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
«31» марта 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Уровень образовательной программы бакалавриат

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль) Прикладная информатика в юриспруденции

Форма обучения очная (заочная)

Срок освоения ОП 4 года (4 года 9 месяцев)

Институт Прикладной математики и информационных технологий

Кафедра разработчик РПД Прикладная информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Хапаева Л.Х.

г. Черкесск, 2021 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность» является ознакомление обучающихся со стандартными задачами профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

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, методы идентификации пользователей, методы защиты программ от вирусов;
-изучение криптографических методов защиты информации в компьютерных системах
-оценивать защищенность компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Информационная безопасность» относится к обязательной части, 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.	Основы правовой информатики	Защита и обработка конфиденциальных документов
2.	Вычислительные системы, сети и телекоммуникации	
3.	Правоведение	

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 09.03.03 Прикладная информатика 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.	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИДК-ОПК-3.2 Применяет в практической деятельности знания основных требований информационной безопасности. ИДК-ОПК-3.3 Использует методы поиска и анализа информации для подготовки документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности. ИДК-ОПК-3.4 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы		**Всего часов**	**Семестр**
			№ 4 часов
1		2	3
Аудиторная контактная работа (всего)		54	54
В том числе:			
Лекции (Л)		18	18
Практические занятия (ПЗ), Семинары (С)		-	-
Лабораторные работы (ЛР)		36	36
Контактная внеаудиторная работа, в том числе:		2	2
Групповые и индивидуальные консультации		2	2
Самостоятельная работа обучающихся (СРО) (всего)		52	52
Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса		15	15
Выполнение и подготовка к защите лабораторной и контрольной работам		15	15
Работа с электронным портфолио		10	10
Подготовка к текущему контролю (Тестовый контроль)		12	12
Промежуточная аттестация	Экзамен(Э)	Э	Э
	экзамен (Э) **в том числе:**	36	36
	Прием экз., час.	0,5	0,5
	Консультация, час.	2	2
	СРО, час.	33,5	33,5
ИТОГО: Общая трудоемкость	**часов**	**144**	**144**
	зач. ед.	**4**	**4**

Заочная форма обучения

Вид учебной работы		Всего часов	Семестр
			№ 4 часов
1		2	3
Аудиторная контактная работа (всего)		8	8
В том числе:			
Лекции (Л)		4	4
Практические занятия (ПЗ), Семинары (С)		-	-
Лабораторные работы (ЛР)		4	4
Контактная внеаудиторная работа, в том числе:		1	1
Групповые и индивидуальные консультации		1	1
Самостоятельная работа обучающихся (СРО) (всего)		126	126
Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса		26	26
Просмотр и конспектирование видеолекций		25	25
Работа с электронным портфолио		25	25
Выполнение и подготовка к защите лабораторной и контрольной работам		25	25
Подготовка к текущему контролю (Тестовый контроль)		25	25
Промежуточная аттестация	Экзамен(Э)	Э	Э
	экзамен (Э) **в том числе:**	9	9
	Прием экз., час.	0,5	0,5
	СРО, час.	8,5	8,5
ИТОГО: Общая трудоемкость	**часов**	**144**	**144**
	зач. ед.	**4**	**4**

4.2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Очная форма обучения

№ 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 4							
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	4	8		12	24	устный опрос, компьютерное тестирование, отчет по лабораторной работе
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	4	6		15	25	устный опрос, компьютерное тестирование, отчет по лабораторной работе
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	6	12		15	33	устный опрос, компьютерное тестирование, отчет по лабораторной работе
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	4	10		10	24	устный опрос, компьютерное тестирование, отчет по лабораторной и контрольной работе
5.	Контактная внеаудиторная работа					2	групповые и индивидуальные консультации
6.	Промежуточная аттестация					36	Экзамен
Итого часов в 4 семестре:		**18**	**36**		**52**	**144**	
Всего:		**18**	**36**		**52**	**144**	

