МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Регламентация работы персонала организации при обеспечении экономической и информационной безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **2, 3**
Семестр: **4, 5**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	5 семестр	Всего	Единицы
1	Лекции	4	2	6	часов
2	Практические занятия	2	4	6	часов
3	Всего аудиторных занятий	6	6	12	часов
4	Из них в интерактивной форме	2	2	4	часов
5	Самостоятельная работа	30	62	92	часов
6	Всего (без экзамена)	36	68	104	часов
7	Подготовка и сдача зачета	0	4	4	часов
8	Общая трудоемкость	36	72	108	часов
				3.0	З.Е.

Контрольные работы: 5 семестр - 1
Зачет: 5 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Доцент кафедры БИС	_____	А. О. Исхакова
Доцент кафедры БИС	_____	А. Ю. Исхаков

Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ	_____	И. В. Осипов
Заведующий выпускающей каф. КИБЭВС	_____	А. А. Шелупанов

Эксперты:

Доцент кафедры КИБЭВС	_____	А. А. Конев
Доцент кафедры БИС	_____	О. О. Евсютин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

заложить терминологический фундамент

научить правильно проводить анализ угроз информационной безопасности

выполнять основные этапы решения задач информационной безопасности

приобрести навыки анализа угроз информационной безопасности

рассмотреть основные общеметодологические принципы теории информационной безопасности

изучение методов и средств обеспечения информационной безопасности

изучение методов нарушения конфиденциальности, целостности и доступности информации.

1.2. Задачи дисциплины

- ознакомление студентов с терминологией информационной безопасности
- развитие мышления студентов
- изучение методов и средств обеспечения информационной безопасности
- обучение определению причин, видов, каналов утечки и искажения информации

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» (Б1.В.ОД.6) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности, Информатика.

Последующими дисциплинами являются: Основы информационной безопасности, Безопасность вычислительных сетей, Безопасность операционных систем, Безопасность систем баз данных, Безопасность электронного документооборота, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Подготовка к сдаче и сдача государственного экзамена.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

В результате изучения дисциплины обучающийся должен:

– **знать** сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

– **уметь** классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта

– **владеть** профессиональной терминологией в области информационной безопасности; навыками изучения и обобщения нормативных и методических материалов; актуальными знаниями по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		4 семестр	5 семестр

Аудиторные занятия (всего)	12	6	6
Лекции	6	4	2
Практические занятия	6	2	4
Из них в интерактивной форме	4	2	2
Самостоятельная работа (всего)	92	30	62
Выполнение индивидуальных заданий	44	14	30
Проработка лекционного материала	25	9	16
Написание рефератов	5	5	0
Подготовка к практическим занятиям, семинарам	18	2	16
Всего (без экзамена)	104	36	68
Подготовка и сдача зачета	4	0	4
Общая трудоемкость, ч	108	36	72
Зачетные Единицы	3.0		

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр					
1 Понятие информационной безопасности, ее роль в национальной безопасности. Терминологические основы информационной безопасности	1	0	8	9	ПК-20
2 Угрозы. Классификация и анализ угроз информационной безопасности	1	1	12	14	ПК-20
3 Модель угроз, модель нарушителя	2	1	10	13	ПК-20
Итого за семестр	4	2	30	36	
5 семестр					
4 Модели оценки угроз конфиденциальности, целостности, доступности	1	2	31	34	ПК-20
5 Функции и задачи защиты информации	1	2	31	34	ПК-20
Итого за семестр	2	4	62	68	
Итого	6	6	92	104	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1 Понятие информационной безопасности, ее роль в национальной безопасности. Терминологические основы информационной безопасности	Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи. Национальные интересы Российской Федерации в информационной сфере. Приоритетные направления в области защиты информации в Российской Федерации. Тенденции развития информационной политики государств и ведомств. Информационная война, проблемы. Правовое обеспечение защиты информации. Информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные.	1	ПК-20
	Итого	1	
2 Угрозы. Классификация и анализ угроз информационной безопасности	Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.	1	ПК-20
	Итого	1	
3 Модель угроз, модель нарушителя	Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные не-преднамеренные.Потенциально возможные злоумышленные действия в автоматизированных системах обработки	2	ПК-20

	данных.Формирование модели нарушителя.		
	Итого	2	
Итого за семестр		4	
5 семестр			
4 Модели оценки угроз конфиденциальности, целостности, доступности	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальных требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.	1	ПК-20
	Итого	1	
5 Функции и задачи защиты информации	Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека	1	ПК-20

