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

Информационная безопасность и защита информации

Уровень образовательной программы бакалавриат

Направление подготовки 09.03.04 Программная инженерия

Направленность (профиль) Программная инженерия

Форма обучения очная

Срок освоения ОП 4 года

Институт Прикладной математики и информационных технологий

Кафедра разработчик РПД Прикладная информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института ПМ и ИТ _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Хапаева Л.Х.

г. Черкесск, 2022 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность и 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, также основы стандартов жизненного цикла ПО.

При этом ***задачами*** дисциплины являются:

- 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, методов идентификации пользователей, методов защиты программ от вирусов;
- изучение криптографических методов защиты информации в компьютерных системах
- оценка защищенности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Информационная безопасность и защита информации» относится к части, формируемой участниками образовательных отношений 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	Архитектура вычислительных систем	Производственная практика (преддипломная практика)
	Анализ данных и машинное обучение	
	Теория языков программирования и методы трансляции	

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 09.03.04. Программная инженерия и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:
1	2	3	4
1	ПК-4	Способен использовать концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), стандарты и модели жизненного цикла, в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	ПК-4.1. Использует основные концепты стандартов жизненного цикла ПО, основы стандартов жизненного цикла ПО, методы использования стандартов и модели жизненного цикла ПО ПК-4.2. Использует основные технологии защиты информации; применяет основы разработки программного обеспечения ПК-4.3. Использует навыки анализа возможностей реализации требований к программному обеспечению, для оценки безопасности, надежности и удобства использования.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды учебной работы

Вид учебной работы		**Всего часов**	**Семестры**	
			№ 7 часов	**№8 часов**
1		2	3	4
Аудиторная контактная работа (всего)			42	50
В том числе:				
Лекции (Л)		24	14	10
Практические занятия (ПЗ)				
Лабораторные работы (ЛР)		68	28	40
Контактная внеаудиторная работа, в том числе		3,4	1,7	1,7
Индивидуальные и групповые консультации		3,4	1,7	1,7
Самостоятельная работа обучающихся (СРО) (всего)		129	64	65
Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса		60	30	30
Выполнение и подготовка к защите лабораторной и контрольной работам		20	10	10
Работа с электронным портфолио		20	10	10
Подготовка к тестированию		20	10	10
Промежуточная аттестация	Зачет (З) **в том числе:**	3	3	-
	Прием зач., час.	0,6	0,3	0,3
	Экзамен (Э) **в том числе:**	**Э (24,5)**	-	**Э (24,5)**
	Прием экз., час.	0,5		0,5
	Консультация, час.	2		2
	СРО, час.	22		22
ИТОГО: Общая трудоемкость	**часов**	**252**	**108**	**144**
	зач. ед.	**7**	**3**	**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	всего	
1	2	3	4	5	6	7	8
Семестр 7							
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	8	16		34	58	устный опрос, тестирование, лабораторные работы, контрольная работа
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	6	12		30	48	устный опрос, тестирование, лабораторные работы
3.	Контактная внеаудиторная работа					1,7	индивидуальные и групповые консультации
4.	Промежуточная аттестация					0,3	зачет
Итого часов в 7 семестре:		**14**	**28**		**64**	**108**	
Семестр 8							
5.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	4	20		30	54	устный опрос, тестирование, лабораторные работы
6.	Раздел 4. Защита компьютерных систем от вредоносных программ	6	20		35	61	тестирование
7.	Контактная внеаудиторная работа					2	индивидуальные и групповые консультации
8.	Промежуточная аттестация					27	экзамен
Итого часов в 8 семестре:		**10**	**40**		**65**	**144**	
Всего:		**24**	**68**		**129**	**252**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов
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.	8
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.	6
		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.	
Итого часов в 7 семестре:				**14**
Семестр 8				
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	Шифрование. Симметричные и асимметричные криптосистемы. Абсолютно стойкий шифр. Хеширование.	2

			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	4
Итого часов в 8 семестре:				**10**
Всего:				**24**

4.2.3. Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Наименование лабораторной работы	Содержание лабораторной работы	Всего часов
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.	8
		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	8