Заочная форма обучения

№ 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 4							
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	2	2		30	34	устный опрос, компьютерное тестирование, отчет по лабораторной работе, защита контрольной работы
2.	Раздел 2. Методы защиты информации от несанкционированного доступа				30	30	устный опрос, компьютерное тестирование, отчет по лабораторной работе, защита контрольной работы
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	2	2		32	36	самостоятельная работа, выполнение и защита контрольной работы
4.	Раздел 4. Защита компьютерных систем от вредоносных программ				34	34	устный опрос, компьютерное тестирование, отчет по лабораторной работе, защита контрольной работы
6.	Контактная внеаудиторная работа					1	групповые и индивидуальные консультации
7.	Промежуточная аттестация					9	Экзамен
Итого часов в 4 семестре:		**4**	**4**		**126**	**144**	
Всего:		**4**	**4**		**126**	**144**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
Семестр 4					
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.	4	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.	2	

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	2
		3.2 Основные понятия криптологии	Шифрование. Симметричные и асимметричные криптосистемы. Абсолютно стойкий шифр. Хеширование. Криптографическая система DES и ее модификация. Криптографическая система.	4	
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 4 семестре:				**18**	**4**
Всего:				**18**	**4**

4.2.3. Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Наименование лабораторного занятия	Содержание лабораторного занятия	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
Семестр 4					
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	2
		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	6	
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.	4	2
		3.2 Создание и передача криптографических ключей.	Освоение криптосистемы с общим ключом. Ключевой обмен Диффи-Хелмана.	4	
		3.3 Криптографические системы	Асимметричная криптосистема RSA, Хеллмана и Эль-Гамаля. Функция Эйлера	4	
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.	4	

			Вывод на экран текущего статуса компонента, обеспечивающего защиту файловой системы ПК от заражения		
		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.	6	
Итого часов в 4 семестре:				**36**	**4**
Всего:				**36**	**4**

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

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Очная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов ОФО
1	**2**	**3**	**4**	**5**
Семестр 4				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	12
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	15
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контрольта)	
		1.4	Составление тематического портфолио	
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	15
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	10
		1.2	Выполнение и подготовка к защите лабораторной и контрольной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
Итого часов в 4 семестре:				**52**
Всего:				**52**

Заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов ЗФО
1	**2**	**3**	**4**	**5**
Семестр 4				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	30
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
2.	Раздел 2. Методы защиты информации от несанкционированного доступа	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	30
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
3.	Раздел 3. Криптографические методы и средства обеспечения информационной безопасности	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	32
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
4.	Раздел 4. Защита компьютерных систем от вредоносных программ	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	34
		1.2	Выполнение и подготовка к защите лабораторной работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
Итого часов в 4 семестре:				**126**
Всего:				**126**

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

Обучение по учебной дисциплине «Информационная безопасность» предполагает изучение дисциплины на аудиторных занятиях и самостоятельную работу обучающихся. Основными видами выполнения аудиторной работы обучающихся по дисциплине являются лекции и лабораторные занятия.

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

С целью обеспечения успешного обучения, обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, знакомит с новым материалом, разъясняет учебные элементы, трудные для понимания, систематизирует учебный материал и ориентирует в учебном процессе. Подготовка к лекционному занятию включает выполнение всех видов заданий размещенных к каждой лекции, т.е. задания выполняются еще до лекционного занятия по соответствующей теме.

В ходе лекционных занятий рекомендуется вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. 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 - в ходе подготовки к лабораторный занятиям изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы. Подготовить тезисы для выступлений по всем учебным вопросам, выносимым на семинар. Готовясь к докладу или реферативному сообщению, обращаться за методической помощью к преподавателю. Составить план-конспект своего выступления. Продумать примеры с целью обеспечения тесной связи изучаемой теории с реальной жизнью. Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих указаний и изучении рекомендованной литературы.

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. Подготовка к лабораторным занятиям и практикумам носит различный характер, как по содержанию, так и по сложности исполнения.

Многие лабораторные занятия требуют большой исследовательской работы, изучения дополнительной научной литературы. Прежде чем приступить к выполнению такой работы, обучающемуся необходимо ознакомиться обстоятельно с содержанием задания, уяснить его, оценить с точки зрения восприятия и запоминания все составляющие его компоненты. Это очень важно, так как при проработке соответствующего материала по конспекту лекции или по рекомендованной литературе могут встретиться определения, факты, пояснения, которые не относятся непосредственно к заданию. Обучающийся должен хорошо знать и понимать содержание задания, чтобы

быстро оценить и отобрать нужное из читаемого. Далее, в соответствии со списком рекомендованной литературы, необходимо отыскать материал к данному заданию по всем пособиям.