	Итого	1	
Итого за семестр		2	
Итого		6	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин				
	1	2	3	4	5
Предшествующие дисциплины					
1 Основы информационной безопасности	+	+	+	+	+
2 Информатика	+	+	+	+	+
Последующие дисциплины					
1 Основы информационной безопасности	+	+	+	+	+
2 Безопасность вычислительных сетей	+	+	+	+	+
3 Безопасность операционных систем	+	+		+	+
4 Безопасность систем баз данных	+	+	+	+	+
5 Безопасность электронного документооборота	+	+			+
6 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+
7 Подготовка к сдаче и сдача государственного экзамена	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ПК-20	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Опрос на занятиях, Тест, Реферат, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий приведены в таблице 6.1.

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные лекции, ч	Всего, ч
4 семестр		
Презентации с использованием слайдов с обсуждением	2	2
Итого за семестр:	2	2
5 семестр		
Презентации с использованием слайдов с обсуждением	2	2
Итого за семестр:	2	2
Итого	4	4

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
2 Угрозы. Классификация и анализ угроз информационной безопасности	Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации	1	ПК-20
	Итого	1	
3 Модель угроз, модель нарушителя	Построение модели угроз, модели нарушителя для информационной системы	1	ПК-20
	Итого	1	
Итого за семестр		2	
5 семестр			
4 Модели оценки угроз конфиденциальности, целостности, доступности	Построение модели угроз для выбранного объекта информатизации	2	ПК-20
	Итого	2	
5 Функции и задачи защиты информации	Оценка безопасности информации на объектах ее обработки	2	ПК-20
	Итого	2	
Итого за семестр		4	
Итого		6	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
4 семестр				
1 Понятие информационной безопасности, ее роль в национальной безопасности. Терминологические основы информационной безопасности	Написание рефератов	5	ПК-20	Домашнее задание, Опрос на занятиях, Реферат, Тест
	Проработка лекционного материала	3		
	Итого	8		
2 Угрозы. Классификация и анализ угроз информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ПК-20	Домашнее задание, Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	3		
	Выполнение индивидуальных заданий	7		
	Итого	12		
3 Модель угроз, модель нарушителя	Проработка лекционного материала	3	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	7		
	Итого	10		
Итого за семестр		30		
5 семестр				
4 Модели оценки угроз конфиденциальности, целостности, доступности	Подготовка к практическим занятиям, семинарам	8	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по практическому занятию, Тест
	Проработка лекционного материала	8		
	Выполнение индивидуальных заданий	15		
	Итого	31		
5 Функции и задачи защиты информации	Подготовка к практическим занятиям, семинарам	8	ПК-20	Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка	8		

	лекционного материала			
	Выполнение индивидуальных заданий	15		
	Итого	31		
Итого за семестр		62		
	Подготовка и сдача зачета	4		Зачет
Итого		96		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк [и др.] ; под ред. Горбатова В.С.. — Электрон. дан. — Москва : Горячая линия-Телеком, 2018. — 288 с. — Режим доступа: https://e.lanbook.com/book/111075 (дата обращения: 19.05.2018).

2. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Вы-пуск 2 [Электронный ресурс] [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Загл. с экрана — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5179 (дата обращения: 19.05.2018).

12.2. Дополнительная литература

1. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информаци-онной безопасности [Электронный ресурс] [Электронный ресурс]: учебное пособие. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5163 (дата обращения: 19.05.2018).

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114 (дата обращения: 19.05.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Основы информационной безопасности [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf (дата обращения: 19.05.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. http://www.iqlib.ru - электронная интернет библиотека;
2. http://www.biblioclub.ru – полнотекстовая электронная библиотека;
3. http://www.elibrary.ru - научная электронная библиотека;
4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
5. http://www.sec.ru – каталог организаций в сфере информационной безопасности
6. https://fstec.ru/ - сайт Федеральной службы по техническому и экспортному контролю
7. http://www.consultant.ru/ - КонсультантПлюс — компьютерная справочная правовая система в России

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория организации финансовых расследований
учебная аудитория для проведения занятий практического типа
634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 400 ауд.
Описание имеющегося оборудования:
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.
Программное обеспечение не требуется.