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	12
Итого часов в 7 семестре:				**28**
Семестр 8				
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.	3.1 Настройка программного генератора паролей.	Создание генератора паролей в среде Lazarus. Шифрование открытого текста файла методом гаммирования.	10
		3.2 Создание и передача криптографических ключей.	Освоение криптосистемы с общим ключом. Ключевой обмен Диффи-Хелмана.	8
		3.3 Криптографические системы	Асимметричная криптосистема RSA, Хеллмана и Эль-Гамаля. Функция Эйлера	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	10
		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.	10
Итого часов в 8 семестре:				**40**
Всего:				**68**

4.2.4. Практические занятия *(не предусмотрены учебным планом)*

4.3. Самостоятельная работа обучающего

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов
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.	34
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	2.1.	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	30
		2.2.	Выполнение и подготовка к защите практической работы	
		2.3.	Подготовка к текущему контролю (Тестовый контроль)	
		2.4.	Составление тематического портфолио	
Итого часов в 7 семестре:				**64**
Семестр 8				
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.	3.1	Защита контрольной работы, презентация работ	30
		3.2	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	
		3.3.	Выполнение и подготовка к защите практической работы	
		3.4.	Подготовка к текущему контролю (Тестовый контроль,)	
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4.1	Изучение конспекта лекций для выполнения практической.	35
		4.2	Изучение конспекта лекций. Выполнения индивидуальных заданий по лабораторному практикуму.	
Итого часов в 8 семестре:				**65**
Всего:				**129**

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

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

Лекция является исходной формой всего учебного процесса, играет направляющую и организующую роль в изучении предмета. Важнейшая роль лекции заключается в личном воздействии лектора на аудиторию.

Изучение дисциплины «Информационная безопасность и защита информации» требует систематического и последовательного накопления знаний по защите информации, следовательно, пропуски отдельных тем не способствуют глубокому пониманию и освоению этого предмета. Именно поэтому необходим систематический контроль преподавателя над вниманием и работой обучающихся во время лекции.

Перед первой лекцией приводится список основной и рекомендуемой литературы. Рекомендуется заострить внимание обучающихся на то, какие знания, умения и навыки приобретут после прослушивания соответствующей темы лекции.

Лектор должен сообщить чётко, ясно, не торопясь, название темы лекции, дать возможность обучающимся записать его. Сказать о значимости данной темы и сообщить о распределении времени на тему. Если не первая лекция по теме, то провести связь с предшествующей лекцией. Перед изложением каждого вопроса эту связь надо называть, и завершить рассмотрение вопроса небольшим выводом.

Большую помощь в обобщении и фиксировании материала оказывает сопровождение объяснения демонстрацией материала с помощью мультимедиа аппаратуры.

Начало лекции имеет большое значение для установления контакта с аудиторией, для вызова у слушателей интереса к теме. В этих целях можно подчеркнуть теоретическое и практическое значение данной темы.

Одним из сложных вопросов методики чтения лекции является обращение с текстом. Привязанность к тексту вследствие плохой подготовки, недостаточного владения материалом приводит к ослаблению связи с аудиторией. В то же время не следует, не владея соответствующими навыками, пытаться проводить лекцию без текста, по памяти. При этом допускаются ошибки, повторения, ослабление логической связи рассуждения, пропуски отдельных важных положений темы и т.п.

В заключительной части лекции следует провести обобщение наиболее важных вопросов лекции, сделать выводы и поставить задачи для самостоятельной проработки некоторых вопросов. Также рекомендуется в конце лекции оставлять несколько минут для ответов на вопросы.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

Ведущей дидактической целью лабораторных занятий является систематизация и обобщение знаний по изучаемой теме, приобретение практических навыков по тому или другому разделу курса, закрепление полученных теоретических знаний. Лабораторные работы сопровождают и поддерживают лекционный курс.

Количество лабораторных работ строго соответствует содержанию курса. Каждая лабораторная предусматривает получение практических навыков по лекционным темам дисциплины «Информационная безопасность и защита информации».

В начале каждого лабораторного занятия кратко приводится теоретический материал, необходимый для выполнения текущей лабораторной работы.

Каждая лабораторная работа содержит список индивидуальных заданий.

Полученные результаты выполнения лабораторной работы оформляется и защищается устно обучающимся.

