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
«27» 03 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Комплексная информационная безопасность

Уровень образовательной программы магистратура

Направление подготовки 09.04.03 Прикладная информатика

Направленность (профиль) Прикладная информатика в экономике и управлении

Форма обучения очная (заочная)

Срок освоения ОП 2 года (2 года 6 месяцев)

Институт Цифровых технологий

Кафедра разработчик РПД Информационные системы и технологии

Выпускающая кафедра Информационные системы и технологии

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор ИЦТ _____ Кумратова А.М.

Заведующий выпускающей кафедрой _____ Кумратова А.М.

г. Черкесск, 2026 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Комплексная информационная безопасность» является:

1. овладение знаниями различных методов и средств по построению комплексной системы информационной безопасности современной организации;
2. овладение навыками применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике;
3. овладение навыками применения современных методов и инструментальных средств прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем.

Задачей дисциплины является приобретение обучаемыми знаний и умений в области:

- формирования представлений об основных аспектах комплексной информационной безопасности;
- формирование представлений об основах криптографии и криптоанализа;
- изучение основных методов, законов и нормативных актов в области компьютерной безопасности;
- овладение навыками применения программно-технических средств защиты информации, обеспечения безопасности сетевых коммуникаций.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Комплексная информационная безопасность» относится к части, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули), имеет тесную связь с другими дисциплинами.

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

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1.	Архитектура корпоративных информационных систем Защищенные информационные системы и среды	Методы и средства обеспечения безопасности информационных систем Технологии облачных вычислений

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 09.04.03 Прикладная информатика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:
1	2	3	4
1.	ПК-2	способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	ПК-2.1 Анализирует применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике ПК-2.2 Разрабатывает и применяет математические модели в области проектирования и управления информационными системами ПК-2.3 Анализирует и оценивает угрозы информационной безопасности; применяет отечественные и зарубежные стандарты в области компьютерной безопасности.
2.	ПК-5	способность применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	ПК-5.1 Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем ПК-5.2 Выбирает и использует облачные сервисы для решения прикладных задач различных классов и создания информационных систем ПК-5.3 Выявляет и анализирует риски информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы		**Всего часов**	**Семестр**
			№ 2
			часов
1		2	3
Аудиторная контактная работа (всего)		**42**	**42**
В том числе:			
Лекции (Л)		14	14
Практические занятия (ПЗ)		28	28
Лабораторные работы (ЛР)		**-**	**-**
Контактная внеаудиторная работа, в том числе		**2**	**2**
Групповые и индивидуальные консультации		2	2
Самостоятельная работа обучаемого (СРО) (всего)		**73**	**73**
Работа с книжными и электронными источниками		40	40
Выполнение индивидуальных практических заданий		15	15
Подготовка к промежуточному контролю (ППК)		2	2
Подготовка к тестированию		16	16
Промежуточная аттестация	экзамен (Э)	**Э (27)**	**Э (27)**
	Прием экз., час.	0,5	0,5
	Консультация, час.	2	2
	СРО, час.	24,5	24,5
ИТОГО: Общая трудоемкость	**часов**	**144**	**144**
	зач. ед.	**4**	**4**

Заочная форма обучения

Вид учебной работы		Всего часов	Семестры
			№2
			Часов
1		2	3
Аудиторная контактная работа (всего)		18	18
В том числе:			
Лекции (Л)		4	4
Практические занятия (ПЗ), Семинары (С)		14	14
Контактная внеаудиторная работа, в том числе		**1**	**1**
Групповые и индивидуальные консультации		1	1
Самостоятельная работа обучающегося(СРО) (всего)		116	116
Работа с книжными источниками		12	12
Работа с электронными источниками		30	30
Просмотр и конспектирование видеолекций		20	20
Подготовка к промежуточному контролю (ППК)		6	6
Выполнение индивидуальных практических заданий		24	24
Подготовка к тестированию		24	24
Промежуточная аттестация	Экзамен(Э)	Э (9)	Э (9)
	Прием экз., час	0,5	0,5
	СРО, час.	8,5	8,5
ИТОГО: Общая трудоемкость	**Часов**	144	144
	зачетных единиц	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 обучаемых (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР	ПЗ	СРО	всего	
1	2	3	4	5	6	7	8
Семестр 2							
1.	Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности	4		4	14	22	Тестирование, выполнение практических заданий
2.	Раздел 2. Защита от несанкционированного доступа к информации.	2		6	14	22	Тестирование, устный опрос
3.	Раздел 3. Модель угроз и модель нарушителей информационной безопасности	2		6	14	22	тестирование, устный опрос, выполнение практических заданий
4.	Раздел 4. Аудит и оценка возможных рисков ИБ	2		6	14	22	тестирование, устный опрос, выполнение практических заданий
5.	Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.	4		6	17	27	тестирование, устный опрос, выполнение практических заданий
	Контактная внеаудиторная работа					2	Индивидуальные и групповые консультации
	Промежуточная аттестация					**27**	**Экзамен**
ИТОГО:		**14**		**28**	**73**	**144**	

Заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучаемых (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР	ПЗ	СРО	всего	
1	2	3	4	5	6	7	8
Семестр 2							
1.	Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности	2		4	24	30	Тестирование, выполнение практических заданий
2.	Раздел 2. Защита от несанкционированного доступа к информации.			2	24	26	Тестирование, устный опрос
3.	Раздел 3. Модель угроз и модель нарушителей информационной безопасности			2	24	26	Тестирование, устный опрос выполнение практических заданий
4.	Раздел 4. Аудит и оценка возможных рисков ИБ	2		2	24	28	Тестирование, устный опрос, выполнение практических заданий
5.	Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.			4	20	24	Тестирование, устный опрос, выполнение практических заданий
6.	Контактная внеаудиторная работа					1	Индивидуальные и групповые консультации
7.	**Промежуточная аттестация**					**9**	**Экзамен**
ИТОГО:		**4**		**14**	**116**	**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 2					
1.	Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности.	Основные понятия безопасности информационных технологий. Изучение федеральных законов в области информационной безопасности.	Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности. Правовое регулирование применения СКЗИ иЭП в корпоративных информационных системах. Специальные нормативные и методические документы ФСБ России по использованию шифровальных(криптографических) средств. Изучение федеральных законов в области информационной безопасности: 63-ФЗ «Об электронной подписи» 2011 года, 98-ФЗ «О коммерческой тайне», 152-ФЗ «О персональных данных», 149-ФЗ «Об информации, информационных технологиях и защите информации» 2006 года с дополнениями 2014 года,187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».	**4**	**2**

2.	Раздел 2. Защитаот несанкционированного доступа к информации.	Защита от несанкционированного доступа к информации. Конфиденциальная информация, конфиденциальный документооборот.	Защита от несанкционированного доступа к информации. Организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа. Конфиденциальная информация. Изучение понятий государственная тайна, коммерческая тайна, персональные данные, данные ограниченного доступа. Правовые документы в области защиты конфиденциальных сведений.	**2**	
3.	Раздел 3. Модель угроз и модель нарушителей информационной безопасности.	Построение модели угрози модели нарушителей информационной безопасности.	Модель угроз и модель нарушителей информационной безопасности. Схема построения моделей на основе стандартовИБ.	**2**	**2**
4.	Раздел 4. Аудит и оценка возможных рисков ИБ	Основные понятия аудита и оценки возможных рисков информационной безопасности.	Аудит и оценка возможных рисков ИБ. Основные понятия	**2**	
5.	Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.	Основные типы атак на информационные системы, основные меры противодействия. Компьютерны е вирусы и защита от них.	Основные типы атак на информационные системы и меры их защиты. Протокол IPsec. Методы аутентификации и шифрования протокола IPsec.	**4**	
	ИТОГО часов в семестре:			**14**	**4**

