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

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Г.Ю. Нагорная
«30» 03 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в компьютерных системах

Уровень образовательной программы бакалавриат

Направление подготовки 01.03.04 Прикладная математика

Направленность (профиль) Прикладная математика

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 _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Кочкаров А.М.

г. Черкесск, 2022 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Защита информации в компьютерных системах» является формирование знаний о защите информации в компьютерных системах в области прикладной математики

При этом задачами дисциплины являются:

- ознакомление обучающихся с общими вопросами защиты информации;
- изучение 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 и 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 в компьютерных системах» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. В таблице 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	Численные методы Теория вероятностей и математическая статистика	Научно-исследовательская работа Преддипломная практика

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 01.03.04 Прикладная математика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	Индикаторы достижения компетенций
1	2	3	4
1.	ПК-3	ПК-3 - Способность ориентироваться в современных алгоритмах компьютерной математики, обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	ПК-3.1 Осуществляет выбор современных алгоритмов компьютерной математики с целью дальнейшей реализации таких алгоритмов в виде прикладных программ или прикладных комплексов ПК-3.2 Способен практически реализовать алгоритм компьютерной математики для дальнейшей автоматизации решения прикладной задачи ПК-3.3 Способен осуществлять оптимизацию алгоритмов при создании прикладных программ или прикладных комплексов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды работы

Очная форма обучения

Вид учебной работы		**Всего часов**	**Семестр**
			№ 7 часов
1		2	3
Аудиторная контактная работа (всего)		**44**	**44**
В том числе:			
Лекции (Л)		**14**	**14**
Практические занятия (ПЗ)			
Лабораторные работы (ЛР)		**30**	**30**
Контактная внеаудиторная работа, в том числе индивидуальные и групповые консультации		**2**	**2**
в том числе индивидуальные и групповые консультации		**2**	**2**
Самостоятельная работа обучающегося (СРО) (всего)		**62**	**62**
Подготовка к лабораторным работам (ЛР)		10	10
Работа с книжными источниками		10	10
Работа с электронными источниками		30	30
Подготовка к тестированию		8	8
Самоподготовка		4	4
Промежуточная аттестация	Экзамен	**Экзамен**	**Экзамен**
	Консультация, час	**2**	**2**
	Прием **Экз**	**0,5**	**0,5**
	Контроль	**33,5**	**33,5**
ИТОГО:	**часов**	**144**	**144**
Общая трудоемкость	**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 (ОФО)
		Л	ЛР	ПЗ	СРО	всего	
1	2	3	4	5	6	7	8
Семестр 7							
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	2	8		16	26	Тестовый контроль, контрольные вопросы; лабораторная работа
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	2	8		16	26	тестовый контроль, контрольные вопросы; лабораторная работа
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	6	8		16	30	тестовый контроль, контрольные вопросы; лабораторная работа
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4	6		14	24	тестовый контроль, контрольные вопросы; лабораторная работа
	Контактная внеаудиторная работа и консультация					2	индивидуальные и групповые консультации.
	Промежуточная аттестация					**36**	**Экзамен**
Итого часов в 7 семестре:		**14**	**30**		**62**	**144**	
Всего часов:							

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов (ОФО)
1	2	3	4	5
Семестр 7				
1.	Раздел 1. Технология 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.	2
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. Порядок доступа в помещения различных категорий персонала. Контрольно-пропускные пункты. Системы контроля доступа. Аутентификация пользователей на основе паролей и модели «рукопожатия». Аутентификация пользователей по биометрическим характеристикам, клавиатурному почерку и росписи мышью.	
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.	6
		3.2 Основные понятия криптологии	Шифрование. Симметричные и асимметричные криптосистемы. Абсолютно стойкий шифр. Хеширова-	

			ние. Криптографическая система DES и ее модификация. Криптографическая система ГОСТ 28147-89.	
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1 Вредоносные программы	Классификация вредоносных программы. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.	2
		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	2
Итого часов в 7 семестре:				**14**
Всего:				**14**

4.2.3. Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Наименование лабораторной работы	Содержание лабораторной работы	Всего часов (ОФО)
1	2	3	4	5
Семестр 7				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1 Комплексный подход к обеспечению информационной безопасности	Ознакомление с комплексом профилактических мероприятий для ПК. Дефрагментация и очистка диска. Определение уровня доступа к информации.	4
		1.2 Межсетевые экраны	Инсталляция межсетевых экранов. Система VPN для безопасного подключения сети Интернет. Освоение технологию системного администрирования при создании локальных учетных записей пользователей и групп в ОС Windows	4

