Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Комарова Светлана Юриевна
Должность: Проректор по образовательной деятельности
Дата подписания: 27.11.2023 12:36:58
Уникальный программный ключ:
43ba42f5deae4116bbfcbb9ac98e39108034237c8fadd207cbee4149f2998d7a

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А.Столыпина»

Экономический факультет

ОПОП по направлению 38.03.01 Экономика

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по освоению учебной дисциплины

Б1.О.33 Информационная безопасность

Направленность (профиль) «Бухгалтерский учет, анализ и аудит»

Обеспечивающая преподавание дисциплины кафедра -	Экономики, бухгалтерского учета и финансового контроля
Разработчик, канд. экон. наук, доцент	В.В. Кузнецова

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1. Настоящее издание является основным организационно-методическим документом учебно-методического комплекса по дисциплине в составе основной профессиональной образовательной программы высшего образования (ОПОП ВО). Оно предназначено стать для них методической основой по освоению данной дисциплины.

2. Содержательной основой для разработки настоящих методических указаний послужила Рабочая программа дисциплины, утвержденная в установленном порядке.

3. Методические аспекты развиты в учебно-методической литературе и других разработках, входящих в состав УМК по данной дисциплине.

4. Доступ обучающихся к электронной версии Методических указаний по изучению дисциплины, обеспечен в информационно-образовательной среде университета.

При этом в электронную версию могут быть внесены текущие изменения и дополнения, направленные на повышение качества настоящих методических указаний.

Уважаемые обучающиеся!

Приступая к изучению новой для Вас учебной дисциплины, начните с вдумчивого прочтения разработанных для Вас кафедрой специальных методических указаний. Это поможет Вам вовремя понять и правильно оценить ее роль в Вашем образовании.

Ознакомившись с организационными требованиями кафедры по этой дисциплине и соизмерив с ними свои силы, Вы сможете сделать осознанный выбор собственной тактики и стратегии учебной деятельности, уберечь самих себя от неразумных решений по отношению к ней в начале семестра, а не тогда, когда уже станет поздно. Используя эти указания, Вы без дополнительных осложнений подойдете к промежуточной аттестации по этой дисциплине. Успешность аттестации зависит, прежде всего, от Вас. Ее залог – ритмичная, целенаправленная, вдумчивая учебная работа, в целях обеспечения которой и разработаны эти методические указания.

1. Место учебной дисциплины в подготовке выпускника

Учебная дисциплина относится к дисциплинам ОПОП университета, состав которых определяется вузом и требованиями ФГОС.

Цель дисциплины – формирование у студентов базовых теоретических знаний и практических профессиональных навыков в области информационной безопасности в рамках решения профессиональных задач.

В ходе освоения дисциплины обучающийся должен:

Иметь способность применять знания (на промежуточном уровне) экономической теории при решении прикладных задач;

владеть:

- владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации;

знать:

- современные информационные технологии и программные средства и применяет для поиска и обработки экономической информации

уметь:

- использует современные информационные технологии и программные средства для поиска и обработки экономической информации.

1.1.Перечень компетенций с указанием этапов их формирования в результате освоения учебной дисциплины:

Компетенции, в формировании которых задействована дисциплина		**Код и наименование индикатора достижений компетенции**	**Компоненты компетенций,** формируемые в рамках данной дисциплины (как ожидаемый результат ее освоения)		
код	наименование		знать и понимать	уметь делать (действовать)	владеть навыками (иметь навыки)
1			2	3	4
Профессиональные компетенции					
ОПК-5	Способность применять знания (на промежуточном уровне) экономической теории при решении прикладных задач;	ИД-1$_{опк-5}$ применяет современные информационные технологии и программные средства для поиска и обработки экономической информации	современные технические средства и информационные технологии для анализа информационной безопасности социальных сетей и платежных систем	использовать современные технические средства и информационные технологии для поиска и обработки экономической информации	владеть навыками применения современных технических средств и информационных технологий для поиска и обработки экономической информации

1.2. Описание показателей, критериев и шкал оценивания и этапов формирования компетенций в рамках дисциплины

Индекс и название компетенции	Код индикатора достижений компетенции	Индикаторы компетенции	Показатель оценивания – знания, умения, навыки (владения)	Уровни сформированности компетенций				Формы и средства контроля формирования компетенций
				компетенция не сформирована	минимальный	средний	высокий	
				Оценки сформированности компетенций				
				2	3	4	5	
				Оценка «неудовлетворительно»	*Оценка «удовлетворительно»*	*Оценка «хорошо»*	*Оценка «отлично»*	
				Характеристика сформированности компетенции				
				Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач	
Критерии оценивания								
ОПК -5	ИД-1$_{опк-5}$	Полнота **знаний**	современные информационные технологии и программные средства для поиска и обработки экономической информации	Не знает современные информационные технологии и программные средства для поиска и обработки экономической информации	Знаком с современными информационными технологиями и программными средствами для поиска и обработки экономической информации	Знает современные информационные технологии и программные средства	Знает современные информационные технологии и программные средства и применяет для поиска и обработки экономической информации	Тестирование; опрос; индивидуальное задание, контрольная работа для заочной формы, презентация для очной и очно-заочной формы
		Наличие **умений**	использовать современные информационные технологии и программные средства для поиска и обработки экономической информации	Не умеет использовать современные информационные технологии и программные средства для поиска и обработки экономической информации	Умеет использовать информационные технологии	Умеет использовать современные информационные технологии и программные средства	В совершенстве использует современные информационные технологии и программные средства для поиска и обработки экономической информации	
		Наличие **навыков** (владение опытом)	навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	Не владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	Владеет навыками применения информационных технологий и программными средствами	Владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	В совершенстве владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	

2. Структура учебной работы, содержание и трудоёмкость основных элементов дисциплины

2.1 Организационная структура, трудоемкость и план изучения дисциплины

Вид учебной работы	Трудоемкость, час			
	семестр, курс*			
	очная / очно-заочная форма		заочная форма	
	3 сем.	4 сем.	2 курса	3 курса
1. Аудиторные занятия, всего	70	28	2	12
- лекции	24	10	2	4
- практические занятия (включая семинары)			-	
- лабораторные работы	46	18	-	8
2. Внеаудиторная академическая работа	74	116	34	92
2.1 Фиксированные виды внеаудиторных самостоятельных работ:				
Выполнение и сдача/защита индивидуального/группового задания в виде**				
- контрольной работы для заочной формы обучения				10
- электронной презентации для очной и очно-заочной форм обучения	10	10		
2.2 Самостоятельное изучение тем/вопросов программы	-	40	34	46
2.3 Самоподготовка к аудиторным занятиям	38	46	-	16
2.4 Самоподготовка к участию и участие в контрольно-оценочных мероприятиях, проводимых в рамках текущего контроля освоения дисциплины (*за исключением учтённых в пп. 2.1 – 2.2):*	26	20	-	20
3. Получение дифференцированного зачёта по итогам освоения дисциплины	+	+	-	4
ОБЩАЯ трудоемкость дисциплины: **Часы**	**144**	**144**	**144**	
Зачетные единицы	**4**	**4**	**4**	

Примечание:
* – ***семестр*** – для очной и очно-заочной формы обучения, ***курс*** – для заочной формы обучения;
** – КР/КП, реферата/эссе/презентации, контрольной работы (для обучающихся заочной формы обучения), расчетно-графической (расчетно-аналитической) работы и др.;

2.2. Укрупнённая содержательная структура учебной дисциплины и общая схема её реализации в учебном процессе