4.2.3. Лабораторный практикум не предполагается

4.2.4. Практические занятия

№ п/п	Наименование раздела дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	7
Семестр 2					
1.	Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности.	Безопасность информационных технологий	Построение системы безопасности предприятия. Разбор основных понятий ФЗ «Об электронной подписи».	4	4
2.	Раздел 2. Защитаот несанкционированного доступа к информации.	Конфиденциальная информация. Несанкционированный доступ к информации	Разбор методов и средств защиты от несанкционированного доступа к информации. Разбор понятий конфиденциального документооборота	6	2
3.	Раздел 3. Модель угроз и модель нарушителей информационной безопасности.	Модель угроз и модель нарушителей информационной безопасности	Построение модели угроз и нарушителей информационной безопасности на примере.	6	2
4.	Раздел 4. Аудит и оценка возможных рисков ИБ.	Аудит и оценка возможных рисков ИБ	Аудит и оценка возможных рисков ИБ предприятия на примере. Основные понятия.	6	2
5.	Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.	Основные типы атак на информационные системы, основные меры противодействия. Компьютерные вирусы и защита от них	Изучение протокола IPsec. Разбор на примерах.	6	4
ИТОГО часов в семестре:				**28**	**14**

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЕМОГО

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов
				ОФО
1	3	4	5	6
Семестр 2				
1.	Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности.	1.1	Работа с книжными и электронными источниками	10
		1.2	Выполнение индивидуальных практических заданий	2
		1.3	Подготовка к тестированию	2
2.	Раздел 2. Защита от несанкционированного доступа к информации.	2.1	Работа с книжными и электронными источниками	4
		2.2	Подготовка к тестированию	10
3.	Раздел 3. Модель угроз и модель нарушителей информационной безопасности.	3.1	Работа с книжными и электронными источниками	6
		3.2	Выполнение индивидуальных практических заданий	6
		3.3	Подготовка к тестированию	2
4.	Раздел 4. Аудит и оценка возможных рисков ИБ.	4.1	Работа с книжными и электронными источниками	10
		4.2	Выполнение индивидуальных практических заданий	2
		4.3	Подготовка к тестированию	2
5.	Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.	5.1	Работа с книжными и электронными источниками	10
		5.2	Выполнение индивидуальных практических заданий	5
		5.3	Подготовка к промежуточному контролю (ППК)	2
ИТОГО часов в семестре:				**73**

Заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов
				ЗФО
1	3	4	5	6
Семестр 2				
1.	Раздел 1. Понятия безопасности информационных технологий.	1.1.	Работа с книжными источниками	6
		1.2.	Работа с электронными источниками	6
		1.3.	Выполнение индивидуальных	6

	Нормативная база обеспечения информационной безопасности.		практических заданий	
		1.4.	Подготовка к тестированию	6
2.	Раздел 2. Защита от несанкционированного доступа к информации.	2.1.	Работа с книжными источниками	6
		2.2.	Работа с электронными источниками	6
		2.3.	Подготовка к тестированию	6
		2.4.	Просмотр видеолекций	6
3.	Раздел 3. Модель угроз и модель нарушителей информационной безопасности.	3.1.	Просмотр видеолекций	6
		3.2.	Работа с электронными источниками	6
		3.3.	Выполнение индивидуальных практических заданий	6
		3.4.	Подготовка к тестированию	6
4.	Раздел 4. Аудит и оценка возможных рисков ИБ.	4.1	Просмотр и конспектирование видеолекций	6
		4.2	Работа с электронными источниками	6
		4.3	Выполнение индивидуальных практических заданий	6
		4.4	Подготовка к тестированию	6
5.	Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.	5.1	Просмотр и конспектирование видеолекций	2
		5.2	Работа с электронными источниками	6
		5.3	Выполнение индивидуальных практических заданий	6
		5.4	Подготовка к промежуточному контролю (ППК)	6
ИТОГО часов за год:				116

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

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

Основными формами обучения дисциплины являются лекции и практические занятия, а также самостоятельная работа.

Лекция является основной формой обучения в высшем учебном заведении. Записи лекций в конспектах должны быть избирательными, полностью следует записывать только определения. В конспекте рекомендуется применять сокращение слов, что ускоряет запись. Вопросы, возникающие в ходе лекции, рекомендуется записывать на полях и после окончания лекции обратиться за разъяснением к преподавателю. Необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях.

Работа над конспектом лекции осуществляется по этапам:

− повторить изученный материал по конспекту;

− непонятные положения отметить на полях и уточнить;

− неоконченные фразы, пропущенные слова и другие недочеты в записях устранить, пользуясь материалами из учебника и других источников;

− завершить техническое оформление конспекта (подчеркивания, выделение главного, выделение разделов, подразделов и т.п.).

Самостоятельную работу следует начинать с доработки конспекта, желательно в тот же день, пока время не стерло содержание лекции из памяти. Работа над конспектом не должна заканчиваться с прослушивания лекции. После лекции, в процессе самостоятельной работы, перед тем, как открыть тетрадь с конспектом, полезно мысленновосстановить в памяти содержание лекции, вспомнив ее структуру, основные положения ивыводы.

С целью доработки необходимо прочитать записи, восстановить текст в памяти, а также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Далее прочитать материал по рекомендуемой литературе, разрешая в ходе чтения, возникшие ранее затруднения, вопросы, а также дополнения и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. В ходе доработки конспекта углубляются, расширяются и закрепляются знания, а также дополняется, исправляется и совершенствуется конспект. Еще лучше, если вы переработаете конспект, дадите его в новой систематизации записей. Это, несомненно, займет некоторое время, но материал вами будет хорошо проработан, а конспективная запись его приведена в удобный для запоминания вид. Введение заголовков, скобок, обобщающих знаков может значительно повысить качество записи. Этому может служить также подчеркивание отдельных мест конспекта красным карандашом, приведение на полях или на обратной стороне листа краткой схемы конспекта и др.

Подготовленный конспект и рекомендуемая литература используется при подготовке к практическому занятию. Подготовка сводится к внимательному прочтению учебного материала, к выводу с карандашом в руках всех утверждений и формул, к решению примеров, задач, к ответам на вопросы, предложенные в конце лекции преподавателем или помещенные в рекомендуемой литературе. Примеры, задачи, вопросы по теме являются средством самоконтроля.

Непременным условием глубокого усвоения учебного материала является знание основ, на которых строится изложение материала. Обычно преподаватель напоминает, какой ранее изученный материал и в какой степени требуется подготовить к очередному занятию. Эта рекомендация, как и требование систематической и серьезной работы над всем лекционным курсом, подлежит безусловному выполнению. Потери логической связи как внутри темы, так и между ними приводит к негативным последствиям: материал учебной дисциплины перестает основательно восприниматься, а творческий труд подменяется утомленным переписыванием. Обращение к ранее изученному материалу не только помогает восстановить в памяти известные положения, выводы, но и приводит разрозненные знания в систему, углубляет и расширяет их. Каждый возврат к старому материалу позволяет найти в нем что-то новое, переосмыслить его с иных позиций, определить для него наиболее подходящее место в уже имеющейся системе знаний. Неоднократное обращение к пройденному материалу является наиболее рациональной формой приобретения и закрепления знаний. Очень полезным, но, к сожалению, еще мало используемым в практике самостоятельной работы, является предварительное ознакомление с учебным материалом. Даже краткое, беглое знакомство с материалом очередной лекции дает многое. Обучающиеся получают общее представление о ее содержании и структуре, о главных и второстепенных вопросах, о терминах и определениях. Все это облегчает работу на лекции и делает ее целеустремленной.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

- не предусмотрены

5.3. Методические указания для подготовки обучающихся к практическим занятиям

Подготовку к практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала, а затем изучение обязательной и дополнительной литературы, рекомендованной к данной теме.

Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы семинара, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий.

5.4. Методические указания по самостоятельной работе обучающихся

Работа с литературными источниками и интернет ресурсами

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Методические рекомендации по проведению устного опроса.

Устный опрос является одним из основных способов учета знаний обучающихся. Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на определенную тему, показывать его умение применять определения, правила в конкретных случаях.

Основные качества устного ответа подлежащего оценке.

1. Правильность ответа по содержанию (учитывается количество и характер ошибок при ответе).

2. Полнота и глубина ответа (учитывается количество усвоенных лексических единиц, грамматических правил и т. п.).

3. Сознательность ответа (учитывается понимание излагаемого материала).

4. Логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией).

5. Рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели).

6. Своевременность и эффективность использования наглядных пособий и

технических средств при ответе (учитывается грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе).

7. Использование дополнительного материала (приветствуется, но не обязательно для всех обучающихся).

8. Рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени, с учетом индивидуальных особенностей обучающихся).