2.	Раздел 2. Методы защиты информации от несанкционированного доступа	2.1 Обеспечение безопасности операционных систем	Установка паролей пользователя и администрации. Аутентификация пользователей на основе паролей. Работа с консолью по управлению политикой безопасности IP	4
		2.2 Настройка программного генератора паролей	Создание генератора паролей в среде Lazarus.	4
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.	3.1. Теория чисел. Деление по модулю.	Шифрование открытого текста файла методом гаммирования.	4
		3.2 Криптографические системы	Асимметричная криптосистема RSA, Хеллмана и Эль-Гамаля. Функция Эйлера	2
		3.3 Создание и передача криптографических ключей.	Освоение криптосистемы с общим ключом. Ключевой обмен Диффи-Хелмана.	2
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1 Антивирусные программы	Анализ и исследование антивирусных программ. Проверка выбранных объектов. Обновление баз и модулей приложения. Вывод на экран текущего статуса компонента, обеспечивающего защиту файловой системы ПК от заражения	4
		4.2 Политика безопасности в КС. Уровни доступа к информации для пользователей	Определение свойств и состава группы пользователей, назначение полномочий. Определение прав доступа к информации.	2
Итого часов 7 семестре:				**30**
Всего:				**30**

4.3. Самостоятельная работа обучающегося

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего Часов (ОФО)
1	3	4	5	6
Семестр 7				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1	Работа с основной и дополнительной литературой. Чтение конспекта лекций. Подготовка к лабораторному практикуму.	16
2.	Раздел 2. Методы защиты	2.1	Проработка лекций, работа с учебниками.	

	информации от несанкционированного доступа		Подготовка к лабораторному практикуму.	16
		2.2	Изучение конспекта лекций. Выполнения индивидуальных заданий по лабораторному практикуму.	
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 хакерства	16
		3.2	Изучение конспекта лекций для выполнения практической и лабораторной работы	
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1	Изучение конспекта лекций для выполнения практической и лабораторной работы.	14
		4.2	Изучение конспекта лекций. Выполнения индивидуальных заданий по лабораторному практикуму.	
Итого часов в 7 семестре:				**62**
Всего:				**62**

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 (не предусмотрен учебным планом)

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 требования: 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.

5.5 Методические указания по подготовке к тестированию

Успешное выполнение тестовых заданий является необходимым условием для закрепления изученного материала. Тестовые задания подготовлены на основе лекционного материала, учебников и учебных пособий по дисциплине, изданных за последние 5 лет. Форма изложения тестовых заданий позволяет закрепить и восстановить в памяти пройденный материал. Предлагаемые тестовые задания охватывают узловые вопросы теоретических и практических основ по дисциплине. Для формирования заданий использована закрытая и открытая формы вопросов. У обучающегося есть возможность выбора правильного ответа или нескольких правильных ответов из числа предложенных вариантов. А в вопросах открытой формы дополнить самостоятельно. Для выполнения тестовых заданий обучающиеся должны изучить лекционный материал по теме, соответствующие разделы учебников, учебных пособий и других литературных источников. Репетиционные тестовые задания содержатся в рабочей учебной программе дисциплины. С ними целесообразно ознакомиться при подготовке к контрольному тестированию.

Промежуточная аттестация

По итогам 7 семестра проводится экзамен. При подготовке к сдаче экзамена рекомендуется пользоваться материалами практических занятий и материалами, изученными в ходе текущей самостоятельной работы. Экзамен проводится в устной форме, включает подготовку и ответы обучающегося на теоретические вопросы. По итогам выставляется оценка.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	№ семестра	Виды учебной работы	Образовательные технологии	Всего часов (ОФО)
1	2	3	4	5
1	7	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 7 семестре:				**14**
Всего:				**14**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

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

Дополнительная литература

1. 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
2. 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
3. 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
4. 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»

http:// fcior.edu.ru - Федеральный центр информационно-образовательных ресурсов;
http://elibrary.ru - Научная электронная библиотека.

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 5. Visio 2007, 2010, 2013 6. Project 2008, 2010, 2013 7. Access 2007, 2010, 2013 и т. д.	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022 (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 № 8DVG-V96F-H8S7-NRBC Срок действия: с 20.10.2022 до 22.10.2023
Цифровой образовательный ресурс IPRsmart	Лицензионный договор № 10423/23П от 30.06.2023 г. Срок действия: с 01.07.2023 г. до 01.07.2024г.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

1. Учебная аудитория для проведения занятий лекционного типа
Специализированная мебель:
Кафедра настольная - 1шт., парты - 31шт., стулья - 54шт., доска меловая - 1шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Проектор Benq – 1 шт.
Экран рулонный настенный – 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
Специализированная мебель:
Парты - 8шт., стулья - 22шт., стол преподавательский -1шт., доска меловая - 1шт., компьютерные столы - 8 шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Компьютер в сборе -7 шт.
Настенный экран – 1 шт.
Проектор -1 шт.
Ноутбук – 1шт.