Номер и наименование раздела учебной дисциплины. Укрупнённые темы раздела		Трудоемкость раздела и её распределение по видам учебной работы, час.							Форма рубежного контроля по разделу	№№ компетенций, на формирование которых ориентирован раздел
		Общая	Аудиторная работа				ВАРС			
			всего	лекции	занятия		всего	Фиксированные виды		
					практические (всех форм)	лабора-торные				
1		2	3	4	5	6	7	8	10	11
Очная форма обучения										
1	Основы теории информационной безопасности	14	8	4	-	4	6	-	тестирование	ОПК-5
	Основные понятия и положения.	14	8	4	-	4	6	-		
2	Ведение в криптографию. Правовое и организационное обеспечение информационной безопасности.	32	22	8	-	14	10	-	тестирование	ОПК-5
	Криптография как способ защиты информации	14	10	4	-	6	4	-		
	Правовое и организационное обеспечение информационной безопасности	18	12	4	-	8	6	-		
3	Меры защиты информации	96	40	12	-	28	56		тестирование	ОПК-5
	Физические и аппаратные меры защиты информации	44	20	6	-	14	24	10		
	Разрушающие программные воздействия	52	20	6	-	14	32	-		
	Промежуточная аттестация		×	×	×	×	×	×	Диф. зачет	
Итого по учебной дисциплине		**144**	**70**	**24**		**46**	**74**	**10**		

Доля лекций в аудиторных занятиях, %			34							
Заочная форма обучения										
1	Основы теории информационной безопасности	12	2		-	2	10	-	тестирование	ОПК-5
	Основные понятия и положения.	12	2		-	2	10	-		
2	Ведение в криптографию. Правовое и организационное обеспечение информационной безопасности.	28	2		-	2	26	-	тестирование	ОПК-5
	Криптография как способ защиты информации	16	2	2	-	-	14	-		
	Правовое и организационное обеспечение информационной безопасности	14	2		-	2	12	-		
3	Меры защиты информации	104	8	4	-	4	90	10	тестирование	ОПК-5
	Физические и аппаратные меры защиты информации	50	4	2	-	2	46	10		
	Разрушающие программные воздействия	48	4	2	-	2	44	-		
	Промежуточная аттестация		×	×	×	×	×	×	Диф. зачет	
Итого по учебной дисциплине		**144**	**14**	**6**	**-**	**8**	**126**	**10**		
Доля лекций в аудиторных занятиях, %			43							
Очно-заочная форма										
1	Основы теории информационной безопасности	14	4	2	-	2	10		тестирование	ОПК-5
	Основные понятия и положения.	14	4	2	-	2	10			
2	Ведение в криптографию. Правовое и организационное обеспечение информационной безопасности.	34	6	2	-	4	28		тестирование	ОПК-5
	Криптография как способ защиты информации	16	3	1	-	2	13			
	Правовое и организационное обеспечение информационной безопасности	18	3	1	-	2	15			
3	Меры защиты информации	96	18	6	-	12	78	10	тестирование	ОПК-5
	Физические и аппаратные меры защиты информации	44	10	4	-	6	34	10		
	Разрушающие программные воздействия	52	8	2	-	6	44			
	Промежуточная аттестация		×	×	×	×	×	×	Диф. зачет	
Итого по учебной дисциплине		**144**	**28**	**10**	**-**	**18**	**116**	**10**		
Доля лекций в аудиторных занятиях, %			35							

3. Общие организационные требования к учебной работе обучающегося

3.1. Организация занятий и требования к учебной работе обучающегося

Организация занятий по дисциплине носит циклический характер. По трем разделам предусмотрена взаимоувязанная цепочка учебных работ: лекция – самостоятельная работа обучающихся (аудиторная и внеаудиторная). На занятиях студенческая группа получает задания и рекомендации.

Для своевременной помощи обучающимся при изучении дисциплины кафедрой организуются индивидуальные и групповые консультации, устанавливается время приема выполненных работ.

Учитывая статус дисциплины к её изучению предъявляются следующие организационные требования;:

- обязательное посещение обучающимся всех видов аудиторных занятий;
- ведение конспекта в ходе лекционных занятий;
- качественная самостоятельная подготовка к практическим занятиям, активная работа на них;
- активная, ритмичная самостоятельная аудиторная и внеаудиторная работа обучающегося;
- в случае наличия пропущенных обучающимся занятиям, необходимо получить консультацию по подготовке и оформлению отдельных видов заданий.

Для успешного освоения дисциплины, обучающемуся предлагаются учебно-информационные источники в виде учебной, учебно-методической литературы по всем разделам.

4. Лекционные занятия

Для изучающих дисциплину читаются лекции в соответствии с планом, представленным в таблице 3.

Таблица 3

№ раздела	№ лекции	Тема лекции. Основные вопросы темы	Трудоемкость по разделу, час. Очная форма	Очно-заочная форма	Заочная форма	Применяемые интерактивные формы
1	1	Основные положения теории информационной безопасности. 1. Основные понятия в сфере информационной безопасности. 2. Угрозы информационной безопасности. 3. Основные методы обеспечения информационной безопасности	4	2		
2	2	Криптография как способ защиты информации. 1. Основные понятия криптографии и криптоанализа. 2. История криптографии. 3. Методы шифрования. 4. Электронная цифровая подпись. 5. Стенография.	4	2	2	
2	3	Правовое и организационное обеспечение информационной безопасности. 1. Конституция РФ об информационной безопасности. 2. Стратегические и доктринальные документы в области информационной безопасности. 3. Законодательство РФ об информационной безопасности. 4. Подзаконные акты по вопросам информационной безопасности. 5. Организационное обеспечение информационной безопасности.	4	2		Лекция-беседа
3	4	Физические и аппаратные меры защиты информации. 1. Технические каналы утечки информации. 2. Системы видеонаблюдения. 3. Тепловидение. 4. Системы контроля доступа. 5. Электронные ключи. 6. Программно-аппаратные комплексы.	6	2	2	Лекция-беседа (для ФЗО)
3	5	Разрушающие программные воздействия. 1.Виды программного обеспечения. 2. Вирусы и программы антивирусной защиты 3. Технологии применения антивирусных средств. 4. Возможные действия злоумышленника для осуществления несанкционированного доступа.	6	2	2	
Общая трудоёмкость лекционного курса			24	10	6	x

Всего лекций по учебной дисциплине:	час	Из них в интерактивной форме:	час
- очная форма обучения	24	- очная форма обучения	4
- очно-заочная форма	10	-очно-заочная форма	2
- заочная форма обучения	6	- заочная форма обучения	2

Примечания:

- материально-техническое обеспечение лекционного курса – см. Приложение 6.
- обеспечение лекционного курса учебной, учебно-методической литературой и иными библиотечно-информационными ресурсами и средствами обеспечения образовательного процесса – см. Приложения 1 и 2

5 Лабораторный практикум.
Примерный тематический план лабораторных занятий по разделам дисциплины

№			Тема лабораторной работы	Трудоемкость ЛР, час.			Связь с ВАРС		Применяемые интерактивные формы
раздела	ЛЗ*	ЛР*		Очная форма	Очно-заочная форма	Заочная форма	Предусмотрена самоподготовка к занятию +/-	Защита отчёта о ЛР во внеаудиторное время +/-	
1	2	3	4	5	6	7	8	9	10
1	1	1	Оценка безопасности электронных платежных систем	2	2	1	+	-	Индивидуальная работа
1	2	-	Тестирование по разделу 1	2	0,5	0,25	+	-	Тестирование
2	3-6	2	Оценка безопасности социальных сетей	8	4	1	+		Индивидуальная работа
2	7-8	3	Криптографические способы защиты информации	4	2	1	+	-	Индивидуальная работа
2	9	-	Тестирование по разделу 2	2	0,5	0,25	+	-	Тестирование
3	10-16	4	Практикум по шифрованию: простые шифры	14	4,5	2	+	-	Разработка и анализ имитационных моделей
3	17-22	5	Практикум по шифрованию: сложные шифры	12	4	2	+	-	Разработка и анализ имитационных моделей
3	23	-	Тестирование по разделу 3	2	0,5	0,5	+	-	Тестирование
Итого ЛР			Общая трудоёмкость ЛР	46	18	8	x		

Примечания:
- материально-техническое обеспечение лабораторного практикума – см. Приложение 6
- обеспечение лабораторного практикума учебной, учебно-методической литературой и иными библиотечно-информационными ресурсами и средствами обеспечения образовательного процесса – см. Приложение 1 и 2

6. Общие методические рекомендации по изучению отдельных разделов дисциплины

При изучении конкретного раздела дисциплины, из числа вынесенных на лекционные и практические занятия, обучающемуся следует учитывать изложенные ниже рекомендации. Обратите на них особое внимание при подготовке к аттестации.