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:
- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную

информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какая из нижеперечисленных задач, изложенных в Доктрине информационной безопасности Российской Федерации, не относится к задачам государственных органов в рамках деятельности по обеспечению информационной безопасности:

a) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

b) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

c) планирование и разработка мер по проведению киберразведовательных операций;

d) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

2. В стандарте США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США" в зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на…

a) 5 классов;

b) 4 группы;

c) 3 множества;

d) 2 подгруппы.

3. Что из нижеперечисленного не относится к перечню сведений конфиденциального характера, утвержденного Президентом Российской Федерации?

a) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

b) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

c) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

d) Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

4. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США» называют …

a) «Желтой книгой»;

b) «Оранжевым документом»;

c) «Оранжевой книгой»;

d) «Красным списком».

5. Модель угроз безопасности информации не включает в себя:

a) Описание информационной системы и ее структурно-функциональных характеристик;

b) Описание угроз безопасности информации;

c) Описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы;

d) Стадии (этапы работ) создания системы защиты информационной системы.

6. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

a) Проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

b) Установка средств мониторинга сетевой инфраструктуры;

c) Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;

d) Внедрение документов, регламентирующих организационные меры по защите информации;

7. Методический документ ФСТЭК России «Методика определения безопасности информации в информационных системах» применяется совместно с:

a) Базой данных уязвимостей, разработанной Федеральной службой безопасности Российской Федерации

b) Банком данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru);

c) Общедоступной базой данных компьютерных угроз;

d) Перечнем сведений конфиденциального характера.

8. Анализ уязвимостей информационной системы проводится в целях:

a) Оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации;

b) Оценки эффективности использования политик разграничения доступа;
c) Оптимизации производительности программно-аппаратных средств защиты информации;
d) Сегментации информационной системы.

9. Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определёнными критериями и показателями безопасности называется:
a) Аттестация;
b) Аудит;
c) Сертификация;
d) Пентест.

10. Что из нижеперечисленного не относится к международным методикам проведения тестирования на проникновение, ориентированных на моделирование атак, направленных на сетевую инфраструктуру организации:
a) Trusted Computer System Evaluation Criteria;
b) PCI DSS;
c) NIST SP800-115;
d) Open Source Security Testing Methodology Manual.

11. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа называется:
a) Характеристика нарушителя;
b) Модель нарушителя;
c) Сценарий нарушителя;
d) Модель источников угроз.

12. Какое из нижеперечисленных направлений не относится к аттестации объектов информатизации по требованиям безопасности информации:
a) Аттестация автоматизированных систем, средств связи, обработки и передачи информации;
b) Аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
c) Аттестация рабочих мест с целью оценки условий труда;
d) Аттестация технических средств, установленных в выделенных помещениях и защищаемых помещениях.

13. Стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта
a) Тестировение черного ящика;
b) Тестирование белого ящика;
c) Тестирование красного ящика;
d) Тестирование неизвестного ящика.

14. Методика тестирования на проникновение называется:
a) Аудит;
b) Пентест;
c) Honeypot;
d) Metasploit.

15. Что из нижеперечисленного не относится к этапу анализа рисков информационной безопасности:
a) Построение модели нарушителя;
b) Идентификация ресурсов;

c) Идентификация бизнес-требований и требований законодательства, применимых к идентифицированным ресурсам;

d) Оценивание идентифицированных ресурсов с учетом выявленных бизнес требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности.

16. Какая угроза безопасности информации является преднамеренной ?

a) Ошибки персонала;

b) Сбой программного обеспечения;

c) Фальсификация, подделка документов;

d) Открытие электронного письма, содержащего вирус.

17. Территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных называется …

a) Неконтролируемой зоной

b) Зоной помещений автоматизированной системы

c) Зоной баз данных защищаемой системы

d) Зоной контролируемой территории.

18. Угроза диверсии относится к …

a) Субъективной преднамеренной причине нарушения целостности информации;

b) Субъективной непреднамеренной причине нарушения целостности информации;

c) Объективной непреднамеренной причине нарушения целостности информации;

d) Объективной преднамеренной причине нарушения целостности информации.

19. Перехват данных является угрозой:

a) Доступности;

b) Конфиденциальности;

c) Целостности;

d) Достоверности.

20. Продолжите тезис верно: Класс задач «Легендирование» по защите информации…

a) Не существует;

b) Потерял актуальность в связи с переходом на новые стандарты симметричных криптосистем;

c) Предполагает включение в состав элементов системы обработки информации дополнительных компонентов;

d) Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта.