3.Лаборатория компьютерной графики
Специализированная мебель:
Стол преподавательский - 1шт., 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.

4.Лаборатория синергетики и фракталов
Специализированная мебель:
Стол преподавательский - 1шт., стул мягкий - 1шт., доска меловая - 1шт., парты - 10шт., компьютерные столы - 11шт., стулья - 21 шт.,
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Персональный компьютер – 11шт.
Экран рулонный настенный – 1 шт.
Проектор – 1 шт.

5. Помещение для самостоятельной работы.
Отдел обслуживания печатными изданиями
Специализированная мебель:Рабочие столы на 1 место – 21 шт.Стулья – 55 шт. Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации: экран настенный – 1 шт.
Проектор – 1шт. Ноутбук – 1шт.
Информационно-библиографический отдел.
Специализированная мебель:

Рабочие столы на 1 место - 6 шт. Стулья - 6 шт.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ФГБОУ ВО «СевКавГА»:
Персональный компьютер – 1шт. Сканер – 1 шт. МФУ – 1 шт. Отдел обслуживания электронными изданиями Специализированная мебель:
Рабочие столы на 1 место – 24 шт. Стулья – 24 шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации:
Интерактивная система - 1 шт. Монитор – 21 шт. Сетевой терминал -18 шт. Персональный компьютер -3 шт. МФУ – 2 шт. Принтер –1шт.

6. Помещение для хранения и профилактического обслуживания учебного оборудования.
Специализированная мебель: Шкаф – 1 шт., стул -2 шт., кресло компьютерное – 2 шт., стол угловой компьютерный – 2 шт., тумбочки с ключом – 2 шт. Учебное пособие (персональный компьютер в комплекте) – 2 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.

Приложение 1.

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ

Защита информации в компьютерных системах

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Защита информации в компьютерных системах

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-3	Способность ориентироваться в современных алгоритмах компьютерной математики, обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах

1. 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)**
	ПК-3
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. Индикаторы достижения компетенций, формируемых в процессе изучения дисциплины

ПК-3 Способность ориентироваться в современных алгоритмах компьютерной математики, обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах

Индикаторы достижения компетенции	**Критерии оценивания результатов обучения**				**Средства оценивания результатов обучения**	
	неудовлетв	**удовлетв**	**хорошо**	**отлично**	**Текущий контроль**	**Промежуточная аттестация**
ПК-3.1 Осуществляет выбор современных алгоритмов компьютерной математики с целью дальнейшей реализации таких алгоритмов в виде прикладных программ или прикладных комплексов	Допускает существенные ошибки в выборе современных алгоритмов компьютерной математики с целью дальнейшей реализации таких алгоритмов в виде прикладных программ или прикладных комплексов	Демонстрирует некоторые способности в знаниях языков программирования, выборе современных алгоритмов компьютерной математики с целью дальнейшей реализации таких алгоритмов в виде прикладных программ или прикладных комплексов	Демонстрирует в целом хорошие способности к выбору современных алгоритмов компьютерной математики с целью дальнейшей реализации таких алгоритмов в виде прикладных программ или прикладных комплексов.	Демонстрирует способность осуществлять выбор современных алгоритмов компьютерной математики с целью дальнейшей реализации таких алгоритмов в виде прикладных программ или прикладных комплексов.	Текущий тестовый контроль, контрольные вопросы, лабораторная работа	Экзамен
ПК-3.2 Способен практически реализовать алгоритм компьютерной математики для дальнейшей автоматизации решения прикладной задачи	Имеет частично освоенное умение реализовать алгоритм компьютерной математики для дальнейшей автоматизации решения прикладной задачи	Демонстрирует в целом удовлетворительные, но не систематизированные умения реализовать алгоритм компьютерной математики для дальнейшей автоматизации решения прикладной задачи.	Демонстрирует в целом хорошие, но содержащие отдельные пробелы: реализовать алгоритм компьютерной математики для дальнейшей автоматизации решения прикладной задачи	Демонстрирует умения реализовать алгоритм компьютерной математики для дальнейшей автоматизации решения прикладной задачи	Текущий тестовый контроль, контрольные вопросы, лабораторная работа	Экзамен
ПК-3.3 Способен осуществлять оптимизацию алгоритмов при создании прикладных программ или прикладных комплексов	Фрагментарно владеет некоторыми современными языками программирования для оптимизации алгоритмов при создании прикладных программ или прикладных комплексов	Владеет отдельными навыками оптимизации алгоритмов при создании прикладных программ или прикладных комплексов	Демонстрирует в целом успешные знания по современным языкам программирования, оптимизации алгоритмов при создании прикладных программ или прикладных комплексов.	Демонстрирует профессиональные навыки оптимизации алгоритмов при создании прикладных программ или прикладных комплексов	Текущий тестовый контроль, контрольные вопросы, лабораторная работа	Экзамен