При проведении промежуточной и итоговой аттестации обучающихся важно всегда помнить, что систематичность, объективность, аргументированность – главные принципы, на которых основаны контроль и оценка знаний обучающихся.

5.3. Методические указания для подготовки обучающихся к практическим занятиям (не предусмотрено 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 обучающим 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 на лабораторных и консультациях неясные вопросы;
-при подготовке к зачету параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на плановых консультациях.

Промежуточная аттестация

По итогам 7 семестра проводится зачет, по итогам 8 семестра проводится экзамен. При подготовке к сдаче экзамена рекомендуется пользоваться материалами лабораторных занятий и материалами, изученными в ходе текущей самостоятельной работы.

Экзамен проводится в устной форме, включает подготовку и ответы обучающегося на теоретические вопросы. По итогам экзамена выставляется оценка.

По итогам обучения проводится экзамен, к которому допускаются обучающиеся, имеющие положительные результаты по защите лабораторных работ.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4
Семестр 8			
1.	3.2 Создание и передача криптографических ключей.	*Командная и групповая работа по индивидуальным заданиям лабораторного практикума с применением компьютерных технологий*	2
2.	3.1 Симметричное шифрование	*Устный контроль по вопросам раздела. Практическое закрепление тем раздела на примерах задач практикума.*	2
3.	3.2 Асимметричное шифрование	*Лабораторная работа, презентация.*	2
4.	4.1 Методика использования антивирусных программ	*Лабораторная работа, презентация.*	2
Итого часов в 8 семестре:			**10**
Всего:			**10**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1. Перечень основной учебной литературы

Список основной литературы	
1.	Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33857.html
2.	Смышляев, А. Г. Информационная безопасность. Лабораторный практикум : учебное пособие / А. Г. Смышляев. — Белгород : Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66655.html
3.	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html
Список дополнительной литературы	
1.	Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.- 324 с.
2.	Горев, А. И. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 с. — ISBN 978-5-88651-642-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/72856.html
3.	Информационная безопасность и защита информации : учебно-методический комплекс / составители С. А. Омарова, К. А. Искакова, Н. А. Тойганбаева. — Алматы : Нур-Принт, 2012. — 98 с. — ISBN 9965-756-05-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/67055.html
4.	Корнеев, И.К. Защита информации в офисе [Текст]: учебник/ И.К. Корнеев, Е.А. Степанов.- М.: ТК Велби, Проспект, 2010.- 336 с.
5.	Куприянов, А.И. Основы защиты информации [Текст]: учеб. пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов.- М.: Академия, 2008.- 256 с.
6.	Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст]: учеб. пособие для студ. высш. учеб. заведений/ П.Б. Хорев - М.: Академия, 2008.- 256 с.

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»
http://elibrary.ru - Научная электронная библиотека.

7.3. Информационные технологии, лицензионное программное обеспечение
В компьютерном классе должны быть установлены средства:

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: 30.06.2022 (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
Консультант Плюс	Договор № 272-186/С-23-01 от 20.12.2022 г.
ЭБС IPR SMART	Лицензионный договор № 9368/22П от 01.07.2022 г. Срок действия: с 01.07.2022 до 01.07.2023
Бесплатное ПО: OpenServer, Notepad ++, MySQL, Sumatra PDF	

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:
Парты - 10шт., стулья - 29шт.; доска меловая - 1шт., кафедра настольная - 1шт., стул мягкий - 1шт., компьютерные столы-12шт.,
стол однотумбовый (преподавательский) -1шт.,
шкаф двухдверный - 1шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации:
Интерактивная доска- 1шт.
Проектор - 1шт.
Ноутбук - 1шт.
ПК- 10шт.

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 - 5шт., стулья - 26шт., доска - 1шт., лаб. столы - 6шт., стол преподавательский - 2шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
ПК – 10 шт.

4. Помещение для самостоятельной работы.
Библиотечно-издательский центр.
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.