Весь подобранный материал нужно хотя бы один раз прочитать или внимательно просмотреть полностью. По ходу чтения помечаются те места, в которых содержится ответ на вопрос, сформулированный в задании. Читая литературу по теме, обучающийся должен мысленно спрашивать себя, на какой вопрос задания отвечает тот или иной абзац прорабатываемого пособия. После того, как материал для ответов подобран, желательно хотя бы мысленно, а лучше всего устно или же письменно, ответить на все вопросы. В случае если обнаружится пробел в знаниях, необходимо вновь обратиться к литературным источникам и проработать соответствующий раздел. Только после того, как преподаватель убедится, что обучающийся хорошо знает необходимый теоретический материал, что его ответы достаточно аргументированы и доказательны, можно считать обучающегося подготовленным к выполнению лабораторных работ.

5.3. Методические указания для подготовки обучающихся к практическим занятиям *(не предусмотрены учебным планом)*

5.4. Методические указания по самостоятельной работе обучающихся
Работа с литературными источниками и интернет ресурсами

Самостоятельная работа обучающегося является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Самостоятельная работа обучающегося над усвоением учебного материала может выполняться в библиотеке, учебных кабинетах, компьютерных классах, а также в домашних условиях. Учебный материал учебной дисциплины, предусмотренный рабочим учебным планом для усвоения обучающимся в процессе самостоятельной работы, выносится на итоговый контроль наряду с учебным материалом, который разрабатывался при проведении учебных занятий. Содержание самостоятельной работы обучающихся определяется учебной программой дисциплины, методическими материалами, заданиями и указаниями преподавателя.

Самостоятельная работа обучающихся осуществляется в аудиторной и внеаудиторной формах.

Самостоятельная работа обучающихся в аудиторное время может включать: конспектирование (составление тезисов) лекций; выполнение контрольных работ; решение задач; работу со справочной и методической литературой; работу с нормативными правовыми актами; выступления с докладами, сообщениями на семинарских занятиях; защиту выполненных работ; участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины; участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях; участие в тестировании и др.

Самостоятельная работа обучающихся во внеаудиторное время может состоять из: повторение лекционного материала; изучения электронной, учебной и научной литературы; изучения нормативных правовых актов (в т.ч. в электронных базах данных); решения задач, выданных на лабораторных занятиях; подготовки к контрольным работам, тестированию и т.д.; подготовки к семинарам устных докладов (сообщений); подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя; выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями на их консультациях; проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах рабочей программы дисциплины задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы.

Формой поиска необходимого и дополнительного материала по дисциплине с целью доработки знаний, полученных во время лекций, есть индивидуальные задания для обучающихся. Выполняются отдельно каждым обучающимся самостоятельно под руководством преподавателей. Именно овладение и выяснения обучающимся рекомендованной литературы создает широкие возможности детального усвоения данной дисциплины.

Индивидуальные задания обучающихся по дисциплине осуществляются путем выполнения одного или нескольких видов индивидуальных или научно-исследовательских задач, избираемых обучающимся с учетом его творческих возможностей, учебных достижений и интересов по согласованию с преподавателем, который ведет лекции или семинарские занятия, или по его рекомендации. Он предоставляет консультации, обеспечивает контроль за качеством выполнения задания и оценивает работу.

Индивидуальные задания должны быть представлены преподавателю и (при необходимости) защищены до окончания учебного курса. Виды, тематика, методические рекомендации и критерии оценки индивидуальных работ определяется отдельными методическими рекомендациями. Результаты выполнения и обсуждения индивидуального задания влияют на выставление итоговой оценки по учебной дисциплине.