Методические рекомендации по подготовке обучающихся к тестированию.

В современном образовательном процессе тестирование как новая форма оценки знаний занимает важное место и требует серьезного к себе отношения.

Цель тестирований в ходе учебного процесса обучающихся состоит не только в систематическом контроле за знанием точных дат, имен, событий, явлений, но и в развитии умения обучающихся выделять, анализировать и обобщать наиболеесущественные связи, признаки и принципы разных исторических явлений и процессов. Одновременно тесты способствуют развитию творческого мышления, умению самостоятельно локализовать и соотносить исторические явления и процессы во времении пространстве.

Как и любая другая форма подготовки к контролю знаний, тестирование имеет ряд особенностей, знание которых помогает успешно выполнить тест.

Можно дать следующие методические рекомендации:

- Прежде всего, следует внимательно изучить обучающемуся структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, какого типа задания в нем содержатся. Это поможет настроиться на работу.
- Лучше начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока не останавливаясь на тех, которые могут вызвать долгие раздумья. Это позволит успокоиться и сосредоточиться на выполнении более трудных вопросов.
- Очень важно всегда внимательно читать задания до конца, не пытаясь понять условия «по первым словам» или выполнив подобные задания в предыдущих тестированиях. Такая спешка нередко приводит к досадным ошибкам в самых легких вопросах.
- Если Вы не знаете ответа на вопрос или не уверены в правильности, следует пропустить его и отметить, чтобы потом к нему вернуться.
- Психологи также советуют думать только о текущем задании. Как правило, задания в тестах не связаны друг с другом непосредственно, поэтому необходимо концентрироваться на данном вопросе и находить решения, подходящие именно к нему. Кроме того, выполнение этой рекомендации даст еще один психологический эффект – позволит забыть о неудаче в ответе на предыдущий вопрос, если таковая имела место.
- Многие задания можно быстрее решить, если не искать сразу правильный вариант ответа, а последовательно исключать те, которые явно не подходят. Метод исключения позволяет в итоге сконцентрировать внимание на одном-двух вероятных вариантах.
- Рассчитывать выполнение заданий нужно всегда так, чтобы осталось время на проверку и доработку (примерно 1/3-1/4 запланированного времени). Тогда вероятность описок сводится к нулю и имеется время, чтобы набрать максимум баллов на легких заданиях и сосредоточиться на решении более трудных, которые вначале пришлось пропустить.
- Процесс угадывания правильных ответов желательно свести к минимуму, так как это чревато тем, что обучающийся забудет о главном: умении использовать имеющиеся накопленные в учебном процессе знания, и будет надеяться на удачу. Если уверенности в правильности ответа нет, но интуитивно появляется

предпочтение, то психологи рекомендуют доверять интуиции, которая считается проявлением глубинных знаний и опыта, находящихся на уровне подсознания.

При подготовке к тесту не следует просто заучивать, необходимо понять логику изложенного материала. Этому немало способствует составление развернутого плана, таблиц, схем, внимательное изучение разделов курса. Большую помощь оказывают опубликованные сборники тестов, Интернет-тренажеры, позволяющие, во-первых, закрепить знания, во-вторых, приобрести соответствующие психологические навыки саморегуляции и самоконтроля. Именно такие навыки не только повышают эффективность подготовки, позволяют более успешно вести себя во время экзамена, но и вообще способствуют развитию навыков мыслительной работы.

Методические рекомендации для выполнения индивидуальных практических заданий.

Методические указания для выполнения индивидуальных практических заданий (мультимедийных проектов). Индивидуальные задания – разнообразные работы научного, методического или учебно-практического характера. Индивидуальные задания носят заведомо нестандартный характер и оцениваются в каждом случае индивидуально. Содержание индивидуального задания должно быть согласовано с преподавателем, ведущим практические занятия.

Презентация.

Содержание презентации соответствует содержанию контрольной работы.

Объем – не менее 10 слайдов.

1-й – тема, ФИО обучающегося, год издания.

2-й – СОДЕРЖАНИЕ.

3-4-й – введение: кратко - актуальность, цели, задачи, объект и предмет исследования, теоретическая, нормативная и эмпирическая основа, методологическая основа, структура работы.

С 5-го - основная часть (текст) со схемами, таблицами, диаграммами, картинками, фото, статистическими данными и т.д. 13

Заключение: краткие выводы по работе. (1-2 слайда).

Список использованной литературы – весь. (1-2 слайда).

Сноски не нужны.

Последний слайд указывает на логическое завершение работы: Спасибо за внимание! или Благодарим за внимание!

Текст выравнивается на слайдах по ширине и приблизительно одинакового размера.

Цвет фона слайда не должен сливаться с цветом шрифта текста.

Рекомендуется применять эффекты анимации. Смену слайдов можно выставлять по времени или «по щелчку». Допускается прикрепление музыкального файла.

Промежуточная аттестация

По итогам 2 семестра проводится экзамен(на ОФО, ЗФО и ОЗФО). При подготовке к сдаче экзамена рекомендуется пользоваться материалами практических занятий и материалами, изученными в ходе текущей самостоятельной работы.

Экзамен проводится в устной или письменной 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 практических работ.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов		
			ОФО	ОЗФО	ЗФО
1	2	3	4	5	6
Семестр 2					
1	Лекция «Модель угроз и модель нарушителей информационной безопасности»	Технология развития критического мышления	**2**	**2**	**2**
2	Практическое занятие «Построение системы безопасности предприятия»	Игровые технологии	**4**	**2**	**2**
3	Практическое занятие «Разбор основных понятий ФЗ «Об электронной подписи»	Технология развития критического мышления	**4**	**2**	**2**
Итого часов:			**10**	**6**	**5**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

Список основной литературы

1. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.1 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. — 193 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/138773.html
2. Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/132693.html
3. Программно-аппаратные средства защиты информации. В 3 частях. Ч.2 : учебное пособие / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 79 с. — ISBN 978-5-8265-2464-0, 978-5-8265-2609-5 (ч.2). — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/141077.html Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф.
4. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html

Список дополнительной литературы

1. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/10677.html

2. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 242 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/62945.html

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://www.rsl.ru/- сайт Российской государственной библиотеки
2. http://www.gpntb.ru/ - сайт Государственной публичной научно-технической библиотеки России
3. https://www.elibrary.ru - сайт Научной электронной библиотеки

7.3. Информационные технологии, лицензионное программное обеспечение

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Антивирус Dr.Web Desktop Security Suite	Лицензионный договор № 621 Срок действия: с 25.09.2025 до 24.09.2026
Консультант Плюс	Договор № 7 от 15.01.2026 г.
Цифровой образовательный ресурс IPR SMART	Лицензионный договор № 12873/25П от 02.07.2025 г. Срок действия: с 01.07.2025 г. до 30.06.2026 г.
ЛИРА	Сублицензионный договор № 2066/А от 21.01.2014 г.
MATLAB	Гос. контракт № 0379100003114000018 от 16 мая 2014 г.
Кодекс	Лицензионное соглашение № 5/4072 от 29.03.2026 г.
Бесплатное ПО	
LibreOffice, OpenOffice, МойОфис, Visual Studio Community, Sumatra PDF, 7-Zip, Adobe Acrobat Reader, 1С: Предприятие Учебная версия, Lazarus, Firebird, IBE Expert, Virtual box, Visual Studio Code, StarUML – унифицированный язык моделирования	

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 - 9шт., 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. ПК-11шт.

2. Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
Доска меловая - 1шт., стол преподавательский - 1шт., парты - 8шт., стулья - 26шт., компьютерные столы - 10шт., стул мягкий – 1шт. Лабораторное оборудование, технические средства обучения, служащие для предоставления

учебной информации большой аудитории:
ПК-10 шт.
3.**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 -1шт.
Проектор -1 шт.
Ноутбук -1 шт.

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 – 1шт.