8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся

1. Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.
2. Рабочие места обучающихся, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ Информационная безопасность и защита информации

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Информационная безопасность и защита информации

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-4	Способен использовать концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), стандарты и модели жизненного цикла, в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества

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) 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-4
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

ПК-4 Способен использовать концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), стандарты и модели жизненного цикла, в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества						
Индикаторы достижения компетенции	**Критерии оценивания результатов обучения**				**Средства оценивания результатов обучения**	
		неудовлетв	**удовлетв**	**хорошо**	**Текущий контроль**	**Промежуточная аттестация**
1	**2**	**3**	**4**	**5**	**6**	**7**
ПК-4.1. Использует основные концепты стандартов жизненного цикла ПО, основы стандартов жизненного цикла ПО, методы использования стандартов и модели жизненного цикла ПО	Не знает и не использует основные концепты стандартов жизненного цикла ПО, основы стандартов жизненного цикла ПО, методы использования стандартов и модели жизненного цикла ПО	Частично использует основные концепты стандартов жизненного цикла ПО, основы стандартов жизненного цикла ПО, методы использования стандартов и модели жизненного цикла ПО	Использует основныеконцепты стандартов жизненного цикла ПО, основы стандартов жизненного цикла ПО, методы использования стандартов и модели жизненного цикла ПО	Успешно использует основные концепты стандартов жизненного цикла ПО, основы стандартов жизненного цикла ПО, методы использования стандартов и модели жизненного цикла ПО	Лабораторные работы, Устный опрос Тестирование, контрольная работа	Зачет, экзамен
ПК-4.2. Использует основные технологии защиты информации; применяет основы разработки программного обеспечения	Не умеет и не готов использовать основные технологии защиты информации; применяет основы разработки программного обеспечения	Не использует основные технологии защиты информации; применяет основы разработки программного обеспечения	Умеет частично использовать основные технологии защиты информации; применяет основы разработки программного обеспечения	Готов и умеет использовать основные технологии защиты информации; применяет основы разработки программного обеспечения		
ПК-4.3. Использует навыки анализа возможностей реализации требований к программному обеспечению, для оценки безопасности, надежности и удобства использования.	Не владеет навыками анализа возможностей реализации требований к программному обеспечению, для оценки безопасности, надежности и удобства использования.	Частично владеет навыками анализа возможностей реализации требований к программному обеспечению, для оценки безопасности, надежности и удобства использования.	Владеет навыками анализа возможностей реализации требований к программному обеспечению, для оценки безопасности, надежности и удобства использования.	Отлично владеет навыками анализа возможностей реализации требований к программному обеспечению, для оценки безопасности, надежности и удобства использования.		

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к зачету

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

Вопросы к экзамену

по дисциплине Информационная безопасность и 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.
5. Правовое обеспечение защиты информации.
6. Способы нарушения защищенности информации и защиты от него в компьютерных системах.
7. Организация базы учетных записей пользователей в ОС Windows
8. Способы аутентификации пользователей.
9. Аутентификация пользователей на основе паролей.
10. Аутентификация пользователей на основе модели «рукопожатия».
11. Программно-аппаратная защита от локального несанкционированного доступа.
12. Аутентификация пользователей на основе их биометрических характеристик.
13. Протоколы прямой аутентификации.
14. Протоколы непрямой аутентификации.
15. Виртуальные частные сети.
16. Разграничение прав пользователей в ОС Windows.
17. Дискреционное, мандатное и ролевое разграничение доступа к объектам.
18. Подсистема безопасности ОС Windows.
19. Разграничение доступа к объектам в ОС Windows.
20. Средства защиты информации в глобальных компьютерных сетях.
21. Стандарты оценки безопасности компьютерных систем и информационных технологий.
22. Элементы теории чисел.
23. Способы симметричного шифрования.
24. Абсолютно стойкий шифр.
25. Генерация, хранение и распространение ключей.
26. Криптографическая система DES и ее модификации.
27. Криптографическая система ГОСТ 28147-89.
28. Применение и обзор современных симметричных криптосистем.
29. Принципы построения, свойства и применение асимметричных криптосистем.
30. Криптографическая система RSA.
31. Криптографические системы Диффи-Хеллмана, Эль-Гамаля и эллиптических кривых.
32. Электронная цифровая подпись и ее применение. Функции хеширования.
33. Принципы построения систем защиты от копирования.
34. Защита инсталляционных дисков и установленного программного обеспечения.
35. Защита программных средств от изучения.
36. Вредоносные программы, их признаки и классификация.
37. Программные закладки и защита от них.
38. Методы обнаружения и удаления вредоносных программ
39. Угрозы конфиденциальности СУБД и способы противодействия.
40. Основные механизмы управления СУБД (транзакция, блокировки, ссылочная целостность, правила – триггеры).
41. Мониторинг серверов СУБД.
42. Криптографические методы защиты баз данных.