5.5 Методические рекомендации по подготовке, написанию и оформлению курсовой работы *(не предусмотрены учебным планом)*

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов	
			ОФО	ЗФО
1	2	3	4	5
Семестр 4				
1.	Лекция: «Государственная политика в области безопасности компьютерных систем»	Мультимедийные технологии	2	2
2.	Лекция: «Основные понятия криптологии»	Технология исследовательского обучения	2	
3.	Лабораторное занятие: «Создание и передача криптографических ключей»	Командная и групповая работа по индивидуальным заданиям лабораторного практикума с применением компьютерных технологий	2	2
4.	Лабораторное занятие: «Политика безопасности в КС. Уровни доступа к информации для пользователей»	Устный контроль по вопросам раздела. Практическое закрепление тем раздела на примерах задач практикума.	2	
Итого часов в 4 семестре:			**8**	**4**
Всего:			**8**	**4**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

Список основной литературы

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html
2. Смышляев, А.Г. Информационная безопасность. Лабораторный практикум [Электронный ресурс]: учебное пособие/ А.Г. Смышляев. — Электрон. текстовые данные. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66655.html
3. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 544 с. — 978-5-4488-0074-0. — Режим доступа: http://www.iprbookshop.ru/63592.html
4. Шаньгин, В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

Список дополнительной литературы

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/33430.html (дата обращения: 08.01.2022). — Режим доступа: для авторизир. пользователе
2. Горев, А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс]: учебно-практическое пособие/ А.И. Горев, А.А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016. — 88 с. — 978-5-88651-642-5. — Режим доступа: http://www.iprbookshop.ru/72856.html
3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 08.01.2022). — Режим доступа: для авторизир. пользователей

Ссылки на видеолекции

1. https://www.google.com/url?q=https://youtu.be/DGLY_X3eHF0&sa=D&source=editors&ust=1639909431756000&usg=AOvVaw1Xra_ureuWj98T8flReiB7
2. https://www.google.com/url?q=https://youtu.be/T8BuNZweJ9w&sa=D&source=editors&ust=1639909431616000&usg=AOvVaw0atHPUKGxZ25Vk5ih8QiuY

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

http://window.edu.ru- Единое окно доступа к образовательным ресурсам;
http:// fcior.edu.ru - Федеральный центр информационно-образовательных ресурсов;
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 6. Project 2008, 2010, 2013	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 № JKS4-D2UT-L4CG-S5CN Срок действия: с 18.10.2021 до 20.10.2022
Консультант Плюс	Договор № 272-186/С-21-01 от 30.12.2020 г.
ЭБС IPRbooks	Лицензионный договор № 8117/21 от 11.06.2021 Срок действия: с 01.07.2021 до 01.07.2022
Свободное ПО: Oracle VM VirtualBox 5.1.8, Python 3.3.4, 7-Zip 9.20, Foxit Reader, Free Pascal, Lazarus, StarUML, R, RStudio, PascalABC.NET.	

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., доска меловая - 1шт., стулья - 65шт., парты - 34шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Экран на штативе – 1 шт.
Проектор – 1 шт.
Ноутбук – 1 шт.

2. Лаборатория сетевых технологий. Лаборатория архитектуры ЭВМ.

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.

3. 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.

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

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.

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 ДИСЦИПЛИНЕ:
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Информационная безопасность»

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2. Этапы формирования компетенции в процессе освоения дисциплины

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

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

Разделы (темы) дисциплины	**Формируемые компетенции (коды)**
	ОПК-3
Раздел 1. Технология защиты информации. Информационная безопасность.	+
Раздел 2. Методы защиты информации от несанкционированного доступа	+
Раздел 3. Криптографические методы и средства обеспечения информационной безопасности.	+
Раздел 4. Защита компьютерных систем от вредоносных программ	+

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

ОПК-3 Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикаторы достижения компетенции	**Критерии оценивания результатов обучения**				**Средства оценивания результатов обучения**	
	неудовлетв	**удовлетв**	**хорошо**	**отлично**	**Текущий контроль**	**Промежуточная аттестация**
1	**2**	**3**	**4**	**5**	**6**	**7**
ИДК-ОПК-3.2 Применяет в практической деятельности знания основных требований информационной безопасности.	Не умеет применять в практической деятельности знания основных требований информационной безопасности.	Частично умеет применять в практической деятельности знания основных требований информационной безопасности.	Хорошо умеет применять в практической деятельности знания основных требований информационной безопасности.	Отлично умеет применять в практической деятельности знания основных требований информационной безопасности.	ОФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование ЗФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование, защита контрольных работ	Экзамен
ИДК-ОПК-3.3 Использует методы поиска и анализа информации для подготовки документов на	Не умеет использовать методы поиска и анализа информации для подготовки	Частично умеет использовать методы поиска и анализа информации для подготовки	Хорошо умеет использовать методы поиска и анализа информации для подготовки	Отлично умеет использовать методы поиска и анализа информации для подготовки	ОФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное	Экзамен

основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	документов на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.	тестирование ЗФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование, защита контрольных работ	
ИДК-ОПК-3.4 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Не владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Частично владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Показывает хорошие способности в умении решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Демонстрирует отличные способности в умении решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование ЗФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование, защита контрольных работ	Экзамен

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к экзамену по дисциплине: «Информационная безопасность»

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.