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– 20 шт.
Монитор - 1 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 обучаемых, 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 Комплексная информационная безопасность

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Комплексная информационная безопасность

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-2	способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике
ПК-5	способность применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем

2. Этапы формирования компетенции в процессе освоения дисциплины

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

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

Разделы (темы) дисциплины	Формируемые компетенции (коды)	
	ПК-2	ПК-5
Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности	+	
Раздел 2. Защита от несанкционированного доступа к информации.	+	
Раздел 3. Модель угроз и модель нарушителей информационной безопасности	+	
Раздел 4. Аудит и оценка возможных рисков ИБ		+
Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.		+

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

ПК-2 способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовлетв	удовлетв	хорошо	отлично	Текущий контроль	Промежуточная аттестация
ПК-2.1 Анализирует применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Не анализирует применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Неполное представление о анализе применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Наличие пробелов в представлении об анализе различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Сформированное представление об анализе различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике.	Устный опрос, тестирование, выполнение практических заданий	Экзамен
ПК-2.2 Разрабатывает и применяет математические модели в области проектирования и управления информационными системами	Фрагментарное умение разрабатывать и применять математические модели в области проектирования и управления информационными системами	Наличие пробелов в умении разрабатывать и применяет математические модели в области проектирования и управления информационными системами	Наличие пробелов в умении разрабатывать и применять математические модели в области проектирования и управления информационными системами	Сформированное умение разрабатывать и применять математические модели в области проектирования и управления информационными системами	Устный опрос, тестирование, выполнение практических заданий	Экзамен

ПК-2.3 Анализирует и оценивает угрозы информационной безопасности; применяет отечественные и зарубежные стандарты в области компьютерной безопасности	Фрагментарное владение навыками анализа и оценивания угрозы информационной безопасности, применение отечественных и зарубежных стандартов в области компьютерной безопасности.	Умение владеть навыками анализа и оценивания угрозы информационной безопасности, применение отечественных и зарубежных стандартов в области компьютерной безопасности.	Наличие пробелов во владении навыками анализа и оценивания угрозы информационной безопасности, применение отечественных и зарубежных стандартов в области компьютерной безопасности.	Сформированное владение навыками анализа и оценивания угрозы информационной безопасности, применение отечественных и зарубежных стандартов в области компьютерной безопасности.	Устный опрос, тестирование, выполнение практических заданий	Экзамен

ПК-5 способность применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовлетв	удовлетв	хорошо	отлично	Текущий контроль	Промежуточная аттестация
ПК-5.1 Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Фрагментарные знания о современных методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Несистематические знаниях о современных методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем.	Наличие пробелов в знаниях о современных методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Сформированные и систематические знания о современных методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Устный опрос, тестирование, выполнение практических заданий	Экзамен

ПК-5.2 Выбирает и использует облачные сервисы для решения прикладных задач различных классов и создания информационных систем	Неумение выбирать и использовать облачные сервисы для решения прикладных задач различных классов и создания информационных систем.	Несистематический характер умений выбирать и использовать облачные сервисы для решения прикладных задач различных классов и создания информационных систем.	Наличие пробелов в умениях выбирать и использовать облачные сервисы для решения прикладных задач различных классов и создания информационных систем.	Сформированные умения выбирать и использовать облачные сервисы для решения прикладных задач различных классов и создания информационных систем.	Устный опрос, тестирование, выполнение практических заданий	Экзамен
ПК-5.3 Выявляет и анализирует риски информационной безопасности	Низкий уровень владения навыками выявления и анализа рисков информационной безопасности	В целом успешное, но несистематическое владение навыками выявления и анализа рисков информационной безопасности.	Наличие пробелов во владении навыками подготовки выявления и анализа рисков информационной безопасности.	Демонстрация владения навыками выявления и анализа рисков информационной безопасности.	Устный опрос, тестирование выполнение практических заданий	Экзамен

4. Комплект контрольно-оценочных средств по дисциплине

Экзаменационные вопросы

по дисциплине Комплексная информационная безопасность

1. Безопасность систем электронного документооборота в банковском учреждении.
2. Безопасность электронного финансового документооборота.
3. Виды реализации Internet угроз (перечислить, пояснить механизмы реализации).
4. Виды реализации программных угроз (перечислить, пояснить механизмы реализации).
5. Дать определение понятию «информационная безопасность». Пояснить составляющие.
6. Дать определение понятию «троянская программа».
7. Дать определение понятию «угроза доступности».
8. Дать определение понятию «угроза конфиденциальности».
9. Дать определение понятию «угроза целостности».
10. Дать определение понятию «угроза».
11. Дать определение понятиям «риск», «управление риском»
12. Защита информации в автоматизированных системах банковских расчетов.
13. Источники угроз безопасности информации.
14. Каковы цели обеспечения информационной безопасности. Дать определение составляющим.
15. Классифицировать способы воздействия угроз.
16. Концепция комплексной системы защиты информации (Схема функций и результатов защиты информации).
17. Криминалистическая характеристика компьютерного преступления. Основные способы совершения компьютерного преступления. Проблемы построение систем защищенного документооборота.
18. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации.
19. Определение информации в задачах информационной безопасности. Автономная информация. Информация воздействия. Информация взаимодействия.
20. Организационно – правовое обеспечение защиты информации. (Организационно-правовая основа, юридические аспекты).
21. Организационные мероприятия по защите конфиденциальной информации.
22. Основные виды технических каналов и источников утечки информации.
23. Перечислить задачи системы антивирусной безопасности.
24. Перечислить и пояснить критерии выбора антивирусных средств.
25. Перечислить цели реагирования на нарушения информационной безопасности.
26. Понятия компьютерного преступления.
27. Пример практического применения механизма ЭЦП.
28. Принципы защиты информации от несанкционированного доступа.
29. Пути и проблемы практической реализации концепции комплексной защиты информации.
30. Системная классификация и общий анализ угроз безопасности информации.
31. Содержание административных мер обеспечения информационной безопасности.
32. Содержание законодательных мер обеспечения информационной безопасности.
33. Содержание и структура понятия «безопасность».
34. Содержание и структура понятия «информационная безопасность».

35. Содержание и структура понятия «обеспечение информационной безопасности».
36. Требования защищенности СВТ от НСД к информации. Классы и группы защищенности СВТ от НСД.
37. Угрозы безопасности информации.
38. Угрозы доступности.
39. Цели безопасности.
40. Средства, используемые для создания механизмов защиты информации в КИС.
41. Методы поиска и сбора информации.
42. Методика устранения компьютерной информации.
43. Уязвимости Windows.
44. Уязвимости UNIX
45. Защита от копирования переносных носителей.
46. Аппаратные ключи защиты.
47. Современные криптосистемы
48. Виды шифров. Методика кодирования.
49. Навесная защита.
50. Антивирусное программное обеспечение.
51. Особенности защиты информации при работе в сети.
52. Безопасная работа в Internet.
53. Целесообразность усиления обороны.
54. Защита от побочного электромагнитного излучения и наводок.
55. Алгоритмы распределения ключей.
56. Аудит и оценка возможных рисков ИБ.
57. Основные типы атак на информационные системы и меры их защиты.
58. Протокол IPsec. Методы аутентификации и шифрования протокола IPsec.
59. Модель угроз и модель нарушителей информационной безопасности.
60. Схема построения моделей на основе стандартов ИБ.
61. Защита от несанкционированного доступа к информации.
62. Организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.
63. Конфиденциальная информация. Изучение понятий государственная тайна, коммерческая тайна, персональные данные, данные ограниченного доступа.
64. Правовые документы в области защиты конфиденциальных сведений.
65. Актуальность проблемы обеспечения информационной безопасности.
66. Термины и определения в области информационной безопасности.
67. Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.
68. Специальные нормативные и методические документы ФСБ России по использованию шифровальных(криптографических) средств.
69. Поясните содержание федеральных законов в области информационной безопасности: 63-ФЗ «Об электронной подписи» 2011 года, 98-ФЗ «О коммерческой тайне», 152-ФЗ «О персональных данных», 149-ФЗ «Об информации, информационных технологиях и защите информации» 2006 года с дополнениями 2014 года,187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Задачи:

1. Создать группу gBuh и выполнить регистрацию двух пользователей uBuh1 и uBuh2, включив их в созданную группу.
2. Создать рабочую папку FBuh. Предоставить полный доступ к папке только членам группы gBuh.
3. Создать папку Share с вложенными папками In и Out. Предоставить сетевой доступ к папкам по принципу: ..Share\In – только на запись, Share\Out – только на чтение.

