решение задачи.
2. Работа в системе Lazarus по программированию криптосистемы Эль-Гамала

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи
- изучение задания к практической работе
- изучение электронных источников по теме работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Практическая работа № 5

Тема: Электронная цифровая подпись. Вычисление ЭЦП.

Цель: Изучить алгоритм шифрования электронной подписи

Краткое содержание:

1. Разобраться с алгоритмом шифрования электронной подписи на примере одной задачи
2. Автоматизировать на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы

Практическая работа № 6

Тема: Шифр Цезаря

Цель: Изучить алгоритм шифрования Цезаря

Краткое содержание:

1. Разобраться с алгоритмом шифрования Цезаря
2. Автоматизировать на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы

Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.

Практическая работа № 7

Тема: Симметричное шифрование

Цель: Изучение алгоритма симметричного шифрования

Краткое содержание:

1. Алгоритм симметричного шифрования
2. Шифрование методом блочной перестановки.
3. Автоматизировать задачу шифрования в системе Lazarus шифра Гронсфельда.

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе.
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: представить листинг программ шифрования на одном из языков программирования методами Гронсфельда и Вижинера. Устная защита. Преподавателю сдать электронный вариант программы.

Практическая работа № 8

Тема: Асимметричное шифрование

Цель: Изучение алгоритма асимметричного шифрования

Краткое содержание:

1. Использование двух ключей: открытый и закрытый.
2. Электронная цифровая подпись с помощью шифра RSA.
3. Шифр Диффи-Хелмана

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: представить листинг программ шифрования на одном из языков программирования для шифров RSA, Диффи-Хелмана и Электронная цифровая подпись. Защитить устно. Преподавателю сдать электронный вариант программ шифрования.

Раздел 4. Защита компьютерных систем от вредоносных программ**Практическая работа № 9**

Тема: Методика использования антивирусных программ

Цель: Изучение интерфейса антивирусных программ

Краткое содержание:

1. Изучение функциональных возможностей антивирусной программы «Антивирус Касперского».
2. Проверка на вирус всех критических областей ПК.

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

5. Методические материалы, определяющие процедуры оценивания компетенции

5.1 Критерии оценивания качества выполнения лабораторного практикума

Оценка **«зачтено»** выставляется обучающемуся, если лабораторная работа выполнена правильно и обучающийся ответил на все вопросы, поставленные преподавателем на защите.

Оценка **«не зачтено»** выставляется обучающемуся, если лабораторная работа выполнена не правильно или обучающийся не проявил глубоких теоретических знаний при защите работы

5.2 Критерии оценивания качества устного ответа

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка **«хорошо»** – за твердое знание основного (программного) материала, за грамотные, без существенных неточностей ответы на поставленные вопросы.

Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала.

Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в материале, за незнание основных понятий дисциплины.

5.3 Критерии оценивания тестирования

При тестировании все верные ответы берутся за 100%.

90%-100% отлично

75%-90% хорошо

60%-75% удовлетворительно

менее 60% неудовлетворительно

5.4 Критерии оценивания результатов освоения дисциплины

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, содержащегося в основных и дополнительных рекомендованных литературных источниках, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы, за умение анализировать изучаемые явления в их взаимосвязи и диалектическом развитии, применять теоретические положения при решении практических задач.

Оценка **«хорошо»** – за твердое знание основного (программного) материала, включая расчеты (при необходимости), за грамотные, без существенных неточностей ответы на поставленные вопросы, за умение применять теоретические положения для решения практических задач.

Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала, за слабое применение теоретических положений при решении практических задач.

Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в расчетах, за незнание основных понятий дисциплины.