МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента науки и инноваций

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

Методы и системы защиты информации, информационная безопасность

Уровень образования: **высшее образование - подготовка кадров высшей квалификации**
Направление подготовки / специальность: **10.06.01 Информационная безопасность**
Направленность (профиль) / специализация: **Методы и системы защиты информации, информационная безопасность**
Форма обучения: **заочная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **2, 3**
Семестр: **4, 5**
Учебный план набора 2017 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	5 семестр	Всего	Единицы
1	Лекции	6	0	6	часов
2	Практические занятия	2	4	6	часов
3	Всего аудиторных занятий	8	4	12	часов
4	Самостоятельная работа	60	32	92	часов
5	Всего (без экзамена)	68	36	104	часов
6	Подготовка и сдача экзамена / зачета	4	36	40	часов
7	Общая трудоемкость	72	72	144	часов
				4.0	З.Е.

Дифференцированный зачет: 4 семестр
Экзамен: 5 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «26» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.06.01 Информационная безопасность, утвержденного 30.07.2014 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент, к.т.н. каф. КИБЭВС _____ Д. Д. Зыков

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Заведующий аспирантурой _____ Т. Ю. Коротина

Доцент лаборатории безопасных биомедицинских технологий ЦТБ КИБЭВС _____ А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Организация работы по подготовке к сдаче кандидатского экзамена по специальной дисциплине по специальности 10.06.01 – Методы и системы защиты информации, информационная безопасность с Номенклатурой специальностей научных работников, утвержденной приказом Минобрнауки России № 59 от 25.02.2009 г. 4. Целью изучения дисциплины аспирантами является приобретение знаний в области методов и систем защиты информации, информационной безопасности.

1.2. Задачи дисциплины

– сформировать способность формулировать научные задачи в области обеспечения информационной безопасности;

– сформировать навыки применения программно-аппаратных и технических средств защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности;

– сформировать углубленное представление о принципах и методах теоретических и экспериментальных исследований для решения задач в области информационной безопасности.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Методы и системы защиты информации, информационная безопасность» (Б1.В.ОД.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Методы и системы защиты информации, информационная безопасность, Методы и системы защиты информации, информационная безопасность, Информационная безопасность.

Последующими дисциплинами являются: Методы и системы защиты информации, информационная безопасность, Методы и системы защиты информации, информационная безопасность, Подготовка к сдаче и сдача государственного экзамена.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-1 способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;

– ПК-3 способность применять программно-аппаратные и технические средства защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности, исследовать, создавать новые и совершенствовать существующие методы защиты информации;

– ПК-4 способность использовать основные законы естественнонаучных дисциплин, применять методы математического анализа и моделирования, теоретического и экспериментального исследования для решения задач в области информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** основные методы управления информационной безопасностью; методы аттестации уровня защищенности автоматизированных систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах.

– **уметь** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию систе-

мы управления информационной безопасностью автоматизированных систем.

– **владеть** навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 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	8	4
Лекции	6	6	0
Практические занятия	6	2	4
Самостоятельная работа (всего)	92	60	32
Проработка лекционного материала	48	36	12
Подготовка к практическим занятиям, семинарам	44	24	20
Всего (без экзамена)	104	68	36
Подготовка и сдача экзамена / зачета	40	4	36
Общая трудоемкость, ч	144	72	72
Зачетные Единицы	4.0		

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 Теория и методология обеспечения информационной безопасности и защиты информации	1	0	10	11	ОПК-1
2 Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации	1	1	20	22	ОПК-1, ПК-4
3 Анализ рисков нарушения информационной безопасности	2	0	10	12	ПК-3, ПК-4
4 Мероприятия и механизмы формирования политики обеспечения информационной безопасности	2	1	20	23	ОПК-1