Задачи к экзамену по дисциплине:
«Информационная безопасность»

1. Зашифруйте сообщение, используя функции MS Excel «НАСТОЯЩИЙ ДРУГ С ТОБОЙ, КОГДА ТЫ НЕ ПРАВ. КОГДА ТЫ ПРАВ, ВСЯКИЙ БУДЕТ С ТОБОЙ» (Марк Твен), используя систему Цезаря со значением ключа соответствующим номеру вашего варианта по журналу учебной группы (например, номер по списку – 5; вариант –5; ключ К = 5).
2. Используя систему Вижинера и функции MS Excel, зашифруйте сообщения «За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами». Ключевое слово «РАДОСТЬ», используя функций MSExcel.
3. Используя систему Вижинера, и функции MS Excel, зашифруйте сообщения «Первые криптографические системы были изобретены в глубокой древности, но не перестали развиваться в наши дни». Ключевое слово «УСПЕХ».
4. Используя систему Вижинера, и функции MS Excel, зашифруйте сообщения «Процесс преобразования открытого текста с целью сделать непонятным его смысл для посторонних называется шифрованием». Ключевое слово «РАДОСТЬ».
5. Используя систему Вижинера, и функции MS Excel, зашифруйте сообщения «За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами». Ключевое слово «УДАЧА».
6. В приложении MS Excel создать книгу, содержащую пронумерованные символы русского алфавита и зашифровать слово «ГЛАГОЛ» с помощью шифра Цезаря с выбранным ключом. К=15.
7. Зашифровать слово КРИПТОГРАФИЯ, выбрав значение ключа шифрования в соответствии с номером своего варианта по журналу учебной группы.
8. Расшифровать криптограмму «пжйжимл», полученную с помощью шифра Цезаря. К=31. Используйте функции MS Excel.
9. Расшифровать криптограмму «юхъыъхщ», полученную с помощью шифра Цезаря, при значении ключа=13. Используйте функции MS Excel.
10. Расшифровать криптограмму «яюышѐшо», полученную с помощью шифра Цезаря, при значении ключа=16. Используйте функции MS Excel.
11. Расшифровать криптограмму «еъѐъщхмх», полученную с помощью шифра Цезаря. К=22. Используйте функции MS Excel.
12. Зашифровать слово «АЛФАВИТ» с помощью шифра Виженера с ключевым словом «СЫР». Используя функции ВПР при шифровании.
13. Зашифровать вручную свои данные «фамилия имя отчество» по парольной фразе из любого известного классического произведения двумя способами: «символы на символы» и «символы на цифры». Представить матрицы-ключи.
14. Зашифровать и дешифровать открытый текст: P= «*информационная безопасность» с ключом* K= *Фамилия (студента)* методом многоалфавитной подстановки на ключе К.
15. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) принтер – ярйыдеа; 2) винчестер – оивжуююее.
16. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) клавиатура – мыеозввшья; 2) проектор – юхюкцчыл;
17. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) монитор – цьъьчак; 2) ноутбук – юудгйты;
18. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) лестница - ьквгхзз; 2) архитектор – мюацдуфюьы;
19. Определить ключ шифрования и дешифровать сообщение, полученное шифром Цезаря: 1) арутуьчн; 2) дьюка.
20. Определить ключ шифрования и дешифровать сообщение, полученное шифром Цезаря: 1) пюынг; 2) омпыж.

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Кафедра «Прикладная информатика»

2021- 2022 учебный год

Экзаменационный билет № 1

по дисциплине: «Информационная безопасность»

для обучающихся направления подготовки 09.03.03 - Прикладная информатика

1. Правовое обеспечение защиты информации
2. Элементы теории чисел
2. Задача: Зашифровать и дешифровать открытый текст: P= «*информационная безопасность» с ключом* K= *Фамилия (студента)* методом многоалфавитной подстановки на ключе K.