Работа по теме прежде всего предполагает ее изучение по учебнику или пособию. Следует обратить внимание на то, что в любой теории, есть либо неубедительные, либо чересчур абстрактные, либо сомнительные положения. Поэтому необходимо вырабатывать самостоятельные суждения, дополняя их аргументацией, что и следует демонстрировать на семинарах. Для выработки самостоятельного суждения важным является умение работать с научной литературой. Поэтому работа по теме кроме ее изучения по учебнику, пособию предполагает также поиск по теме научных статей в научных журналах. Такими журналами являются: Вопросы правоведения, Экономика и право др. Выбор статьи, относящейся к теме, лучше делать по последним в году номерам, где приводится перечень статей, опубликованных за год.

Самостоятельная подготовка предполагает использование ряда методов.

1. Конспектирование. Конспектирование позволяет выделить главное в изучаемом материале и выразить свое отношение к рассматриваемой автором проблеме.

Техника записей в конспекте индивидуальна, но есть ряд правил, которые могут принести пользу его составителю: начиная конспект, следует записать автора изучаемого произведения, его название, источник, где оно опубликовано, год издания. Порядок конспектирования:

а) внимательное чтение текста;

б) поиск в тексте ответов на поставленные в изучаемой теме вопросы;

в) краткое, но четкое и понятное изложение текста;

г) выделение в записи наиболее значимых мест;

д) запись на полях возникающих вопросов, понятий, категорий и своих мыслей.

2. Записи в форме тезисов, планов, аннотаций, формулировок определений. Все перечисленные формы помогают быстрой ориентации в подготовленном материале, подборе аргументов в пользу или против какого- либо утверждения.

3. Словарь понятий и категорий. Составление словаря помогает быстрее осваивать новые понятия и категории, увереннее ими оперировать. Подобный словарь следует вести четко, разборчиво, чтобы удобно было им пользоваться.

ВОПРОСЫ
для самоподготовки к лабораторным занятиям

Самостоятельное изучение тем рекомендуется проводить в следующем порядке:

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме.
2) На этой основе составить развёрнутый план изложения темы
3) Оформить отчётный материал в форме расчетно-аналитической работы
4) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
5) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы
6) Принять участие в указанном мероприятии

Рекомендации по конкретным темам дисциплины

Основные положения теории информационной безопасности.

1. Основные понятия в сфере информационной безопасности.
2. Угрозы информационной безопасности.
3. Основные методы обеспечения информационной безопасности

Криптография как способ защиты информации.

1. Основные понятия криптографии и криптоанализа.
2. История криптографии.
3. Методы шифрования.
4. Электронная цифровая подпись.
5. Стенография.

Правовое и организационное обеспечение информационной безопасности.

1. Конституция РФ об информационной безопасности.
2. Стратегические и доктринальные документы в области информационной безопасности.
3. Законодательство РФ об информационной безопасности.
4. Подзаконные акты по вопросам информационной безопасности.
5. Организационное обеспечение информационной безопасности.

Физические и аппаратные меры защиты информации.

1. Технические каналы утечки информации.
2. Системы видеонаблюдения.
3. Тепловидение.
4. Системы контроля доступа.
5. Электронные ключи.
6. Программно-аппаратные комплексы.

Разрушающие программные воздействия.

1.Виды программного обеспечения.
2. Вирусы и программы антивирусной защиты
3. Технологии применения антивирусных средств.
4. Возможные действия злоумышленника для осуществления несанкционированного доступа.

КРИТЕРИИ ОЦЕНКИ
самоподготовки по темам лабораторных занятий

- оценка «зачтено» выставляется обучающемуся, если все вопросы темы раскрыты, во время дискуссии высказывается собственная точка зрения на обсуждаемую проблему, демонстрируется способность аргументировать доказываемые положения и выводы.
- оценка «не зачтено» выставляется, если обучающийся не способен доказать и аргументировать собственную точку зрения по изученной теме, не способен ссылаться на мнения ведущих специалистов по обсуждаемой проблеме.

7. Общие методические рекомендации по оформлению и выполнению отдельных видов ВАРС

7.1. Перечень примерных тем презентаций для обучающихся очной и очно-заочной форм обучения

1. Информационная безопасность в социальных сетях;
2. Безопасность применения платежных систем – законодательство и практика.
3. Принципы работы с электронной почтой. Создание почтовых ящиков на общедоступных сайтах и на серверах учреждений. Адресная книга.
4. Угрозы паролям.
5. Сравнительная характеристика антивирусных программ.
6. Законодательство о персональных данных.
7. Безопасность применения пластиковых карт – законодательство и практика.
8. Идентификация по голосу. Скрытые возможности.
9. Бухгалтерская отчетность как источник рассекречивания информации.
10. Информационная безопасность: экономические аспекты.
11. Безопасность розничной торговли.
12. Биопаспорт.
13. Сравнительная характеристика симметричных и ассиметричных методов шифрования.
14. Особенности и проблемы применения биометрических средств защиты информации.
15. Ответственность за нарушения в сфере информационного права.

7.2. Рекомендации по оформлению презентации

Презентация начинается с титульного листа, содержащего ее название и, возможно, имена авторов. Эти элементы обычно выделяются более крупным шрифтом, чем основной текст работы. Также на первый слайд целесообразно поместить логотип ВУЗа, от лица которой делается презентация. В качестве фона первого листа можно использовать рисунок или фотографию, имеющую непосредственное отношение к теме работы, однако текст поверх такого изображения должен читаться очень легко. Подобное правило соблюдается и для фона остальных листов (см. ниже). Тем не менее, монотонный фон или фон в виде мягкого градиента будет смотреться на первом листе тоже вполне эффектно.

Для оформления работы следует использовать стандартные, широко распространенные пропорциональные шрифты, такие как Arial, Tahoma, Verdana, Times New Roman, Georgia и др.

Для работы изначально необходимо подобрать цветовую гамму: обычно это три—пять цветов, среди которых есть как теплые, так и холодные. Очевидно, любой из этих цветов должен отлично читаться на выбранном ранее фоне; малейшее подозрение на то, что цвет шрифта хотя бы немного сливается с фоном — и что-то одно из этого подлежит немедленной замене: не вынуждайте тех, для кого делается презентация, портить зрение.

Ни в коем случае не стоит стараться разместить на одном листе как можно больше текста. Для того, чтобы прочесть мелкий текст, многим необходимо существенно напрягать зрение, и, скорее всего, по своей воле никто это- го делать не будет. Поэтому, чем больше текста на одном листе вы предложите аудитории, тем с меньшей вероятностью она его прочитает.

Хорошо известно, что любая речь воспринимается намного лучше, если она произносится докладчиком, обратившим свой взор к слушателям, фактически, находящимся с аудиторией в прямом зрительном контакте. Если же докладчик начинает читать с листа, то эффективность передачи информации значительно снижается. И уж совсем нелепо выглядит человек, делающий презентацию, когда ему приходится читать текст непосредственно со слайда. В этом случае слушатели, как правило, перестают и слушать, и читать то, что изображено на экране. Докладчику, потерявшему в такой момент внимание аудитории, очень сложно вернуть его в дальнейшем. Старайтесь не использовать текст на слайде как часть вашей речи; лучше поместите туда важные тезисы и лишь один—два раза обернитесь к ним, посвятив остальное время непосредственной коммуникации с

вашими слушателями. Обязательно иллюстрируйте презентацию рисунками, фотографиями, наглядными схемами, графиками и диаграммами. Яркие картинки привлекают внимание куда эффективнее, чем сухой текст или, порой, даже очень неплохая речь. Изображению всегда следует придавать как можно больший размер; если это возможно, иллюстрации стоит распределить по нескольким слайдам, нежели размещать их на одном но в уменьшенном виде. Подписи вполне допустимо располагать не над и не под изображением, а сбоку, если оно, например, имеет вертикальную ориентацию. Нет ничего забавнее, чем маленькая картинка и подпись к ней, выполненная крупным шрифтом.