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Экзаменационный билет № **_1___**

по дисциплине Информационная безопасность и защита информации
для обучающихся направления подготовки ___*09.03.04 Программная инженерия*

1. Угрозы безопасности и каналы утечки информации
2. Криптографическая система DES и ее модификации.

3.Зашифруйте следующий текст методом замена: «Изучение методов шифрования/расшифрования перестановкой символов».

Зав. кафедрой Хапаева Л.Х.

Контрольная работа

по дисциплине Информационная безопасность и защита информации

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?

Вопросы к устному опросу

по дисциплине Информационная безопасность и 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?
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?

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?

10. Как происходит заражение и функционирование загрузочных вирусов?

11. Какие типы файлов могут заражаться файловыми вирусами?

12. Как происходит заражение программных файлов?

13. Почему файлы документов могут содержать вирусы?

14. 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 вопросы

по дисциплине Информационная безопасность и защита информации

1. 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.

2. Дайте определение защиты информации.

3. К основным характеристикам защищаемой информации относится
   1. Кодируемость, корректность, целостность
   2. Государственность, служебность, доступность
   3. Конфиденциальность, целостность и доступность
   4. Целостность, защищенность и доступность

4. Угроза безопасности информации_____
   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

5. Перечислите уровни правового обеспечения информационной безопасности

6. Перечислите инженерно-технической средства защиты информации

7. Дайте определение комплексной системы защиты информации.

8. 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

9. 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

10. 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»

11. Что относится к биометрическим характеристикам пользователей, которые могут применяться для их аутентификации

12. Двухфакторная аутентификация это

1. метод идентификации пользователя в каком-либо сервисе при помощи запроса всевозможных аутентификационных данных

2. система доступа, основанная на двух «ключах»: 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

13.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.)

14.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

15. Дополните предложение:

Протокол Kerberos предназначен для_____

16. Отметьте применяемые разновидности межсетевых экранов:

1.фильтрующие маршрутизаторы

2. шлюзы сеансового уровня

3.шлюзы прикладного уровня

4. все вышеперечисленные

17. VPN предназначены для _____

18.В чем достоинства и недостатки использования пароля программы BIOS Setup

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

1. *.pwl

2. *.scr

3. *.sys
4. *.pvl

20. 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

21. 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

22. В чем разница между симметричными и асимметричными криптографическими системами

23. Какие основные способы применяются при создании алгоритмов симметричной криптографии

24.Дополните предложение:
Разница между потоковыми и блочными шифрами состоит в том, что

25.Дополните предложение:
Идеальным (по К. Шеннону) шифром может считаться …

26.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

27.Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста:

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

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

1. сложная замена, гаммирования, гаммирования 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

29. 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

30. 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

31. Провайдеры криптографического обслуживания предоставляют услуги _____

32. На следующих принципах строится взаимодействие прикладной программы и криптопровайдера _____

33. Вставьте пропущенное слово:
В _____ модели жизненного цикла делается упор на начальные этапы: анализ и проектирование.

34. 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

35. Вирус внедряется в исполняемые файлы и при их запуске активируется

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

Задания для лабораторной работы

по дисциплине Информационная безопасность и защита информации

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:

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 лабораторных работ

Оценка **«зачтено»** выставляется обучающему, если лабораторная работа выполнена правильно и студент ответил на все вопросы, поставленные преподавателем на защите.
Оценка **«не зачтено»** выставляется обучающему, если лабораторная работа выполнена не правильно или студент не проявил глубоких теоретических знаний при защите работы

5.2 Критерии оценивания качества устного опроса

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 зачете

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.

5.5.Критерии оценивания результатов освоения дисциплины(экзамен)

-оценка **«отлично»** выставляется обучающемуся 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 незнание основных понятий дисциплины.

5.6 Критерии оценивания контрольной работы

При проверке контрольной работы:
выполнено 5 заданий – отлично
выполнено 4 задания – хорошо
выполнено 2-3 задания – удовлетворительно
выполнено менее 2 заданий – неудовлетворительно