4. Выполнить настройки парольной защиты: длина пароля, срок действия, сложность.
5. Выполнить регистрацию пользователя и предоставить ему административные права.
6. Выполнить регистрацию пользователя, включить пользователя в группу "Опытные пользователи". Создать рабочую папку для зарегистрированного пользователя в папке c:\work и предоставить только этому пользователю полный доступ к созданной папке.
7. Провести настройку входа в систему: в окне регистрации отображаются поля для ввода логина и пароля пользователя.
8. Настроить политику блокировки учетных записей: пороговое значение блокировки, продолжительность блокировки учетной записи.
9. Настроить политику аудита: Аудит входа в систему, Аудит системных событий.
10. Написать командный файл, выполняющий регистрацию пользователя. Имя пользователя (логин) и пароль должны вводиться по запросу.
11. Написать командный файл, который добавляет новую группу и регистрирует в этой группе пользователя. Имя группы и пользователя вводятся по запросу.
12. Написать командный файл, выводящий список зарегистрированных пользователей и формирующий запрос на удаление пользователя: имя удаляемого запрашивается.
13. Выполнить отключение служб:
    - Удаленный реестр.
    - Удаленные рабочие столы.
    - Вспомогательный IP.
    - Удаленный реестр (его лучше отключать даже в том случае, если вы работаете в сети).
    - Модуль NetBios.
    - Браузер персональных компьютеров.
    - Сервер.
    - Поставщик домашних групп.
14. Выполните поиск законодательных актов по запросу "Информационная безопасность", "Защита персональных данных".
15. Изучить поправки в закон о персональных данных источни https://kontur.ru/articles/4816
16. Написать программу, реализующую простейший генератор паролей по заданному условию с использованием генератора случайных чисел: пользователь вводит последовательность символов a1,a2,….aN идентификатор с клавиатуры, где N-количество символов идентификатора(может быть любым), ai –i-символ идентификатора пользователя. Условие: сформировать пароль пользователя b1,b2,….bM , где

    2)M=6 количество символов пароля, b1,b2 , b3 – случайные малые буквы английского алфавита, b4 ,b5 – случайные заглавные буквы английского алфавита, b6 - двузначные числа, равные N4 mod100(если остаток –однозначное число, то b6=0).

    3)M=8 количество символов пароля, b1,b2 , b3 – случайные цифры, b4 ,b5 – случайные цифры из множества {!, “,#,$,%,&,’,(,),*}, b6,b7 - случайные заглавные буквы английского алфавита, ,b8 –P-ая по счету малая буква английского алфавита, где P=N2mod10+N3 mod10+1

    4)M=9 количество символов пароля, b1,b2 , b1+Q – случайные символы из множества {!, “,#,$,%,&,’,(,),*}, где Q=Nmod5. Оставшиеся символы пароля, кроме b9 - случайные малые буквы английского алфавита; b9- случайная цифра.

    6)M=11 количество символов пароля, b1,b2 – случайные цифры, b3,b3+Q случайные большие буквы английского алфавита, где Q=Nmod8; b4+Q… b11 - случайные символы из множества {!, “,#,$,%,&,’,(,),*}.

    7)M=11 количество символов пароля, b1,b2 – случайные цифры, b3,b3+Q случайные малые буквы русского алфавита, где Q=Nmod8; b4+Q… b11 - случайные символы из множества {!, “,#,$,%,&,’,(,),*}.

    8)M=12 количество символов пароля, b1,b1+Q – случайные малые буквы английского алфавита, где Q=N3mod5; b1+ Q +1…. b1+Q+1+P - случайные большие буквы

английского алфавита, где P= N2mod6. Оставшиеся символы пароля- случайные цифры.
9)M=12 количество символов пароля, b1,b1+Q – случайные малые буквы русского алфавита, где Q=N3mod5; b1+ Q +1…. b1+Q+1+P - случайные большие буквы русского алфавита, где P= N2mod6. Оставшиеся символы пароля- случайные цифры.
10)M=10 количество символов пароля, b10-Q,b10 – случайные цифры, где Q=Nmod6; b1,b2 - случайные большие буквы русского алфавита, b3…. b10-Q-1 - случайные малые буквы русского алфавита.
11)M=9 количество символов пароля, b1,b2 , b1+Q – случайные символы из множества {!, “,#,$,%,&,’,(,),*}, где Q=Nmod5. Оставшиеся символы пароля, кроме b9 - случайные малые буквы русского алфавита; b9- случайная цифра.
12)M=8 количество символов пароля, b1,b2 , b3 – случайные цифры, b4,b5, b6– случайные цифры из множества {!, “,#,$,%,&,’,(,),*}, b7 – случайная заглавная буква русского алфавита, ,b8 –P-ая по счету малая буква русского алфавита, где P=N2mod15+N3 mod15+1
13)M=7 количество символов пароля, b1,b2 , b3 – случайные малые буквы русского алфавита, b4 ,b5 – случайные заглавные буквы русского алфавита, b6, b7 - двузначные числа, равные N4 mod100(если остаток –однозначное число, то b6=0).
14)M=6 количество символов пароля, b1,b2 – случайные заглавные буквы русского алфавита, b3=N2mod10, (mod10 –остаток от деления числа на 10), b4 – случайная цифра; b5 – случайный символ из множества {!, “,#,$,%,&,’,(,),*}, b6- случайная малая буква русского алфавита.
15)M=6 количество символов пароля, b1,b2 – случайные заглавные буквы английского алфавита, b3=N2mod10, (mod10 –остаток от деления числа на 10), b4 – случайная цифра; b5 – случайный символ из множества {!, “,#,$,%,&,’,(,),*}, b6- случайная малая буква английского алфавита.

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Кафедра «Информационные системы и технологии»

20__– 20__учебный год

Экзаменационный билет № _____

по дисциплине Комплексная информационная безопасность

для обучаемых направления подготовки 09.04.03 Прикладная информатика

1. Содержание и структура понятия «обеспечение информационной безопасности».

2. Безопасность систем электронного документооборота в банковском учреждении.

3. Создать рабочую папку FBuh. Предоставить полный доступ к папке только членам группы gBuh.

Зав. кафедрой Кумратова А.М.

Вопросы для устного опроса

по дисциплине Комплексная информационная безопасность

1. Требования руководящих документов по порядку разработки и содержанию «Положения о подразделении (специалисте) по защите информации».
2. Организационные мероприятия, проводимые с целью защиты СВТ и АС от НСД.
3. Четыре основные составляющие национальных интересов РФ в информационной сфере.
4. Требования руководящих документов по порядку разработки и содержанию «Руководства по защите информации …».
5. Внешние источники угроз безопасности информации.
6. Типовой перечень внутренних организационно-распорядительных документов по защите конфиденциальной информации.
7. Внутренние источники угроз безопасности информации.
8. Основные направления обеспечения защиты информации от НСД.
9. Положение по аттестации объектов информатизации.
10. Основные принципы защиты информации от НСД.
11. Порядок согласования и утверждения Руководства по защите информации.
12. В чем заключаются интересы личности в информационной сфере
13. В чем заключаются интересы общества в информационной сфере
14. В чем заключаются интересы государства в информационной сфере
15. Виды угроз
16. Внешние источники угроз
17. Внутренние источники угроз

Индивидуальные задания к практическим занятиям

по дисциплине Комплексная информационная безопасность

1. Создать группу gBuh и выполнить регистрацию двух пользователей uBuh1 и uBuh2, включив их в созданную группу.
2. Создать рабочую папку FBuh. Предоставить полный доступ к папке только членам группы gBuh.
3. Создать папку Share с вложенными папками In и Out. Предоставить сетевой доступ к папкам по принципу: ..Share\In – только на запись, Share\Out – только на чтение.
4. Выполнить настройки парольной защиты: длина пароля, срок действия, сложность.
5. Выполнить регистрацию пользователя и предоставить ему административные права.
6. Выполнить регистрацию пользователя, включить пользователя в группу "Опытные пользователи". Создать рабочую папку для зарегистрированного пользователя в папке c:\work и предоставить только этому пользователю полный доступ к созданной папке.
7. Провести настройку входа в систему: в окне регистрации отображаются поля для ввода логина и пароля пользователя.
8. Настроить политику блокировки учетных записей: пороговое значение блокировки, продолжительность блокировки учетной записи.
9. Настроить политику аудита: Аудит входа в систему, Аудит системных событий.
10. Написать командный файл, выполняющий регистрацию пользователя. Имя пользователя (логин) и пароль должны вводиться по запросу.
11. Написать командный файл, который добавляет новую группу и регистрирует в этой группе пользователя. Имя группы и пользователя вводятся по запросу.
12. Написать командный файл, выводящий список зарегистрированных пользователей и формирующий запрос на удаление пользователя: имя удаляемого запрашивается.
13. Выполнить отключение служб:

- Удаленный реестр.
- Удаленные рабочие столы.
- Вспомогательный IP.
- Удаленный реестр (его лучше отключать даже в том случае, если вы работаете в сети).
- Модуль NetBios.
- Браузер персональных компьютеров.
- Сервер.
- Поставщик домашних групп.