И, наконец, завершать работу следует кратким резюме, содержащим ее основные положения, важные данные.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

Оценка «зачтено» выставляется обучающемуся при соблюдении следующих условий:

- содержание задания полностью соответствует ее теме;
-высокая/достаточная/приемлемая полнота и глубина раскрытия темы презентации;
- степень самостоятельности обучающегося при подготовке презентации не вызывает сомнения;
- общие требования к оформлению презентации соблюдены полностью/ соблюдены на приемлемом уровне;
- уровень понимания обучающимся материала, отражённого в презентации, соответствует требуемому полностью/находится на приемлемом уровне.

Оценка «не зачтено» выставляется обучающемуся при соблюдении следующих условий:

- содержание презентации не соответствует ее теме;
- не приемлемая полнота и глубина раскрытия темы презентации;
- степень самостоятельности обучающимся при подготовке презентации вызывает сомнения;
- уровень понимания обучающимся материала, не соответствует минимально требуемому.

7.3. Перечень заданий для контрольных работ обучающихся заочной формы обучения

1. Настройка безопасности ОС Windows при работе в сети
2. Организация мер по защите
3. Разработка методики противодействия социальному инжинирингу
4. Организация антивирусной защиты частного предприятия с 25-ю рабочими станциями
5. Отправка сообщения в будущее
6. Криптографические системы защиты данных
7. Преступления в сфере компьютерной информации
8. Компьютерная преступность и компьютерная безопасность
9. Ответственность за нарушения в сфере информационного права
10. Комплекс технических решений по защите информации, записанной на отчуждаемых электронных носителях.
11. Проектирование системы информационной безопасности
12. Современные угрозы и каналы утечки информации в компьютерных сетях
13. Правовая охрана программ для ЭВМ и баз данных
14. Рекреационная география
15. Настройка параметров безопасности операционной системы Windows
16. Оптимизация ОС Windows Vista с целью обеспечения информационной безопасности
17. Администрирование ОС Windows
18. Безопасность файловых ресурсов сети Windows
19. Разработка программы приема и передачи сообщений в локальной сети Microsoft
20. Оценка и анализ структуры системы защиты информации
21. Методы защиты информации в телекоммуникационных сетях
22. Защита информации от несанкционированного доступа методом криптопреобразования
23. Преступления в сфере компьютерной информации : криминологический анализ
24. Общая характеристика преступлений в сфере компьютерной информации
25. Понятие и характеристика преступлений в сфере компьютерной информации
26. Расследование преступлений в сфере компьютерной информации
27. Практика привлечения к административной ответственности лиц, совершивших правонарушения в области избирательного права
28. Правовые основы обеспечения информационной безопасности Российской Федерации
29. Проблемы защиты информации
30. Информационное право и правовая защита информации
31. Правовое регулирование в сфере защиты информации
32. Проектирование системы информационной безопасности

33. Современные угрозы и каналы утечки информации в компьютерных сетях
34. Антивирусная защита ПО для серверов
35. Принципы работы с электронной почтой. Создание почтовых ящиков на общедоступных сайтах и на серверах учреждений. Адресная книга. Настройка Outlook Express
36. Организация и функционирование электронной почты
37. Защита электронной почты в Internet
38. Электронная почта как сервис глобальной сети. Протоколы передачи почты
39. Защита информации в Интернет
40. Системы обнаружения атак. (Анализаторы сетевых протоколов и сетевые мониторы)
41. Спам и нормы пользования сетью
42. Российский рынок информационной безопасности
43. Информация и личная безопасность
44. Компьютерная преступность в России.
45. Пользователи и злоумышленники сети Internet.
46. Защита от сбоев в электропитании. Источники бесперебойного питания: назначение, характеристики, принципы работы.
47. Защита от формирования электромагнитных полей (излучений). Средства защиты кабельной системы.
48. Средства защиты от сбоев в работе устройств хранения информации.
49. Биометрические средства и технологии установления подлинности.
50. Особенности и проблемы применения биометрических средств защиты информации.
51. Угрозы паролям.
52. Модели разграничения прав доступа.
53. Использование цифровой подписи и хэш-функций.
54. Понятие цифровых сертификатов.
55. Стандарт шифрования AES.
56. Стандарт шифрования RIJNDAEL.
57. Сравнительная характеристика симметричных и ассиметричных методов шифрования.
58. Структура современных компьютерных вирусов.
59. Подробное описание основных классов вирусов.
60. Троянские вирусы.
61. Вирусы - черви.
62. Полиморфные и стелс - вирусы.
63. Политика безопасности антивирусных программ.
64. Сравнительная характеристика антивирусных программ.
65. Политика безопасности брандмауэра.
66. Фильтрация пакетов: достоинства и недостатки.
67. Прокси - серверы.
68. Особенности защиты баз данных.
69. Стандарты защищенности.
70. Методы борьбы с фишинговыми атаками.
71. Законодательство о персональных данных.
72. Защита авторских прав.
73. Назначение, функции и типы систем видеозащиты.
74. Как подписывать с помощью ЭЦП электронные документы различных форматов.
75. Обзор угроз и технологий защиты Wi-Fi-сетей.
76. Проблемы внедрения дискового шифрования.
77. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
78. Особенности процессов аутентификации в корпоративной среде.
79. Квантовая криптография.
80. Утечки информации: как избежать. Безопасность смартфонов.
81. Безопасность применения пластиковых карт - законодательство и практика.
82. Защита CD- и DVD-дисковот копирования.
83. Современные угрозы и защита электронной почты.
84. Программные средства анализа локальных сетей на предмет уязвимостей.
85. Безопасность применения платежных систем - законодательство и практика.
86. Аудит программного кода по требованиям безопасности.
87. Антишпионское ПО (antispyware).
88. Обеспечение безопасности Web-сервисов.
89. Защита от внутренних угроз.
90. Технологии RFID.
91. Уничтожение информации на магнитных носителях.
92. Ботнеты - плацдарм современных кибератак.
93. Цифровые водяные знаки в изображениях.
94. Электронный документооборот. Модели нарушителя.
95. Идентификация по голосу. Скрытые возможности.

96. Безопасность океанских портов.
97. Безопасность связи.
98. Безопасность розничной торговли.
99. Банковская безопасность.
100. Информатизация управления транспортной безопасностью.
101. Биопаспорт.
102. Обзор современных платформ архивации данных.
103. Что такое консалтинг в области ИБ.
104. Бухгалтерская отчетность как источник рассекречивания информации.
105. Управление рисками: обзор употребительных подходов.
106. Категорирование информации и информационных систем.
107. Обеспечение базового уровня информационной безопасности.
108. Распределенные атаки на распределенные системы.
109. Оценка безопасности автоматизированных систем.
110. Функциональная безопасность программных средств.
111. Технологические процессы и стандарты обеспечения функциональной безопасности в
112. жизненном цикле программных средств.
113. Информационная безопасность: экономические аспекты.

7.4. Рекомендации по оформлению контрольной работы

Начинать знакомство с избранной темой лучше всего с чтения обобщающих работ по данной проблеме, постепенно переходя к узкоспециальной литературе.

На основе анализа прочитанного и просмотренного материала по данной теме следует составить тезисы по основным смысловым блокам, с пометками, собственными суждениями и оценками. Предварительно подобранный в литературных источниках материал может превышать необходимый объем контрольной работы, но его можно использовать для составления плана контрольной работы.