Итого за семестр	6	2	60	68	
5 семестр					
5 Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет	0	2	8	10	ПК-3, ПК-4
6 Модели и методы оценки защищенности информации и информационной безопасности объекта	0	0	8	8	ПК-3, ПК-4
7 Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.	0	1	8	9	ПК-3, ПК-4
8 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов.	0	1	4	5	ПК-3, ПК-4
9 Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.	0	0	4	4	ПК-3, ПК-4
Итого за семестр	0	4	32	36	
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 Теория и методология обеспечения информационной безопасности и защиты информации	Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.	1	ОПК-1
	Итого	1	
2 Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения	1	ОПК-1, ПК-4

	информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.		
	Итого	1	
3 Анализ рисков нарушения информационной безопасности	Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем. Модели и методы оценки защищенности информации и информационной безопасности объекта. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.	2	ПК-3, ПК-4
	Итого	2	
4 Мероприятия и механизмы формирования политики обеспечения информационной безопасности	Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности. Модели и методы управления информационной безопасностью.	2	ОПК-1
	Итого	2	
Итого за семестр		6	
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	6	7	8	9
Предшествующие дисциплины									
1 Методы и системы защиты информации, информационная безопасность	+	+	+	+	+	+	+	+	+
2 Методы и системы защиты информации, информационная безопасность	+	+	+	+	+	+	+	+	+

3 Информационная безопасность	+	+	+	+	+	+	+	+	+
Последующие дисциплины									
1 Методы и системы защиты информации, информационная безопасность	+	+	+	+	+	+	+	+	+
2 Методы и системы защиты информации, информационная безопасность	+	+	+	+	+	+	+	+	+
3 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.	
ОПК-1	+	+	+	Опрос на занятиях, Тест, Дифференцированный зачет
ПК-3	+	+	+	Экзамен, Тест
ПК-4	+	+	+	Экзамен, Тест, Дифференцированный зачет

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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 Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.	1	ОПК-1, ПК-4
	Итого	1	
4 Мероприятия и механизмы	Принципы и решения (технические, математические, организационные и др.) по со-	1	ОПК-1

формирования политики обеспечения информационной безопасности	зданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности. Модели и методы управления информационной безопасностью.		
	Итого	1	
Итого за семестр		2	
5 семестр			
5 Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет	Анализ угроз нарушения информационной безопасности в компьютерных сетях, включая Интернет. Построение систем защиты информации в компьютерных сетях.	2	ПК-3, ПК-4
	Итого	2	
7 Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.	Основные критерии защищенности. Анализ рисков.	1	ПК-3, ПК-4
	Итого	1	
8 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов.	Идентификация. Аутентификация. Разграничение доступа.	1	ПК-3, ПК-4
	Итого	1	
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 Теория и методология	Проработка лекционного материала	10	ОПК-1	Тест

обеспечения информационной безопасности и защиты информации	Итого	10		
2 Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации	Подготовка к практическим занятиям, семинарам	12	ОПК-1, ПК-4	Дифференцированный зачет, Тест
	Проработка лекционного материала	8		
	Итого	20		
3 Анализ рисков нарушения информационной безопасности	Проработка лекционного материала	10	ПК-3, ПК-4	Тест
	Итого	10		
4 Мероприятия и механизмы формирования политики обеспечения информационной безопасности	Подготовка к практическим занятиям, семинарам	12	ОПК-1	Опрос на занятиях, Тест
	Проработка лекционного материала	8		
	Итого	20		
Итого за семестр		60		
	Подготовка и сдача зачета	4		Дифференцированный зачет
5 семестр				
5 Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет	Подготовка к практическим занятиям, семинарам	8	ПК-3, ПК-4	Тест, Экзамен
	Итого	8		
6 Модели и методы оценки защищенности информации и информационной безопасности объекта	Проработка лекционного материала	8	ПК-3, ПК-4	Тест, Экзамен
	Итого	8		
7 Модели и методы	Подготовка к практиче-	8	ПК-3, ПК-4	Тест, Экзамен

оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.	ским занятиям, семинарам			
	Итого	8		
8 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов.	Подготовка к практическим занятиям, семинарам	4	ПК-3, ПК-4	Тест, Экзамен
	Итого	4		
9 Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.	Проработка лекционного материала	4	ПК-3, ПК-4	Тест, Экзамен
	Итого	4		
Итого за семестр		32		
	Подготовка и сдача экзамена	36		Экзамен
Итого		132		

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. Основы защиты информации [Электронный ресурс] [Электронный ресурс]: учебное пособие. Изд. 5-е, перераб. и доп. – Томск: В-Спектр, 2011. – 244 с. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf. - (дата обращения: 22.08.2018). — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf (дата обращения: 28.11.2018).

2. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: https://e.lanbook.com/book/5154. - (дата обращения: 06.08.2018). — Режим доступа: https://e.lanbook.com/book/5154 (дата обращения: 28.11.2018).

12.2. Дополнительная литература

1. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122. (дата обращения: 06.08.2018). — Режим доступа: https://e.lanbook.com/book/1122 (дата обращения: 28.11.2018).

2. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: https://e.lanbook.com/book/5178. (дата обращения: 06.08.2018). — Режим доступа: https://e.lanbook.com/book/5178 (дата обращения: 28.11.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: https://e.lanbook.com/book/5154. - (дата обращения: 06.08.2018). (Методические указания к практическим заданиям и самостоятельной работе. – С.380 – 514). — Режим доступа: https://e.lanbook.com/book/5154 (дата обращения: 28.11.2018).

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. Крупнейший российский информационный портал в области науки, технологии, медицины и образования www.elibrary.ru. Интернет библиотека с доступом к реферативным и полнотекстовым статьям и материалам конференций www.ieeexplore.ieee.org.

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 программно-аппаратных средств обеспечения информационной безопасности, операционных систем и систем баз данных

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже M/B ASUSTeK S-775 P5B i965 / Core 2 Duo E6300 / DDR-II DIMM 2048 Mb / Sapphire PCI-E Radeon 256 Mb / 160 Gb Seagate (15 шт.);
- 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 ниже перечисленных 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-розыскного, 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) Тестирование 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. Экзаменационные вопросы

1. Теория защиты информации. Основные направления.

2. Обеспечение информационной безопасности. Основные задачи обеспечения информационной безопасности.

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

4. Требования к системе защиты информации.

5. Угрозы информации.

6. Виды угроз. Основные нарушения.

7. Характер происхождения угроз.

8. Источники угроз. Предпосылки появления угроз.

9. Система защиты информации. Принципы построения систем защиты информации. Интеграция систем защиты.

10. Классы каналов несанкционированного получения информации.

11. Причины нарушения целостности информации.

12. Методы и модели оценки уязвимости информации.

13. Общая модель воздействия на информацию.

14. Общая модель процесса нарушения физической целостности информации.

15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.

16. Методологические подходы к оценке уязвимости информации.

17. Модель защиты системы с полным перекрытием.

18. Рекомендации по использованию моделей оценки уязвимости информации.

19. Допущения в моделях оценки уязвимости информации.

20. Методы определения требований к защите информации.

21. Защита локальных сетей и операционных систем.

22. Требования к содержанию нормативно-методических документов по защите информации.

23. Основные понятия традиционных симметричных криптосистем. Шифры перестановки.

24. схема шифрования Полига—Хеллмана.

25. Схема шифрования эль-Гамаля, комбинированный метод шифрования.

26. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.

27. Методы идентификации и проверки подлинности пользователей компьютерных систем.

28. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации.

29. Средства защиты, управляемые модемом. Надежность средств защиты.

30. Компьютерные преступления и особенности их расследования.

14.1.3. Темы опросов на занятиях

Понятие информации и смежных ним: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы — определения, сопоставление. Идентификация, аутентификация, авторизация.

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 непреднамеренные.

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.

Обсуждение результатов курса дисциплины. Итоговое тестирование. Подведение итогов.

14.1.4. Вопросы дифференцированного зачета

Модели нарушителя.

Модели угроз конфиденциальности, целостности, доступности.

Методы анализа рисков нарушения информационной безопасности.

Мероприятия и механизмы формирования политики обеспечения информационной безопасности.

Средства защиты информации, циркулирующей в системах документооборота.

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.