Зав. кафедрой Хапаева Л.Х.

Вопросы к устному опросу по дисциплине:
«Информационная безопасность»

1. Каковы уровни правового обеспечения информационной безопасности?
2. Какие законодательные акты составляют основу российского информационного права?
3. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?
4. Какие существуют способы несанкционированного доступа к информации в компьютерных системах?
5. Какие способы аутентификации пользователей могут применяться в компьютерных системах?
6. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?
7. В чем специфика аутентификации пользователей на основе их клавиатурного почерка и росписи мышью?
8. Какие элементы аппаратного обеспечения могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем?
9. В чем разница между симметричными и асимметричными криптографическими системами?
10. В каких режимах может использоваться криптосистема DES?
11. Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста?
12. В каких режимах может использоваться криптосистема ГОСТ 28147-89? Как в ней обеспечивается аутентичность и целостность шифротекстов.
13. В чем особенности и основные сферы применения асимметричных криптосистем?
14. На чем основана криптостойкость систем RSA и Эль-Гамаля?
15. Что такое электронная цифровая подпись, как она получается и проверяется?
16. Какова роль в системах ЭЦП функций хеширования?
17. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?
18. Какие функции CryptoAPI используются для получения и проверки электронной цифровой подписи?
19. Каков порядок вызова функций CryptoAPI при получении ЭЦП?
20. В чем разница между загрузочными и файловыми вирусами?
21. Как происходит заражение программных файлов?
22. Почему файлы документов могут содержать вирусы?
23. Как обеспечивается автоматическое получение управления макровирусами?
24. Как включить встроенную защиту от вирусов в макросах в программах Microsoft Office? В чем недостатки этой защиты?
25. Какие существуют основные каналы заражения вирусами объектов компьютерной системы?
26. Какие существуют методы автоматического обнаружения и удаления вирусов? В чем их достоинства и недостатки?
27. Как осуществляется взаимодействие внедренной в КС программной закладки и нарушителя?
28. Какие существуют методы защиты от программных закладок? Что такое изолированная программная среда?
29. На каких принципах должна основываться разработка системы защиты от копирования?
30. Какие требования предъявляются к системам защиты от копирования?

Тестовые вопросы и задачи по дисциплине:
«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

9. Комплексная система защиты информации это

1. Это совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в КС.

2. Это совокупность объединенных единым целевым назначением средств, для обеспечения защиты информации в КС.

3. Это совокупность правил, законов и писем, в которых прописаны методы и средства обеспечивающих необходимую эффективность защиты информации в КС.

4. Это свод правил утвержденные законодательно в целях организации эффективной защиты информации в КС

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

11. 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

12. 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»

13. 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

14. 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

15. 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

16. 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

17. 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

18. 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.)

19. 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

20. Протокол Kerberos предназначен для

1. обеспечения конфиденциальности передаваемой по сети информации, используя при этом функции шифрования, а также технологию выдачи мандатов

2.однопользовательских рабочих станций, для целей безопасной передачи информации по локальной сети

3. для аутентификации субъекта объектом через специальные ключи шифрования

4.централизованного администрирования учетных записей пользователей работающих в сети интернет

21.Применяемые разновидности межсетевых экранов

1.фильтрующие маршрутизаторы

2. шлюзы сеансового уровня

3.шлюзы прикладного уровня

4. все вышеперечисленные

22. VPN предназначены?

1. для создания всевозможных межсетевых экранов

2.виртуальные частные сети для скрытия топологии внутренних сетей организаций, обменивающихся информацией по сети интернет, и защиты трафика между ними.