Составление плана. Автор по предварительному согласованию с преподавателем может самостоятельно составить план контрольной работы, с учетом замысла работы, либо взять за основу рекомендуемый план, приведенный в данных методических указаниях по соответствующей теме. Правильно построенный план помогает систематизировать материал и обеспечить последовательность его изложения.

Наиболее традиционной является следующая структура контрольной работы:

Титульный лист.
Оглавление (план, содержание).
Введение.
Глава 1 (полное наименование главы).
1.1. (полное название параграфа, пункта);
1.2. (полное название параграфа, пункта).
Глава 2 (полное наименование главы).
2.1. (полное название параграфа, пункта);
2.2. (полное название параграфа, пункта).
Заключение (или выводы).
Список использованной литературы.
Приложения (по усмотрению автора).

} Основная часть

Титульный лист заполняется по единой форме (Приложение 1).

Оглавление (план, содержание) включает названия всех разделов (пунктов плана) контрольной работы и номера страниц, указывающие начало этих разделов в тексте контрольной работы.

Введение. В этой части контрольной работы обосновывается актуальность выбранной темы, формулируются цели работы и основные вопросы, которые предполагается раскрыть в контрольной работы, указываются используемые материалы и дается их краткая характеристика с точки зрения полноты освещения избранной темы. Объем введения не должен превышать 1-1,5 страницы.

Основная часть контрольной работы может быть представлена одной или несколькими главами, которые могут включать 2-3 параграфа (подпункта, раздела).

Здесь достаточно полно и логично излагаются главные положения в используемых источниках, раскрываются все пункты плана с сохранением связи между ними и последовательности перехода от одного к другому.

Автор должен следить за тем, чтобы изложение материала точно соответствовало цели и названию главы (параграфа). Материал в контрольной работе рекомендуется излагать своими словами, не допуская дословного переписывания из литературных источников. В тексте обязательны ссылки на первоисточники, т.е. на тех авторов, у которых взят данный материал в виде мысли, идеи, вывода, числовых данных, таблиц, графиков, иллюстраций и пр.

Работа должна быть написана грамотным литературным языком. Сокращение слов в тексте не допускается, кроме общеизвестных сокращений и аббревиатуры. Каждый раздел рекомендуется заканчивать кратким выводом.

Заключение (выводы). В этой части обобщается изложенный в основной части материал, формулируются общие выводы, указывается, что нового лично для себя вынес автор контрольной работы из работы над ним. Выводы делаются с учетом опубликованных в литературе различных точек зрения по проблеме рассматриваемой в контрольной работе, сопоставления их и личного мнения автора контрольной работы. Заключение по объему не должно превышать 1,5-2 страниц.

Приложения могут включать графики, таблицы, расчеты. Они должны иметь внутреннюю (собственную) нумерацию страниц.

Библиография (список литературы) здесь указывается реально использованная для написания контрольной работы литература, периодические издания и электронные источники информации. Список составляется согласно правилам библиографического описания.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

Оценка «зачтено» выставляется обучающемуся при соблюдении следующих условий:

- содержание задания полностью соответствует ее теме;
- высокая/достаточная/приемлемая полнота и глубина раскрытия темы контрольной работы;
- степень самостоятельности обучающегося при подготовке контрольной работы не вызывает сомнения;
- общие требования к оформлению контрольной работы соблюдены полностью/ соблюдены на приемлемом уровне;
- уровень понимания обучающимся материала, отражённого в контрольной работе, соответствует требуемому полностью/находится на приемлемом уровне.

Оценка «не зачтено» выставляется обучающемуся при соблюдении следующих условий:

- содержание контрольной работы не соответствует ее теме;
- не приемлемая полнота и глубина раскрытия темы контрольной работы;
- степень самостоятельности обучающимся при подготовке контрольной работы вызывает сомнения;
- уровень понимания обучающимся материала, не соответствует минимально требуемому.

7.5. Рекомендации по самостоятельному изучению тем

ВОПРОСЫ
для самостоятельного изучения темы

Номер раздела дисциплины	Тема в составе раздела/ вопрос в составе темы раздела, вынесенные на самостоятельное изучение	Расчетная трудоемкость, час.	Форма текущего контроля по теме
1	2	3	4
Очная/ очно-заочная форма обучения			
3	Эффективные меры антивирусной защиты	-/20	презентация
3	Новейшие аппаратные средства защиты информации	-/20	презентация
Заочная форма обучения			
3	Эффективные меры антивирусной защиты	28	опрос
3	Новейшие аппаратные средства защиты информации	26	опрос
3	Новейшие программные средства защиты информации	26	опрос
Примечание: Учебная, учебно-методическая литература и иные библиотечно-информационные ресурсы и средства обеспечения самостоятельного изучения тем – см. Приложения 1, 2, 3, 4.			

Общий алгоритм самостоятельного изучения темы

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме (ориентируясь на вопросы для самоконтроля).
2) На этой основе составить развёрнутый план изложения темы
3) Выбрать форму отчетности – презентация (для обучающихся очно-заочной формы обучения)
2) Оформить отчётный материал в установленной форме в соответствии методическими рекомендациями
3) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
4) Предоставить отчётный материал преподавателю по согласованию с ведущим преподавателем
5) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы
6) Принять участие в указанном мероприятии, пройти рубежное тестирование по разделу на аудиторном занятии и заключительное тестирование в установленное для внеаудиторной работы

время

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ ПРЕЗЕНТАЦИИ

Оценка «зачтено» выставляется обучающемуся при соблюдении следующих условий:
- содержание задания полностью соответствует ее теме;
-высокая/достаточная/приемлемая полнота и глубина раскрытия темы презентации;
- степень самостоятельности обучающегося при подготовке презентации не вызывает сомнения;
- общие требования к оформлению презентации соблюдены полностью/ соблюдены на приемлемом уровне;
- уровень понимания обучающимся материала, отражённого в презентации, соответствует требуемому полностью/находится на приемлемом уровне.

Оценка «не зачтено» выставляется обучающемуся при соблюдении следующих условий:
- содержание презентации не соответствует ее теме;
- не приемлемая полнота и глубина раскрытия темы презентации;
- степень самостоятельности обучающимся при подготовке презентации вызывает сомнения;
- уровень понимания обучающимся материала, не соответствует минимально требуемому.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ ОПРОСА
для заочной формы обучения

- оценка «зачтено» по самостоятельно изученной теме выставляется обучающемуся, если он, принимал активное участие в обсуждении темы на лабораторной занятии, а именно: выступил на лабораторном занятии по одному или нескольким вопросам темы, дал обоснованные ответы на вопросы, задавал вопросы по теме другим обучающимися.

- оценка «не зачтено» по самостоятельно изученной теме выставляется обучающемуся, если он, не принимал активное участие в обсуждении темы на лабораторном занятии, а именно: не выступил на лабораторном занятии по одному или нескольким вопросам темы, не дал обоснованные ответы на вопросы, не задавал вопросы по теме другим обучающимися.

.

8. Текущий (внутрисеместровый) контроль хода и результатов учебной работы студента

8.1. Текущий контроль успеваемости

В течение семестра, проводится текущий контроль успеваемости по дисциплине, к которому студент должен быть подготовлен.

Отсутствие пропусков аудиторных занятий, активная работа на лабораторных занятиях, общее выполнение графика учебной работы, подготовка и проведение тестирования, подготовка презентации (контрольной работы для заочной формы) являются основанием для получения положительной оценки по текущему контролю.