Тестовые задания для входного контроля

по дисциплине Комплексная информационная безопасность

Цель входного контроля – определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания обучаемого используются как начальные значения в индивидуальном профиле академической успешности обучаемого.

Форма проведения – тестирование.

Длительность тестирования – 45 минут.

Задание для входного тестирования

Выбрать из предложенных вариантов ответа один верный:

1. За единицу количества информации принимается:

a) Байт;
b) Код;
c) Бит;
d) Бод;

2. В какой из последовательностей единицы измерения указаны в порядке возрастания:

a) гигабайт, мегабайт, килобайт, байт;
b) мегабайт, килобайт, байт, гигабайт;
c) гигабайт, килобайт, мегабайт, байт;
d) байт, килобайт, мегабайт, гигабайт;

3. Свойство информации, определяющее ее достаточность для принятия решения называется:

a) Достоверность;
b) Адекватность;
c) Полнота;
d) Доступность;

4. Укажите количество бит в сообщении объемом четверть килобайта

a) 250;
b) 512;
c) 2000;
d) 2048;

5. Комплекс аппаратных и программных средств, позволяющих компьютерам обмениваться данными, – это:

a) Магистраль;
b) Шина данных;
c) Компьютерная сеть;
d) Интерфейс;

6. Глобальная компьютерная сеть – это;

a) множество компьютеров, связанных каналами передачи информации и находящихся в пределах одного помещения, здания;
b) совокупность хост - компьютеров и файл-серверов;
c) совокупность локальных сетей и компьютеров, расположенных на больших расстояниях и соединенных с помощью каналов связи в единую систему;
d) информационная система с гиперсвязями;

7. Аппаратное подключение периферийного устройства к магистрали производится через:

a) Регистр;
b) Драйвер;

c) Контроллер;
d) Стример;

8. Охарактеризуйте понятие «кэш-память»

a) память, предназначенная для долговременного хранения информации, независимо от того, работает ЭВМ или нет;
b) это сверхоперативная память, в которой хранятся наиболее часто используемые участки оперативной памяти;
c) память, в которой хранятся системные файлы операционной системы;
d) память, в которой обрабатывается одна программа в данный момент времени;

9. При выключении компьютера вся информация стирается:

a) на гибком диске;
b) на CD-диске;
c) на жестком диске;
d) в оперативной памяти;

10. Устройством ввода является...

a) Сканер;
b) Принтер;
c) Стример;
d) Дисплей;

11. Что является характеристикой монитора? ...

a) цветовое разрешение;
b) тактовая частота;
c) дискретность;
d) время доступа к информации;

12. К прикладному программному обеспечению не относятся:

a) текстовые процессоры;
b) СУБД;
c) Операционные оболочки;
d) Игры;

13. Минимальным объектом, используемым в растровом графическом редакторе, является...

a) точка экрана (пиксель);
b) объект (прямоугольник, круг и т.д.);
c) палитра цветов;
d) знакоместо (символ);

14. Минимальным объектом, используемым в векторном графическом редакторе, является...

a) точка экрана (пиксель);
b) объект (прямоугольник, круг и т.д.);
c) палитра цветов;
d) знакоместо (символ);

15. Программа Excel используется для...

a) создания текстовых документов;
b) создания электронных таблиц;
c) создания графических изображений;
d) все варианты верны;

16. Адрес диапазона ячеек в Excel задаётся указанием:

a) ссылок первой и последней его ячеек;
b) указанием имени листа;
c) указанием имени файла;
d) указанием адреса последней ячейки;

17. Свойство алгоритмов, означающие, что результат выполнения алгоритма не зависит от исполнителя, а определяется только входными данными и шагами:

a) Результативность;
b) Детерминированность;
c) Дискретность:
d) Определенность.

18. Совокупность данных, сохраняемых внутри некоторой системы, – это информация

a) Внешняя;
b) Выходная;
c) Внутренняя;
d) Промежуточная;

19. Охарактеризуйте понятие «модель системы»:

a) описание системы, отображающее определенную группу ее свойств;
b) возникновение и сохранение структуры и целостных свойств системы;
c) множество существенных свойств, которыми система обладает в данный момент времени;
d) порядок системы;

20. Осуществляет сбор, передачу и переработку информации об объекте:

a) информационное пространство;
b) информационная система;
c) информационная среда;
d) информационный рынок;

21. Хранение и поиск информации являются фундаментальными функциями:

a) локальных баз данных;
b) корпоративных информационных систем;
c) справочной системы;
d) автоматизированных информационных систем;

22. Свойство производительности информационной системы – это:

a) время отклика на запрос клиента;
b) максимальное использование ресурсов памяти компьютеров;
c) максимальное использование возможностей аппаратного обеспечения информационной системы;
d) пропускная способность информационной системы;

23. Корпоративные информационные системы – это:

a) информационная система, осуществляющая бизнес в Интернете;
b) информационная система, предоставляющая услуги по доступу в Интернет;
c) компьютерная сеть корпорации;
d) информационная система, обеспечивающая работу корпорации;

24. Распределенные информационные системы могут быть:

a) клиент-серверными или файл-серверными;
b) корпоративными или вычислительными;
c) автоматизированными или клиент-серверными;
d) персональными или экономическими;

25. Для ввода, обработки, хранения и поиска графических образов бумажных документов, предназначены:

a) системы управления проектами;
b) системы автоматизации деловых процедур;
c) системы обработки изображений документов;
d) системы оптического распознавания символов;

26. Для управления файлами и папками в ОС Windows можно использовать

a) программу проводник;
b) панель задач;
c) панель управления;
d) меню кнопки «Пуск»;

27. World Wide Web – это служба Интернет, предназначенная для:

a) поиска и просмотра гипертекстовых документов, включающих в себя графику, звук и

видео;
b) передачи файлов;
c) передачи электронных сообщений;
d) общения в реальном времени с помощью клавиатуры;

28. Охарактеризуйте термин COM:

a) программные компоненты;
b) коммерческий сервер;
c) коммутатор;
d) среда объектно-ориентированного программирования;

29. Охарактеризуйте термин структура системы:

a) совокупность элементов и связей между ними;
b) совокупность подсистем;
c) описание системы, отображающее определенную группу ее свойств;
d) порядок системы;

30. Охарактеризуйте какие функции не выполняют информационные системы:

a) информационно-справочные;
b) Контрольные;
c) Расчетные;
d) Организационные.

Тестовые вопросы

по дисциплине Комплексная информационная безопасность

Раздел 1. Понятия безопасности информационных технологий. Нормативная база обеспечения информационной безопасности.

1. Укажите какие два слова пропущены в следующей фразе(ПК-2)

«Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации- это _____ _____.»

2. Административный уровень знаний комплексной информационной безопасности включает (ПК-2):

1)Комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации;

2) Комплекс мероприятий, реализующих практические механизмы уничтожения защищаемой информации с истекшим сроком хранения;

3) Комплекс мероприятий, реализующих практические механизмы эксплуатации систем защиты информации;

4) Комплекс приказов и распоряжений, устанавливающих степень ответственности работников организации при работе с защищаемой информацией.

3. Укажите какие два слова пропущены в следующей фразе(ПК-2)

«Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё - это _____ _____.»

Ответ: защита информации

4. Укажите что из перечисленного не относится к числу основных аспектов информационной безопасности (ПК-2):

1) Доступность;
2) Целостность;
3) Защита от копирования;
4) Конфиденциальность.

5.Укажите что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных (ПК-2)

1) Безопасная OECD;
2) ISO\IEC;
3) OECD;
4) CPTED.