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к экзамену

по дисциплине Защита информации в компьютерных системах

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. Организация базы учетных записей пользователей в ОС Windows
6. Способы аутентификации пользователей.
7. Аутентификация пользователей на основе паролей и модели «рукопожатия».
8. Программно-аппаратная защита от локального несанкционированного доступа.
9. Аутентификация пользователей на основе их биометрических характеристик.
10. Протоколы прямой аутентификации.
11. Протоколы непрямой аутентификации.
12. Разграничение прав пользователей в ОС Windows.
13. Дискреционное, мандатное и ролевое разграничение доступа к объектам.
14. Подсистема безопасности ОС Windows.
15. Разграничение доступа к объектам в ОС Windows.
16. Средства защиты информации в глобальных компьютерных сетях.
17. Стандарты оценки безопасности компьютерных систем
18. Элементы теории чисел.
19. Способы симметричного шифрования. Абсолютно стойкий шифр.
20. Генерация, хранение и распространение ключей.
21. Криптографическая система ГОСТ 28147-89.
22. Применение и обзор современных симметричных криптосистем.
23. Принципы построения, свойства и применение асимметричных криптосистем.
24. Криптографическая система RSA.
25. Криптографические системы Диффи-Хеллмана, Эль-Гамаля
26. Электронная цифровая подпись и ее применение.
27. Принципы построения систем защиты от копирования.
28. Защита инсталляционных дисков и установленного программного обеспечения.
29. Защита программных средств от изучения.
30. Вредоносные программы, их признаки и классификация.
31. Программные закладки и защита от них.
32. Методы обнаружения и удаления вредоносных программ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Кафедра Математики

20__ - 20__ учебный год

Экзаменационный билет № **1**

по дисциплине Защита информации в компьютерных системах

для обучающихся направления подготовки 01.03.04 Прикладная математика

1. Проблема защиты информации и подходы к ее решению.
2. Основные понятия защиты информации.

Зав. кафедрой Кочкаров А.М.

Контрольные вопросы к разделам

по дисциплине Защита информации в компьютерных системах

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?
17. Какие правила применяются при предоставлении доступа субъекта к объекту в соответствии с мандатным управлением доступом к объектам КС? В чем их смысл?

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-Гамаля?

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?

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 копирования?

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 в компьютерных системах

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, хранимая 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. Кодируемость, 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-технической 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

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 утвержденные 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_____

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 Mamory, 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 Mamory, 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_____

17. **В основе работы протокола S/Key лежит протокол PAP для _____**

18. Протокол CHAP основан на модели _____

19. Протокол Kerberos предназначен для_____

20. Применяемые разновидности межсетевых экранов

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

21. VPN предназначены_____

22. Дстоинства 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 _____

26. Редактор системных правил Windows называется

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

28. Достоинства дискреционного управления доступом к объектам КС

1. простота идентификации, возможность описания пользователем доступ к своим ре-

сурсам

2. детализированность и назначение прав доступа

3. простата реализации доступом к объектам КС и гибкость

4. простота администрирования и гибкость

29. Достоинства мандатного управления доступом к объектам КС

1. простата построения общей схемы доступа и простата 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 <u>a</u> 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. Количество ключей, применяемое в симметричном шифровании _____

33. Основные способы, которые 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

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. К асимметричным криптографическим системам относятся

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

37. 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

38. 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

Раздел 4. Защита компьютерных систем от вредоносных программ

39. В операционной системе обеспечиваются аутентичность и целостность криптопровайдера