9. Промежуточная (семестровая) аттестация по курсу

1) действующее «Положение о текущем контроле успеваемости, промежуточной аттестации обучающихся по программам высшего образования (бакалавриат, специалитет, магистратура) и среднего профессионального образования в ФГБОУ ВО Омский ГАУ»	
Основные характеристики промежуточной аттестации студентов по итогам изучения дисциплины	
Цель промежуточной аттестации -	установление уровня достижения каждым студентом целей и задач обучения по данной дисциплине, изложенным в п.2.2 настоящей программы
Форма промежуточной аттестации -	зачёт с оценкой
Место процедуры получения зачёта в графике учебного процесса	1) участие студента в процедуре получения зачёта осуществляется за счёт учебного времени (трудоёмкости), отведённого на изучение дисциплины
	2) процедура проводится в рамках ВАРС, на последней неделе семестра
Основные условия получения студентом зачёта:	1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по

	дисциплине; 2) прошёл итоговое тестирование; 3) подготовил презентацию (контрольную работу по заочной форме).
Процедура получения зачёта -	
Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:	Представлены в Фонде оценочных средств по данной учебной дисциплине (см. – Приложение 9)

9.1 Рубежное тестирование по итогам изучения разделов дисциплины

По итогам изучения раздела дисциплины, обучающиеся проходят рубежное тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

Тестирование осуществляется по разделам дисциплины.

Процедура тестирования не ограничена во времени и предполагает максимальное сосредоточение студента на выполнении теста, содержащего несколько тестовых заданий.

Тестирование проводится в электронной форме в системе ЭИОС. В каждый вариант теста включаются вопросы закрытые (одиночный выбор).

Бланк теста

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Омский государственный аграрный университет имени П.А. Столыпина»

Тестирование по итогам освоения раздела дисциплины
«Информационная безопасность»
Для обучающихся направления подготовки 38.03.01 - Экономика

ФИО_____группа_____
Дата_____

Уважаемые студенты!

Прежде чем приступить к выполнению заданий внимательно ознакомьтесь с инструкцией:

1. Отвечая на вопрос с выбором правильного ответа, правильный, на ваш взгляд, ответ (ответы) обведите в кружок.
2. За каждый верный ответ Вы получаете 1 балл, за неверный – 0 баллов. Максимальное количество полученных баллов 30.

Желаем удачи!

ТЕСТОВЫЕ ВОПРОСЫ
для проведения контроля

РАЗДЕЛ 1. Основы теории информационной безопасности

1. Кто является основным ответственным за определение уровня классификации информации?
A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство

6. Что такое процедура?
A. Правила использования программного и аппаратного обеспечения в компании
B. Пошаговая инструкция по выполнению задачи
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
A. Поддержка высшего руководства
B. Эффективные защитные меры и методы их внедрения
C. Актуальные и адекватные политики и процедуры безопасности
D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?
A. Пошаговые инструкции по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Широкие, высокоуровневые заявления руководства
D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
A. Анализ рисков
B. Анализ затрат / выгоды
C. Результаты ALE
D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?
A. Количественно оценить уровень безопасности среды
B. Оценить возможные потери для каждой контрмеры
C. Количественно оценить затраты / выгоды
D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:
A. Среднесрочное планирование
B. Долгосрочное планирование
C. Ежедневное планирование
D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?
A. Нечто, приводящее к ущербу от угрозы
B. Любая потенциальная опасность для информации или систем
C. Любой недостаток или отсутствие информационной безопасности
D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:
A. Технических и нетехнических методов
B. Контрмер и защитных механизмов
C. Физической безопасности и технических средств защиты
D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
A. Внедрение управления механизмами безопасности
B. Классификацию данных после внедрения механизмов безопасности
C. Уровень доверия, обеспечиваемый механизмом безопасности
D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
A. Только военные имеют настоящую безопасность
B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?
A. Угрозы x Риски x Ценность актива
B. (Угрозы x Ценность актива x Уязвимости) x Риски
C. SLE x Частоту = ALE
D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?
A. Делегирование полномочий
B. Количественная оценка воздействия потенциальных угроз
C. Выявление рисков
D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
A. Поддержка
B. Выполнение анализа рисков
C. Определение цели и границ
D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
A. Чтобы убедиться, что проводится справедливая оценка
B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков?
A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
D. Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим?
A. Он достижим и используется
B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
C. Это связано с точностью количественных элементов
D. Количественные измерения должны применяться к качественным элементам

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
A. Много информации нужно собрать и ввести в программу
B. Руководство должно одобрить создание группы
C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
D. Множество людей должно одобрить данные

РАЗДЕЛ 2. Ведение в криптографию. Правовое и организационное обеспечение информационной безопасности.

1. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?
A. Стандарты
B. Должный процесс (Due process)
C. Должная забота (Due care)
D. Снижение обязательств

2. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
D. Открытый стандарт, определяющий цели контроля

3. Из каких четырех доменов состоит CobiT?
A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

4. Что представляет собой стандарт ISO/IEC 27799?
A. Стандарт по защите персональных данных о здоровье
B. Новая версия BS 17799
C. Определения для новой серии ISO 27000
D. Новая версия NIST 800-60

5. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
C. COSO учитывает корпоративную культуру и разработку политик
D. COSO – это система отказоустойчивости

6. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
A. NIST и OCTAVE являются корпоративными
B. NIST и OCTAVE ориентирован на ИТ
C. AS/NZS ориентирован на ИТ
D. NIST и AS/NZS являются корпоративными

7. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
A. Анализ связующего дерева
B. AS/NZS

C. NIST
D. Анализ сбоев и дефектов

8. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

A. Безопасная OECD
B. ISO\IEC
C. OECD
D. CPTED

9. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

10. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

11. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

12. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

13. Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

14. Естественные угрозы безопасности информации вызваны:

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.

15. Икусственные угрозы безопасности информации вызваны:
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.

16. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

РАЗДЕЛ 3. Меры защиты информации

1. К посторонним лицам нарушителям информационной безопасности относится:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.
7. лица, нарушившие пропускной режим;

2. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

3. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

4. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

5. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

6. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

7. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

8. Активный перехват информации это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

9. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

11. Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

КРИТЕРИИ ОЦЕНКИ
ответов на тестовые вопросы рубежного контроля

- *оценка «отлично»* выставляется обучающемуся, если получено более 81% правильных ответов.
- *оценка «хорошо»* - получено от 71 до 80% правильных ответов.
- *оценка «удовлетворительно»* - получено от 61 до 70% правильных ответов.
- *оценка «неудовлетворительно»* - получено менее 61% правильных ответов.

9.2 Итоговое тестирование по итогам изучения дисциплины

По итогам изучения дисциплины, обучающиеся проходят итоговое тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

9.2.1 Подготовка к итоговому тестированию по итогам изучения дисциплины

Тестирование осуществляется по всем темам и разделам дисциплины, включая темы, выносимые на самостоятельное изучение.

Процедура тестирования не ограничена во времени и предполагает максимальное сосредоточение студента на выполнении теста, содержащего несколько тестовых заданий.

Тестирование проводится в электронной форме в системе ЭИОС. В каждый вариант теста включаются вопросы закрытые (одиночный выбор).

На тестирование выносится по 10 вопросов из каждого раздела дисциплины.

Бланк теста

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Омский государственный аграрный университет имени П.А. Столыпина»

Тестирование по итогам освоения дисциплины
«Информационная безопасность»
Для обучающихся направления подготовки 38.03.01 - Экономика

ФИО_____**группа**_____
Дата_____

Уважаемые студенты!

Прежде чем приступить к выполнению заданий внимательно ознакомьтесь с инструкцией:

1. Отвечая на вопрос с выбором правильного ответа, правильный, на ваш взгляд, ответ (ответы) обведите в кружок.
2. За каждый верный ответ Вы получаете 1 балл, за неверный – 0 баллов. Максимальное количество полученных баллов 30.

Желаем удачи!

ВОПРОСЫ
для проведения итогового тестирования

Как называется умышленно искаженная информация?
Дезинформация
Информативный поток
Достоверная информация
Перестает быть информацией
Как называется информация, к которой ограничен доступ?
Конфиденциальная
Противозаконная
Открытая
Недоступная
Какими путями может быть получена информация?
Проведением, покупкой и противоправным добыванием информации научных исследований
Захватом и взломом ПК информации научных исследований
Добыванием информации из внешних источников и скремблированием информации научных исследовании
Захватом и взломом защитной системы для информации научных исследований
Основной документ, на основе которого проводится политика информационной безопасности?
программа информационной безопасности
регламент информационной безопасности

политическая информационная безопасность
Протекторат

К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

Информационным процессам
Мыслительным процессам
Машинным процессам
Микропроцессам

Под непреднамеренным воздействием на защищаемую информацию понимают?

Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
Процесс ее преобразования, при котором содержание информации изменяется на ложную
Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Основные предметные направления Защиты Информации?

охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
Охрана золотого фонда страны
Определение ценности информации
Усовершенствование скорости передачи информации

Государственная тайна это

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Коммерческая тайна это….

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Банковская тайна это….

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Профессиональная тайна

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

К основным объектам банковской тайны относятся следующие:

Все ответы верны
Тайна банковского счета
Тайна операций по банковскому счету
Тайна банковского вклада

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

управление доступом
конфиденциальность
аутентичность
целостность
доступность

К открытым источникам информация относятся.
Газеты, Радио, Новости
Информация украденная у спецслужб
Из вскрытого сейфа
Украденная из правительственной организации
По сведениям Media и Pricewaterhouse Coopers, на чью долю приходится 60% всех инцидентов IT-безопасности?
Хакерские атаки
Различные незаконные проникновения
Инсайдеры
Технические компании
Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?
Индивидуальный подход к защите
Комплексный подход к защите
Смешанный подход к защите
Рациональный подход к защите
Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
Информационная безопасность
Защитные технологии
Заземление
Конфиденциальность
Можно выделить следующие направления мер информационной безопасности
Правовые
Организационные
Все ответы верны
Технические
Что можно отнести к правовым мерам ИБ?
Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
Охрану вычислительного центра, установку сигнализации и многое другое
Что можно отнести к организационным мерам ИБ?
Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.
Что можно отнести к техническим мерам ИБ?
Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в

случае нарушения работоспособности отдельных звеньев и многое другое
Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Потенциальные угрозы, против которых направлены технические меры защиты информации

Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения
Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
Потери информации из-за не достаточной установки сигнализации в помещении.
Процессы преобразования, при котором информация удаляется

Шифрование информации это

Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
Процесс преобразования, при котором информация удаляется
Процесс ее преобразования, при котором содержание информации изменяется на ложную
Процесс преобразования информации в машинный код

Какие сбои оборудования, при которых теряется информация, бывают?

случайное уничтожение или изменение данных
перебои электропитания
некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных;
несанкционированное копирование, уничтожение или подделка информации

Какие потери информации бывают из-за некорректной работы программ?

потери при заражении системы компьютерными вирусами
сбои дисковых систем
перебои электропитания
сбои работы серверов, рабочих станций, сетевых карт и тд

Какие потери информации, связанные с несанкционированным доступом, бывают?

несанкционированное копирование, уничтожение или подделка информации
потери при заражении системы компьютерными вирусами
случайное уничтожение или изменение данных
сбои дисковых систем

Потери из-за ошибки персонала и пользователей бывают?

несанкционированное копирование, уничтожение или подделка информации
потери при заражении системы компьютерными вирусами
случайное уничтожение или изменение данных
сбои дисковых систем

О**т сбоев устройств для хранения информации?**

установка источников бесперебойного питания (UPS)
симметричное мультипроцессирование
Каждую минуту сохранять данные
Организация надежной и эффективной системы резервного копирования и дублирования данных

Средства защиты данных, функционирующие в составе программного обеспечения.

Программные средства защиты информации
Технические средства защиты информации
Источники бесперебойного питания (UPS)
Смешанные средства защиты информации

Программные средства защиты информации.

средства архивации данных, антивирусные программы
Технические средства защиты информации
Источники бесперебойного питания (UPS)
Смешанные средства защиты информации

Программное средство защиты информации.

криптография
источник бесперебойного питания
резервное копирование
дублирование данных

Обеспечение достоверности и полноты информации и методов ее обработки.

Конфиденциальность
Целостность
Доступность
Целесообразность

Обеспечение доступа к информации только авторизованным пользователям?

Конфиденциальность
Целостность
Доступность
Целесообразность

Виды защиты БД

защита паролем, защита пользователем,
учётная запись группы администратора
приложение, которое используется для управления базой данных
группа Users

Наибольшую угрозу для безопасности сети представляют.

несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение;
вскрытие стандартной учётной записи пользователя
вскрытие стандартной учётной группы администратора
копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании

Защита через права доступа заключается.

присвоении каждому пользователю определенного набора прав
запереть серверы в специальном помещении с ограниченным доступом
присвоить пароль каждому общедоступному ресурсу
в наличии преобразователья микрофона

Дифференцированное резервное копирование это

Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании;
Копирование всех выбранных файлов без отметки о резервном копировании
Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования;
Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

Полное копирование данных это

Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
Копирование всех выбранных файлов без отметки о резервном копировании
Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

Наиболее распространенный криптографический код

Код Хэмминга
код Рида-Соломона
код Морзе
итеративный код

Наиболее простой и недорогой метод предотвратить катастрофическую потерю данных

Резервное копирование на магнитную ленту
Шифрование данных
Бездисковые компьютеры
Все ответы верны

Право Execute дает вам возможность

Запуск (выполнение) программ из каталога
Создание новых файлов в каталоге
Запрещение на доступ к каталогу, файлу, ресурсу
Чтение и копирование файлов из совместно используемого каталога

Право No Access дает вам возможность

Удаление файлов в каталоге
Запрещение на доступ к каталогу, файлу, ресурсу
Запуск (выполнение) программ из каталога
Создание новых файлов в каталоге

Право Read дает вам возможность

Удаление файлов в каталоге
Запуск (выполнение) программ из каталога
Запрещение на доступ к каталогу, файлу, ресурсу
Чтение и копирование файлов из совместно используемого каталога

Право Write дает вам возможност

Удаление файлов в каталоге
Запрещение на доступ к каталогу, файлу, ресурсу
Создание новых файлов в каталоге
Чтение и копирование файлов из совместно используемого каталога

Методы сохранение данных при чрезвычайных ситуаций
резервное копирование на магнитную ленту;
источники бесперебойного питания (UPS);
отказоустойчивые системы
Все ответы верны
Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках).
Журнал резервного копирования
Отказоустойчивые системы
Метод резервного копирования
Шифрование данных
Пароль доступа к ресурсам
Доступ только для чтения
такой пароль не существует
Отказоустойчивые системы
Метод резервного копирования
Шифрование данных
Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?
установка источников бесперебойного питания (UPS)
Такого средства не существует
Каждую минуту сохранять данные
Перекидывать информацию на носитель, который не зависит от энергии
Ежедневное копирование данных это
Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
Копирование всех выбранных файлов без отметки о резервном копировании
Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании
Способ защиты от сбоев процессора?
установка источников бесперебойного питания (UPS)
симметричное мультипроцессирование
Каждую минуту сохранять данные
Перекидывать информацию на носитель, который не зависит от энергии
Способ защиты от сбоев устройств для хранения информации?
установка источников бесперебойного питания (UPS)
симметричное мультипроцессирование
Каждую минуту сохранять данные
Организация надежной и эффективной системы резервного копирования и дублирования данных
Средства защиты данных, функционирующие в составе программного обеспечения.
Программные средства защиты информации
Технические средства защиты информации
Источники бесперебойного питания (UPS)
Смешанные средства защиты информации
Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?
источник бесперебойного питания (UPS)
источник питания
электро-переключатель
все перечисленное
Что такое Информационная безопасность?
меры по защите информации от неавторизованного доступа
меры по защите ПК
безопасность личной информации
все перечисленное
Целью информационной безопасности является?
все перечисленное
обезопасить ценности системы
защитить и гарантировать точность и целостность информации
минимизировать разрушения
Укажите направления мер информационной безопасности.
правовые, организационные, технические
правовые, аппаратные, программные
личные, организационные