6. Укажите какое из указанных ниже действий следует предпринять руководству если различным группам пользователей с различным уровнем доступа требуетсядоступ к одной и той же информации (ПК-2)

1) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;

2) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;

3)Улучшить контроль за безопасностью этой информации;

4) Снизить уровень классификации этой информации.

7.Определите какое из следующих определений наиболее точно отражает понятие

«информационная безопасность» (ПК-2)

a) Состояние защищенности информации от всех возможных угроз.
b) Состояние защищенности информации, при котором обеспечиваются её конфиденциальность, целостность и доступность (триада CIA).
c) Процесс установки антивирусного программного обеспечения и межсетевого экрана.
d) Набор законов, запрещающих несанкционированный доступ к данным.

8.Определите что из перечисленного является ключевым принципом (свойством) информационной безопасности, означающим гарантию того, что информация не будет раскрыта неавторизованным лицам(ПК-2)

a) Целостность (Integrity).
b) Конфиденциальность (Confidentiality).
c) Доступность (Availability).
d) Подотчетность (Accountability).

9.Определите какой из перечисленных документов является базовым законом Российской Федерации в сфере защиты информации(ПК-2)

a) ГОСТ Р ИСО/МЭК 27001.
b) Приказ ФСТЭК России №17.
c) Федеральный закон №152-ФЗ «О персональных данных».
d) Уголовный кодекс РФ, глава 28.

10. Определите какой международный стандарт определяет требования к системе менеджмента информационной безопасности (СМИБ) (ПК-2)

a) ISO 9001.
b) ISO/IEC 27001.
c) PCI DSS.
d) ГОСТ Р 34.

Раздел 2. Защита от несанкционированного доступа к информации.

1. Укажите пропущенное слово в предложении (ПК- 2)

«Широкие, высокоуровневые заявления руководства - _____ безопасности.»
Ответ: политика

2. Информация по способу доступа к ней бывает (ПК-2):

1. открытая (общедоступная) и закрытая (конфиденциальная);
2. избыточная, достаточная и недостаточная;
3. исходная, промежуточная и результирующая;
4. постоянная, переменная и смешанная

3. Укажите как называются отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (ПК-2):

1) Информационные ресурсы;
2) Реляционная база данных;
3) Файловая база данных;
4) D-дерево.

4. Укажите кто является основным ответственным за определение уровня классификацииинформации по степени важности (ПК-2)

1) Руководитель среднего звена;
2) Руководитель организации или замещающее его лицо;
3) Владелец;
4) Пользователь.

5. Укажите что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности (ПК-2)

1) Поддержка;
2) Выполнение анализа рисков;
3) Определение цели и границ;
4) Делегирование полномочий.

6. Для подтверждения того факта, что данный открытый ключ принадлежит конкретному лицу и никому другому служит (ПК-2):

1) Сертификат;
2) Дайджест;
3) Контрольная сумма.

7. Определите что является примером аутентификации по фактору «то, что вы знаете» (ПК-2)

a) Смарт-карта.
b) Отпечаток пальца.
c) Пароль или PIN-код.
d) Голос.

8. Определите какой принцип разграничения доступа предполагает, что права субъекта на доступ к объекту определяются на основе статичной матрицы «субъект-объект» (ПК-2)

a) Ролевой (Role-Based Access Control, RBAC).
b) Дискреционный (Discretionary Access Control, DAC).
c) «Модель дискреционного управления доступом (модель Харрисона-Рузо-Ульмана)».

9. Укажите какой тип межсетевого экрана (МЭ) анализирует состояние активных соединений и принимает решения на основе контекста (порт, состояние TCP-сессии) (ПК-2)

a) Пакетный фильтр (Packet Filtering Firewall).
b) МЭ с проверкой состояний (Stateful Inspection Firewall).
c) Прикладной шлюз (Application-level Gateway/Proxy).
d) МЭ экспертного уровня.

10. Охарактеризуйте «принцип минимальных привилегий» (Principle of Least Privilege) (ПК-2)

a) Назначение пользователю только тех прав, которые ему необходимы для выполнения его рабочих задач.
b) Запрет на использование простых паролей.
c) Обязательное шифрование всех данных.

Раздел 3. Модель угроз и модель нарушителей информационной безопасности.

1. Укажите какое слово пропущено в следующей фразе(ПК-2)

«Субъект (лицо или группа лиц), реализующий угрозы информационной безопасности организации (по ошибке, незнанию или осознанно), путем нарушения предоставленных ему полномочий по доступу к активам организации или по распоряжению ими – это _____ информационной безопасности.»

Ответ: нарушитель

2. Системы, которые используют два математически связанных друг с другом ключа, называют (ПК-2):

1) асимметричными;
2) симметричным;
3) квадратурными;
4) циклическими.

3.Искусственные угрозы безопасности информации вызваны(ПК-2):
1) Деятельностью человека;
2) Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4) Корыстными устремлениями злоумышленников;
5) Ошибками при действиях персонала.

4. Укажите пропущенное слово в следующем предложении (ПК-2)
«Наиболее рискованной для организации с точки зрения вероятного мошенничества и нарушения безопасности является категория людей -_____ организации.»
Ответ: сотрудники

5. Укажите какая наука пропущена в следующем предложении (ПК-2)
«Поиском и исследованием математических методов преобразования информации занимается _____.»
Ответ: криптография
6. Укажите какое слово пропущено в следующем предложении(ПК-2)
«Открытый стандарт, определяющий цели контроля и относящийся к программам безопасности называется _____.»
Ответ: COBIT

7.Укажите что является конечным результатом процесса моделирования угроз информационной безопасности(ПК-2)
1) Список установленного программного обеспечения.
2) Структурированный перечень потенциальных угроз с оценкой их вероятности и последствий.
3) План эвакуации персонала.
4) Перечень всех сотрудников компании.

8.Укажите к какой категории нарушителей обычно относятся хакеры, действующие из идеологических или политических побуждений(ПК-2)
1) Внешний нарушитель с низким потенциалом (любопытствующий).
2) Внешний нарушитель с высоким потенциалом (кибертеррорист, хактивист).
3) Внутренний нарушитель по неосторожности.
4) Внутренний злоумышленник (недовольный сотрудник).

9.Укажите какой компонент модели угроз описывает уязвимость, которая может быть использована для реализации угрозы(ПК-2)
a) Актив (Asset).
b) Слабость (Vulnerability).
c) Угроза (Threat).
d) Риск (Risk).

10.Определите что из перечисленного является примером внутреннего нарушителя(ПК-2)

a) Конкурент, пытающийся похитить коммерческую тайну.
b) Бывший сотрудник, использующий старый пароль для доступа.
c) Случайный посетитель сайта.
d) Автоматизированный бот для сканирования портов.

Раздел 4. Аудит и оценка возможных рисков ИБ

1.Укажите когда целесообразно не предпринимать никаких действий в отношении выявленных рисков (ПК-5)

1) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;
2) Когда риски не могут быть приняты во внимание по политическим соображениям;
3) Когда необходимые защитные меры слишком сложны;
4)Когда стоимость контрмер превышает ценность актива и потенциальные потери.

2.Укажите какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой (ПК-5)

5) Анализ связующего дерева;
6) AS/NZS;
7) NIST;
8) Анализ сбоев и дефектов.

3. Укажите что из перечисленного не является целью проведения анализа рисков (ПК-5)

1) Делегирование полномочий;
2) Количественная оценка воздействия потенциальных угроз;
3) Выявление рисков;
4) Определение баланса между воздействием риска и стоимостью необходимых контрмер.

4. Укажите какое слово пропущено в следующем предложении (ПК-5)
«Перехват данных является угрозой _____.»
Ответ: конфиденциальности
5. Укажите какое слово пропущено в следующем предложении(ПК-5)
«_____- данный антивирус не только находит зараженные вирусами файлы, но и «лечит» их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние (ПК-5).
Ответ:доктор

6.Укажите основную цель проведения качественной оценки рисков информационной безопасности(ПК-5)
a) Получить точную финансовую оценку возможного ущерба в рублях.
b) Ранжировать риски по уровням (например, Высокий/Средний/Низкий) для определения приоритетов обработки.
c) Составить полный список всего оборудования.
d) Нанять новых специалистов по безопасности.