21. Риск информационной безопасности это

a) Число уязвимостей в системе;

b) Отношение стоимости системы защиты к вероятности её «простоя»;

c) Сочетание вероятности угрозы информационной безопасности и последствий её наступления;

d) Оценка стоимости защитных средств.

22. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации называется …

a) Угрозой безопасности;

b) Компьютерной безопасностью;

c) Анализом угроз;

d) Атакой на информационную систему.

23. Что из перечисленного происходит при использовании RAID-массивов?
a) Производится полное шифрование данных
b) Обеспечивается более высокий уровень защиты от вирусов
c) Повышается надёжность хранения данных
d) Увеличивается максимальная пропускная способность сети

24. Заключительным этапом построения системы защиты является …
a) Анализ уязвимых мест;
b) Планирование;
c) Обследование;
d) Сопровождение.

25. Что из перечисленного не используется в биометрической аутентификации?
a) Рисунок папиллярного узора;
b) Клавиатурный почерк;
c) Пластиковая карта с магнитной полосой;
d) Радужная оболочка глаза.

26. К какой подсистеме не предъявляются требования в Руководящем документе «Классификация автоматизированных систем и требований по защите информации»?
a) управления доступом;
b) регистрации и учета;
c) технической защиты информации;
d) обеспечения целостности.

27. Защита информации это:
a) Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё;
b) Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
c) Процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
d) Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

28. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
a) Отсутствием управления доступом.
b) Произвольным управлением доступом;
c) Принудительным управлением доступом;
d) Верифицируемой безопасностью.

29. Свойство доступности достигается за счет применения мер, направленных на повышение:
a) Аутентичности;
b) Непротиворечивости;
c) Отказоустойчивости;
d) Неотказуемости.

30. Каким термином называется защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?

a) Конфиденциальная информация;
b) Секретная информация;
c) Военная тайна;
d) Государственная тайна.

31. Получение доступа к информации субъектом в нарушение действующей политики разграничения доступа называется…
a) Несанкционированный доступ;
b) Злоумышленный доступ
c) Неразрешенный доступ;
d) Запретный доступ.

32. Какой вид информации не относится к категории конфиденциальной информации?
a) Коммерческая тайна;
b) Тайна судопроизводства;
c) Персональные данные;
d) Государственная тайна.

33. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?
a) Конфиденциальная информация;
b) Персональные данные;
c) Информация про личность;
d) Информация с ограниченным доступом.

34. Каналы несанкционированного получения информации сгруппированы в…
a) 3 класса;
b) 4 класса;
c) 7 классов;
d) 9 классов.

35. Набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, называется …
a) Моделью безопасности;
b) Методом шифрования;
c) Компьютерной безопасностью;
d) Политикой безопасности.

36. Общая, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов – это …
a) Миссия;
b) Стратегия;
c) Функция;
d) Процесс.

37. Что из перечисленного не является целью проведения аудита безопасности?
a) Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы;
b) Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы;
c) Оценка будущего уровня защищенности системы;

d) Оценка соответствия системы существующим стандартам в области информационной безопасности.

38. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:
a) Сравнением исследуемого объекта с ранее известными образцами-эталонами;
b) Способностью обнаруживать ранее неизвестные атаки;
c) Простотой в настройке и эксплуатации для конечного пользователя системы;
d) Популярностью использования в системах антивирусной защиты.

39. Задачи по резервированию системы защиты делятся на:
a) Теплое и холодное резервирование;
b) Холодное и горячее резервирование;
c) Белое и серое резервирование;
d) Толстое и тонкое резервирование.

40. Модель системы с полным перекрытием характеризуется следующим положением:
a) В автоматизированной системе средствами защиты «перекрыто» большинство каналов утечки;
b) В механизме защиты должно содержаться по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации;
c) В системе защиты присутствует только одно средство для перекрытия всех угроз безопасности;
d) Автоматизированная система является системой множественного доступа.