технические
Технические меры защиты можно разделить на:
средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и тд;
правовые, организационные, технические
правовые, аппаратные, программные
личные, организационные
Программные средства защиты можно разделить на:
криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и тд
административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и тд
правовые, организационные, технические
правовые, аппаратные, программные
К наиболее важному элементу аппаратной защиты можно отнести?
защита от сбоев серверов, рабочих станций и локальных компьютеров
защиту от вирусов
защиту от хакеров
все перечисленное
Как связаны ключи шифрования между собой?
математической функцией
связкой
шифром
специальным паролем
В чем заключается уникальность гибких дисков?
в форматировании
в быстродействии
их защищенность
в простоте обработки данных
Что такое пароль?
механизм управления доступом
средство защиты
безопасность личной информации
Безопасность людей
Меры по защите информации от неавторизованного доступа называется
Информационной безопасностью
Безопасностью ПК
Личной безопасностью
Безопасностью группы администратора
Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к?
техническим мерам защиты
не правовым мерам защиты
организационным мерам защиты
программным средствам защиты
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
аппаратным средствам защиты
программным средствам защиты
техническим средствам защиты
правовым средствам защиты
Как еще называют радиомикрофон с дистанционным (кодовым) включением через любой телефон?
«электронное ухо»
«электронный микрофон»
«громкоговоритель»
«электронный приемник»
К программным средствам защиты можно отнести?
средства идентификации и аутентификации пользователей
средства защиты авторских прав программистов
неиспользованные дорожки на дискете
дорожки дискеты
К правовым мерам следует отнести?
разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов
охрану вычислительного центра и аппаратуры связи
проектирование ЛВС и ГБС

средства идентификации и аутентификации пользователей
Сбои дисковых систем относится к?
техническим и организационным мерам защиты
правовым мерам защиты
мерам защиты от НДС и кражи
к средствам идентификации и аутентификации
Потеря или изменение данных при ошибках ПО относится к
техническим и правовым мерам защиты
организационным мерам защиты
правовым мерам защиты
мерам защиты от НДС и кражи
к средствам идентификации и аутентификации
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
Аппаратным и техническим средствам защиты
Программным средствам защиты
Средствам защиты идентификации и аутентификации
Организационным и общим средствам защиты
Криптографические средства относится к?
Программным средствам
Аппаратным средствам
Организационным средствам защиты
Захвату данных
Служат обеспечению сохранения целостности программного обеспечения в составе вычислительной системы
пароль
корпус вычислительной системы
шифры
сигналы
В каких случаях криптография неэффективна?
когда элементы текста известны в зашифрованном и исходном виде
когда элементы текста известны в открытом и активном виде
если есть пароль и логин
когда элементы текста представлены в открытом и не полном виде
В каком случае надежнее шифр?
короткий зашифрованный текст
длинный зашифрованный текст
зашифрованный текст среднего размера
зашифрованный текст не влияет на надежность шифра
В каких случаях возможно вычисление одного ключа с помощью другого
Использованием только ЭВМ
Ни в каких случаях невозможна
Использованием математической функцией
Использованием только ЛВС
Назначение пароля в ИС?
механизм управления доступом, средство защиты и безопасность личной информации
скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ
технические меры защиты и средство защиты данных
участки магнитной ленты скрытые шифром
механизм управления средствами защиты и безопасность доступа к ОЗУ в ПЗУ
Меры по защите информации от неавторизованного доступа называется
Информационной безопасностью
Безопасностью ПК
Личной безопасностью
Средства защиты
Меры скрытия копирования
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
аппаратным средствам защиты
программным средствам защиты
техническим средствам защиты
правовым средствам защиты
Какие атакующие средства включены в современные способы несанкционированного доступа?
активные и пассивные
положительные и отрицательные
большие и маленькие
объединенные и разъединенные

односторонние и разносторонние
Что относится к пассивным средствам защиты информации?
Фильтры
Детекторы поля
Сканирующие приемники
Комплекс радио контроля
Нелинейные локаторы
Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак.
лаборатория Касперского
Российский центр по защите от вредоносных программ
компания McAfee Security
лаборатория доктора Веб
компания Тумар
Метод резервного копирования когда, копирование всех выбранных файлов производится без отметки о резервном копировании
Полное копирование
Копирование
Ежедневное копирование
Дифференцированное резервное копирование
Резервное копирование с приращением
Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
Полное копирование
Копирование
Ежедневное копирование
Дифференцированное резервное копирование
Резервное копирование с приращением

Дифференцированный зачет выставляется студенту по факту выполнения графика учебных работ, предусмотренных рабочей программой дисциплины. По итогам изучения дисциплины, студенты проходят итоговое тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

Тестирование осуществляется по всем темам и разделам дисциплины, включая темы, выносимые на самостоятельное изучение.

Процедура тестирования ограничена во времени и предполагает максимальное сосредоточение студента на выполнении теста, содержащего несколько тестовых заданий.

Студенту рекомендуется:

1. при неуверенности в ответе на конкретное тестовое задание пропустить его и переходить к следующему, не затрачивая много времени на обдумывание тестовых заданий при первом проходе по списку теста;
2. при распределении общего времени тестирования учитывать (в случае компьютерного тестирования), что в автоматизированной системе могут возникать небольшие задержки при переключении тестовых заданий.

Необходимо помнить, что:

1. тест является индивидуальным. Общее время тестирования и количество тестовых заданий ограничены и определяются преподавателем в начале тестирования;
2. по истечении времени, отведённого на прохождение теста, сеанс тестирования завершается;
3. допускается во время тестирования только однократное тестирование;
4. вопросы студентов к преподавателю по содержанию тестовых заданий и не относящиеся к процедуре тестирования не допускаются;

Тестируемому во время тестирования запрещается:

1. нарушать дисциплину;
2. пользоваться учебно-методической и другой вспомогательной литературой, электронными средствами (мобильными телефонами, электронными записными книжками и пр.);
3. использование вспомогательных средств и средств связи на тестировании допускается при разрешении преподавателя-предметника.
4. копировать тестовые задания на съёмный носитель информации или передавать их по электронной почте;
5. фотографировать задания с экрана с помощью цифровой фотокамеры;
6. выносить из класса записи, сделанные во время тестирования.

На рабочее место тестируемому разрешается взять ручку, черновик, калькулятор.

За несоблюдение вышеперечисленных требований преподаватель имеет право удалить тестируемого, при этом результат тестирования удаленного лица аннулируется.

Тестируемый имеет право:

Вносить замечания о процедуре проведения тестирования и качестве тестовых заданий.

Перенести сроки тестирования (по уважительной причине) по согласованию с преподавателем.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

10. Информационное и методическое обеспечение учебного процесса по дисциплине

В соответствии с действующими государственными требованиями для реализации учебного процесса по дисциплине обеспечивающей кафедрой разрабатывается и постоянно совершенствуется учебно-методический комплекс (УМКД), соответствующий данной рабочей программе и прилагаемый к ней. При разработке УМКД кафедра руководствуется установленными университетом требованиями к его структуре, содержанию и оформлению. В состав УМКД входят перечисленные ниже и другие источники учебной и учебно-методической информации, средства наглядности.

Электронная версия актуального УМКД, адаптированная для обучающихся, выставляется в информационно-образовательной среде университета.

ПЕРЕЧЕНЬ
литературы, рекомендуемой
для изучения дисциплины

Автор, наименование, выходные данные	Доступ
Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	http://znanium.com
Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	http://znanium.com
Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820 . - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1784437 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	http://znanium.com
Дубинин, Е. А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - Москва : ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; + 11 с.. - (Научная мысль). ISBN 978-5-369-01371-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/471787 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	http://znanium.com
Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	http://znanium.com
Информационные технологии и вычислительные системы: журнал - М. : Российская академия наук. -	НСХБ
Экономическая безопасность : учебное пособие / под ред. Н.В. Манохиной. — Москва : ИНФРА-М, 2020. — 320 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1831. - ISBN 978-5-16-009002-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1092382 (дата обращения: 16.07.2021). – Режим доступа: по подписке.	http://znanium.com