3. виртуальные частные сети для выделения числа защищаемых подсетей и выделения специального криптомаршрутизатора для безопасной передачи данных по сети интернет

4. виртуальные частные сети для открытия топологии внутренних сетей организаций, обменивающихся информацией по сети интернет, и защиты трафика между ними с использованием криптомаршрутизатора

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

1. все пользователи получают разные пароли, сложность замены пароля если он забыт, слабая защищенность, технические пароли позволяют загрузить операционную систему неавторизованным пользователям

2. все пользователи получают одинаковые пароли, простора замены пароля если он забыт, слабая защищенность, технические пароли позволяют загрузить операционную систему неавторизованным пользователям

3. все пользователи получают разные пароли, сложность замены пароля если он забыт, слабая защищенность, технические пароли не позволяют загрузить операционную систему неавторизованным пользователям

4. все пользователи получают общий пароль, сложность замены пароля если он забыт, слабая защищенность, технические пароли позволяют загрузить операционную систему неавторизованным пользователям

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

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

25. Редактор системных правил Windows называется и предназначен

1. edit и предназначен для редактирования реестра ОС

2. poledit и предназначается для ввода определенных ограничений на права конкретного пользователя или всех пользователей системы

3. editor и предназначается для ввода запрета на выполнение программ в режиме эмуляции DOS

4. poleditor и предназначен для ввода определенных ограничений на настройку панели управления ОС

26. 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

27. Достоинства дискреционного управления доступом к объектам КС

1. простота идентификации, возможность описания пользователем доступ к своим ресурсам

2. детализированность и назначение прав доступа

3. простата реализации доступом к объектам КС и гибкость

4. простота администрирования и гибкость

28. 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

29. 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

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

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

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

3. Если $b = 1$, a = b {mod n} и $|b| < n$, то b называют вычетом числа a по модулю n.

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

Задания к контрольной работе по дисциплине:
«Информационная безопасность»

Вариант № 1

Открыть в Internet Explorer на вкладке «Безопасность» режим «Просмотр InPrivate» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 2

Открыть в Internet Explorer на вкладке «Безопасность» режим «Удалить журнал обозревателя» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 3

Открыть в Internet Explorer на вкладке «Безопасность» режим «Политика конфиденциальности веб-страницы» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 4

Открыть в Internet Explorer на вкладке «Безопасность» режим «Параметры фильтрации InPrivate» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 5

Открыть в Internet Explorer на вкладке «Безопасность» режим «Фильтр SmartScreen» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 6

Открыть в Internet Explorer через «Сервис»–«Свойства обозревателя» вкладку «Общие» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 7

Открыть в Internet Explorer через «Сервис»–«Свойства обозревателя» вкладку «Безопасность» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 8

Открыть в Internet Explorer через «Сервис»–«Свойства обозревателя» вкладку «Конфиденциальность» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Вариант № 9

Составить программу для шифрования методом перестановки с повышенной криптостойкость одним из следующих способов. Для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования. При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы – они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы. Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

Вариант № 10

Зашифровать вручную свои данные «фамилия имя отчество» по парольной фразе из любого известного классического произведения двумя способами: «символы на символы» и «символы на цифры». В отчете представить матрицы-ключи.

Задания к лабораторной работе по дисциплине:
«Информационная безопасность»

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.

5. Методические материалы, определяющие процедуры оценивания компетенции

5.1 Критерии оценивания качества выполнения лабораторного практикума

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

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

5.2 Критерии оценивания качества устного ответа

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

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

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

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

5.3 Критерии оценивания тестирования

При тестировании все верные ответы берутся за 100%.
90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно
менее 60% неудовлетворительно

5.4 Критерии оценивания выполнения контрольной работы

Оценка **«отлично»** выставляется при условии, что обучающийся полностью выполнил задание контрольной и проявил отличные знания учебного материала. При этом работа оформлена в соответствии с требованиями и ГОСТом, к ней можно предъявить минимум замечаний.

Оценка **«хорошо»** ставится тогда, когда обучающийся выполнил все задания, показал хорошие знания по пройденному материалу, но не сумел обосновать предложенные решения задач, когда есть недочеты в оформлении контрольной работы и общие небольшие замечания, не влияющие на ее качество.

Оценку **«удовлетворительно»** обучающийся получает за полностью выполненное задание контрольной при наличии в ней существенных неточностей и недочетов, не умении обучающимся верно применить полученные знания, в оформлении работы есть нарушения ГОСТ, не аргументированные ответы, неактуальные или ненадежные источники информации.

Оценку **«неудовлетворительно»** обучающийся получает в том случае, когда он не полностью выполнил задание проявил недостаточный уровень знаний, не смог объяснить полученные результаты. Такая контрольная работа не отвечает требованиям, содержит противоречивые сведения, задачи в ней решены неверно.

5.5 Критерии оценивания результатов освоения дисциплины на экзамене

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.