41. Инструментальная комплексность в сфере информационной безопасности подразумевает:
a) Непрерывность осуществления мероприятий по защите информации;
b) Защиту информации от внешних и внутренних угроз;
c) Интеграцию всех видов и направлений ИБ для достижения поставленных целей;
d) Обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

42. Какой документ устанавливает цель, задачи и структуру стандартов по защите информации, объединяющий аспекты стандартизации в данной области и являющийся основополагающим стандартом в области защиты информации:
a) ГОСТ Р 52069.0-2013
b) ФЗ №152 от 27.07.2006
c) Постановление Правительства РФ №119 от 01.11.2012
d) Конституция РФ

43. Деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России) называется
a) Аттестация средств защиты информации
b) Сертификация средств защиты информации
c) Комплексное тестирование средств защиты информации
d) Выборка средств защиты информации

44. Положения Федерального закона №149 от 27.06.2006 не распространяются на:
a) Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации;
b) Отношения, возникающие при применении информационных технологий;
c) Отношения, возникающие при обеспечении защиты информации

d) Отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации

14.1.2. Темы индивидуальных заданий

Одиночно стоящий компьютер в бухгалтерии.

Сервер в бухгалтерии

Почтовый сервер

Веб-сервер

Компьютерная сеть материальной группы

Одноранговая локальная сеть без выхода в Интернет

Одноранговая локальная сеть с выходом в Интернет

Сеть с выделенным сервером без выхода в Интернет

Сеть с выделенным сервером с выхода в Интернет

Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях

Телефонная сеть

Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры)

Банковские операции (внесение денег на счет и снятие)

Операции с банковскими пластиковыми карточками

Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия

Компьютер, хранящий конфиденциальную информацию о разработках предприятия

Материалы для служебного пользования на твердых носителях в производстве

Материалы для служебного пользования на твердых носителях на закрытом предприятии

Материалы для служебного пользования на твердых носителях в архиве

Материалы для служебного пользования на твердых носителях в налоговой инспекции

Комната для переговоров по сделкам на охраняемой территории

Комната для переговоров по сделкам на неохраняемой территории

Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.)

Судебные материалы (твердая копия)

Паспортный стол РОВД

Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.)

Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.)

Сведения по тоталитарным сектам и другим общественно-вредным организациям

Сведения по общественно-полезным организациям (красный крест и др.)

Партийные списки и руководящие документы

14.1.3. Зачёт

Теория защиты информации. Основные направления

Обеспечение информационной безопасности и направления защиты

Комплексность (целевая, инструментальная, структурная, функциональная, временная)

Требования к системе защиты информации

Угрозы информации

Виды угроз. Основные нарушения

Характер происхождения угроз

Источники угроз. Предпосылки появления угроз

Система защиты информации

Классы каналов несанкционированного получения информации

Причины нарушения целостности информации

Методы и модели оценки уязвимости информации

Общая модель воздействия на информацию

Общая модель процесса нарушения физической целостности информации

Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных

Методологические подходы к оценке уязвимости информации

Модель защиты системы с полным перекрытием

Рекомендации по использованию моделей оценки уязвимости информации

Допущения в моделях оценки уязвимости информации

Методы определения требований к защите информации

Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации

Классификация требований к средствам защиты информации

Требования к защите, определяемые структурой автоматизированной системы обработки данных

Требования к защите, обуславливаемые видом защищаемой информации

Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации

Анализ существующих методик определения требований к защите информации

Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения

Руководящий документ Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации",выпущенном в 1992 году. Часть 1

Классы защищенности средств вычислительной техники от несанкционированного доступа

Функции защиты информации

Стратегии защиты информации

Способы и средства защиты информации

Способы "абсолютной системы защиты"

Архитектура систем защиты информации. Требования

Общеметодологических принципов архитектуры системы защиты информации

Построение средств защиты информации

Ядро системы защиты

Семирубежная модель защиты

Средства защиты информации. Антивирусы, средства анализа защищенности, средства обнаружения вторжений

Регуляторы в области защиты информации

14.1.4. Темы домашних заданий

Определение каналов несанкционированного доступа для личного компьютера (ноутбука)
Построение модели нарушителя для ИСПДн

14.1.5. Темы рефератов

Структура органов государственной власти, регламентирующая деятельность по защите информации в РФ
Современные способы идентификации и аутентификации в информационных системах
Анализ руководящих документов по оценке защищенности автоматизированных систем

14.1.6. Темы опросов на занятиях

Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.

Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.

Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные не-преднамеренные.

Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.

Формирование модели нарушителя.

Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальных требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.

Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего

персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека

14.1.7. Темы контрольных работ

Модели оценки угроз конфиденциальности, целостности, доступности

14.1.8. Вопросы для подготовки к практическим занятиям, семинарам

Оценка безопасности информации на объектах ее обработки

Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации

Построение модели угроз для выбранного объекта информатизации

Построение модели угроз, модели нарушителя для информационной системы

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.