7.Определите какой этап процесса управления рисками следует непосредственно за этапом «Идентификация рисков» (ПК-5)
a) Мониторинг и пересмотр.
b) Анализ и оценка рисков.
c) Обработка (снижение) рисков.
d) Игнорирование рисков.

8.Определите понятие «приемлемый риск» в контексте управления рисками ИБ(ПК-5)

a) Риск, вероятность которого равна нулю.
b) Риск, который технически невозможно снизить.
c) Риск, уровень которого организация сознательно принимает, так как затраты на его дальнейшее снижение превышают возможный ущерб.
d) Риск, о котором руководство не знает.

8.Укажите какой из методов обработки рисков предполагает передачу финансовой ответственности за последствие реализации риска третьей стороне (например, страховой компании) (ПК-5)
a) Снижение (Mitigation).
b) Передача (Transfer).
c) Избегание (Avoidance).
d) Принятие (Acceptance).

Раздел 5. Основные типы атак на информационные системы, основные меры противодействия.

1. В алгоритмах этого вида и для шифрования, и для дешифрования информации применяется один и тот же секретный ключ (ПК-5):
1) Симметричные алгоритмы;
2) Ассиметричные алгоритмы;
3) Алгоритмы Ньютона-Дирихле.

2.**Во время войны с галлами Ю.Цезарь (102-44 г. до н.э.) использовал (ПК-5):**
1) Шифр замены;
2) Шифр подмены;
3) Шифр перестановки.

3. SNMP – протокол позволяет (ПК-5):
1) управлять конфигурацией оборудования в сети;
2) соединять сетевые приложения;
3) обмениваться служебной информацией маршрутизаторам.

4.Укажите какой уровень стека протоколов TCP/IP определяет маршрут между компьютерами, находящимися в разных сетях (ПК-5)
1) Сетевой;
2) Транспортный;
3) Физический;
4) Канальный.
5.**Алгоритм, преобразующий массив входных данных произвольной длины в (выходную) битовую строку фиксированной длины называют (ПК-5):**
1) Хэш-функцией;
2) Бит-функцией;
3) Байт-функцией;
4) Алгоритмом Френеля.
6. Укажите какое слово пропущено в следующей фразе(ПК-5)
«Порт транспортного протокола (называемый также сокетом или сеансом в других протоколах), подобен _____ каналу между двумя коммуникационными процессами.»)
Ответ:виртуальному
7. Укажите какая из приведенных техник является самой важной при выборе конкретных защитных мер (ПК-5):
1) Анализ рисков;

2)Анализ затрат / выгоды;
3) Результаты ALE;
4) Выявление уязвимостей и угроз, являющихся причиной риска.

8.Укажите какая атака направлена на переполнение буфера приложения с целью выполнения произвольного кода(ПК-5)

a) Фишинг (Phishing).
b) **Атака на основе переполнения буфера (Buffer Overflow).**
c) DoS-атака.
d) SQL-инъекция.

9.Назовите атаку, при которой злоумышленник занимает позицию между двумя легитимными узлами и перехватывает/изменяет их трафик(ПК-5)

a) Спуфинг (Spoofing).
b) **Атака «человек посередине» (Man-in-the-Middle, MitM).**
c) Реверсивная разработка (Reverse Engineering).
d) Перехват сессии (Session Hijacking).

10.Определите какая основная мера защиты эффективна против атак типа «отказ в обслуживании» (DoS/DDoS) (ПК-5)

a) Установка антивируса на все рабочие станции.
b) **Использование специализированных аппаратно-программных комплексов (DDoS-фильтрация) и избыточность каналов связи.**
c) Шифрование жестких дисков.
d) Строгая парольная политика.

11.Определите против какого типа атак в первую очередь защищает корректное использование подготовленных выражений (prepared statements) при разработке веб-приложений(ПК-5)

a) Межсайтовый скриптинг (XSS).
b) **Внедрение SQL-кода (SQL-injection).**
c) Фишинг.
d) Подбор паролей (Brute-force).

5. Методические материалы, определяющие процедуры оценивания компетенции

1.1. Критерии оценки тестирования.

- от 0 до 49,9 % выполненного решения – неудовлетворительно;
- от 50% до 69,9% – удовлетворительно;
- от 70% до 89,9% – хорошо;
- от 90% до 100% – отлично

5.2 Критерии оценки устного опроса

Оценка «отлично» выставляется обучающемуся, если он свободно владеет терминологией, демонстрирует прекрасное знание предмета, соединяя при ответе знания из разных разделов дисциплины, добавляя комментарии, пояснения, может быстро и безошибочно проиллюстрировать ответ собственными примерами. Владеет аргументацией, грамотной, доступной и понятной речью.

Оценка «хорошо», владеет терминологией, делая ошибки, при неверном употреблении сам может их исправить, хорошо владеет содержанием изучаемой темы, видит взаимосвязи, может провести анализ, но не всегда делает это самостоятельно без помощи преподавателя, может подобрать соответствующие примеры, чаще из имеющихся в учебных материалах. Хорошая аргументация, четкость, лаконичность ответов.

Оценка «удовлетворительно», редко использует при ответе термины, подменяет одни понятия другими, не всегда понимая разницы, отвечает на конкретный вопрос соединяя знания только при наводящих вопросах преподавателя, с трудом может соотнести теорию и практические примеры из учебных материалов; примеры не всегда правильные. Слабая аргументация, нарушена логика при ответе, однообразные формы изложения мыслей.

Оценка «неудовлетворительно», при ответе не владеет профессиональной терминологией. Неуверенное и логически непоследовательно излагает материал, обнаруживает пробелы в знаниях основного учебного материала, не может привести примеры из учебной литературы, затрудняется с ответом на поставленные преподавателем вопросы.

5.3 Критерии оценки экзамена

Оценка «отлично» выставляется обучающемуся, если он свободно владеет терминологией, демонстрирует прекрасное знание предмета, соединяя при ответе знания из разных разделов дисциплины, добавляя комментарии, пояснения, может быстро и безошибочно проиллюстрировать ответ собственными примерами. Владеет аргументацией, грамотной, доступной и понятной речью.

Оценка «хорошо», владеет терминологией, делая ошибки, при неверном употреблении сам может их исправить, хорошо владеет содержанием изучаемой темы, видит взаимосвязи, может провести анализ, но не всегда делает это самостоятельно без помощи преподавателя, может подобрать соответствующие примеры, чаще из имеющихся в учебных материалах. Хорошая аргументация, четкость, лаконичность ответов.

Оценка «удовлетворительно», редко использует при ответе термины, подменяет одни понятия другими, не всегда понимая разницы, отвечает на конкретный вопрос соединяя знания только при наводящих вопросах преподавателя, с трудом может соотнести теорию и практические примеры из учебных материалов; примеры не всегда правильные. Слабая аргументация, нарушена логика при ответе, однообразные формы изложения мыслей.

Оценка «неудовлетворительно», при ответе не владеет профессиональной терминологией. Неуверенное и логически непоследовательно излагает материал, обнаруживает пробелы в знаниях основного учебного материала, не может привести примеры из учебной литературы, затрудняется с ответом на поставленные преподавателем вопросы.

5.4 Критерии оценки индивидуальных практических заданий:

оценка **«отлично»** выставляется обучающемуся, если даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно решены практические задания, при ответах выделялось главное, все теоретические положения умело увязывались с требованиями руководящих документов, ответы были четкими и краткими, а мысли излагались в логической последовательности, показано умение самостоятельно анализировать факты, события явления, процессы в их взаимосвязи и диалектическом развитии.

- оценка **«хорошо»** выставляется обучающемуся, если даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания; при ответах не всегда выделялось главное, отдельные положения недостаточно увязывались с требованиями руководящих документов; ответы в основном были краткими, но не всегда четкими и по существу;
- оценка **«удовлетворительно»** выставляется обучающемуся, если даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования; на уточняющие вопросы даны правильные ответы; при ответах невыделялось главное; ответы были многословными, нечеткими и без должной логической последовательности; на отдельные дополнительные вопросы не даны положительные ответы;
- оценка **«неудовлетворительно»** выставляется обучающемуся, если даны неправильные ответы на большинство вопросов; обучающийся путается в определениях и понятиях; не владеет практическими навыками решения задач.

.