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

40 По способу распространения в КС подразделяются вирусы на

1.паразитические
2.загрузочные
3.файловые
4.ссылки

41.Вредоносные программы – это_____

42. Вирус, который внедряется в исполняемые файлы и при их запуске_____

Комплект заданий для лабораторной работы

по дисциплине Защита информации в компьютерных системах

Лабораторная работа № 1
Тема: Комплексный подход к обеспечению информационной безопасности
Цель: Определение защищенности ОС и ПК в целом
Краткое содержание:
1. Ознакомление с комплексом профилактических мероприятий для ПК.
2. Дефрагментация и очистка диска.
3. Определения уровня доступа к информации
4. Используя программу «Сведения о системе» определить параметры ПК: сведения о портах, звуковом устройстве, о системных драйверах, автоматически загружаемых программах
5. Изучение консоля управления ОС Windows

Рекомендации по организации самостоятельной работы:
- изучение описания лабораторной работы
- изучение задания к лабораторной работе
- изучение панелей инструментов, предусмотренных заданиями к лабораторной работе
- изучение электронных источников по теме лабораторной работы.

Содержание отчёта:
подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 2
Тема: Межсетевые экраны
Цель: Научиться инсталлировать межсетевые экраны
Краткое содержание:
1. Инсталляция межсетевых экранов.
2. Система VPN для безопасного подключения сети Интернет
3. Установка паролей на пользователя
4. Работа с консолью по управлению политикой безопасности IP

Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи
- изучение задания к лабораторной работе
- изучение электронных источников по теме лабораторной работы.

Содержание отчёта:
подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 3
Тема Обеспечение безопасности операционных систем
Цель: Освоение стандартных средств ОС Windows обеспечения ИБ
Краткое содержание:
1. Аутентификация пользователей на основе паролей.
2. Установка паролей пользователя и администрации.
3.Архивация данных компьютера. Резервное копирование.
4. Изучение программы восстановления информации на носителях.

5. Освоение технологии системного администрирования при создании локальных учетных записей пользователей и групп в ОС Windows

Рекомендации по организации самостоятельной работы:

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

Содержание отчёта:

подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 4

Тема: Настройка программного генератора паролей

Цель: Научиться создавать в системе Lazarus генератора паролей

Краткое содержание:

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

Рекомендации по организации самостоятельной работы:

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

Содержание отчёта:

подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 5

Тема: Создание и передача криптографических ключей.

Цель: Освоить метод шифрования Диффи-Хелмана.

Краткое содержание:

1. Создание ключей для обмена.
2. Ключевой обмен Диффи-Хелмана.
3.Написать программу на одном из языков программирования метода шифрования Диффи-Хелмана

Рекомендации по организации самостоятельной работы:

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

Содержание отчёта:

подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 6

Тема: Криптографические системы

Цель: Изучение криптографической системы RSA

Краткое содержание:

1. Изучение алгоритма асимметричной криптосистемы RSA
2. Функция Эйлера
3. Работа в Lazaruse по программированию криптосистемы RSA

Рекомендации по организации самостоятельной работы:

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

Содержание отчёта:
подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 7
Тема: Криптографические системы
Цель: Изучение алгоритма Эль-Гамаля.

Краткое содержание:
1. Алгоритм Эль-Гамаля. Решение задачи.
2. Работа в системе Lazarus по программированию криптосистемы Эль-Гамаля

Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи
- изучение задания к лабораторной работе
- изучение электронных источников по теме лабораторной работы.

Содержание отчёта:
подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 8
Тема: Антивирусные программы
Цель: Анализ и исследование антивирусных программ. Изучение действие вирусов различного типа.

Краткое содержание:
1. Выход на сайт Касперского
2. Ознакомиться детально с антивирусной программой Касперского
3. Настройка всех компонентов под нужды конкретного пользователя
4. Задать расписание работы антивирусной программы
5. Проверка выбранных объектов.
6. Обновление баз и модулей приложения.
7. Вывод на экран текущего статуса компонента, обеспечивающего защиту файловой системы ПК от заражения
8. Запуская поочередно программы из пакета демонстрационных программ, изучить проявление вирусного заражения. По окончании наблюдения перезагрузить компьютер.

Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи
- изучение задания к лабораторной работе
- изучение электронных источников по теме лабораторной работы.

Содержание отчёта:
подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной работы.

Лабораторная работа № 9
Тема: Политика безопасности в КС. Уровни доступа к информации для пользователей
Цель: Определение уровня доступа пользователей к данным

Краткое содержание:
1. Определение свойств и состава группы пользователей, назначение полномочий.
2. Определение прав доступа к информации
3. Пароль администратора

Рекомендации по организации самостоятельной работы:

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

Содержание отчёта:

подготовка отчета в соответствии с заданием к лабораторной работе.

Форма отчёта: устная защита лабораторной 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 на контрольные вопросы

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 на экзамен

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 постав-

ленные 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.