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
_____ В. М. Рулевский
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **1**
Семестр: **2**
Учебный план набора 2017 года

Распределение рабочего времени

№	Виды учебной деятельности	2 семестр	Всего	Единицы
1	Практические занятия	40	40	часов
2	Всего аудиторных занятий	40	40	часов
3	Самостоятельная работа	32	32	часов
4	Всего (без экзамена)	72	72	часов
5	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Зачет: 2 семестр

Томск 2018

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 31.05.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Согласована на портале № 46509

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) 10.06.01 Информационная безопасность, утвержденного 30.07.2014 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. БИС _____ О. О. Евсютин

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 кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Согласована на портале № 46509

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Формирование у аспирантов методологических основ обеспечения информационной безопасности.

1.2. Задачи дисциплины

– формирование терминологического фундамента информационной безопасности;

– изучение методов нарушения конфиденциальности, целостности и доступности информации;

– освоение методов противодействия угрозам информационной безопасности;

– развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» (Б1.Б.3) относится к блоку 1 (базовая часть).

Последующими дисциплинами являются: Интеллектуальные методы в информационной безопасности, Математическое моделирование в информационной безопасности, Методы и системы защиты информации, информационная безопасность, Методы и средства защиты информации, Стандарты в области информационной безопасности.

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;

– ОПК-2 способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;

– ОПК-3 способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

– ОПК-4 способность организовать работу коллектива по проведению научных исследований в области информационной безопасности;

– ОПК-5 готовность к преподавательской деятельности по основным образовательным программам высшего образования;

В результате изучения дисциплины обучающийся должен:

– **знать** сущность и понятие информационной безопасности и характеристику ее составляющих; основной круг проблем (задач), встречающихся в области информационной безопасности, и основные способы (методы, алгоритмы) их решения; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные методы и средства обеспечения информационной безопасности, принципы построения систем защиты информации; методы анализа эффективности методов защиты информации.

– **уметь** классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта защиты; находить (выбирать) наиболее эффективные методы решения основных типов проблем (задач), встречающихся в области информационной безопасности; при решении исследовательских и практических задач в области информационной безопасности генерировать новые идеи, поддающиеся операционализации, исходя из наличных ресурсов и ограничений; организовывать и проводить экспериментальные исследования и компьютерное моделирование объектов защиты информации с применением современных средств и методов; анализировать результаты теоретических и экспериментальных исследований, вырабатывать рекомендации по совершенствованию средств и систем защиты информации.

– **владеть** профессиональной терминологией в области информационной безопасности; методологическими основами информационной безопасности как отрасли современной науки; на-

Согласована на портале № 46509

выками использования современных информационных технологий в области информационной безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыками изучения и обобщения нормативных и методических материалов.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Аудиторные занятия (всего)	40	40
Практические занятия	40	40
Самостоятельная работа (всего)	32	32
Выполнение индивидуальных заданий	14	14
Подготовка к практическим занятиям, семинарам	18	18
Всего (без экзамена)	72	72
Общая трудоемкость, ч	72	72
Зачетные Единицы	2.0	2.0

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	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр				
1 Понятие информационной безопасности, ее роль в национальной безопасности.	2	2	4	ОПК-5
2 Терминологические основы информационной безопасности.	2	2	4	ОПК-5
3 Угрозы. Классификация и анализ угроз информационной безопасности.	8	4	12	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
4 Модель угроз, модель нарушителя.	8	4	12	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
5 Модели оценки угроз конфиденциальности, целостности, доступности.	4	4	8	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
6 Функции и задачи защиты информации	4	4	8	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
7 Правовые основы информационной безопас-	4	4	8	ОПК-1, ОПК-2,

Согласована на портале № 46509

ности.				ОПК-3, ОПК-4, ОПК-5
8 Организационные основы информационной безопасности.	4	4	8	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
9 Методология и культура теоретических и экспериментальных исследований и организация работы исследовательского коллектива в области информационной безопасности	2	2	4	ОПК-4
10 Организация преподавательской деятельности по основным образовательным программам высшего образования в области информационной безопасности	2	2	4	ОПК-5
Итого за семестр	40	32	72	
Итого	40	32	72	

5.2. 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 5.2.

Таблица 5.2 – 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	10
Последующие дисциплины										
1 Интеллектуальные методы в информационной безопасности	+	+	+							
2 Математическое моделирование в информационной безопасности	+	+	+	+	+	+				
3 Методы и системы защиты информации, информационная безопасность	+	+	+	+	+	+	+	+		
4 Методы и средства защиты информации	+	+	+	+	+	+	+	+		
5 Стандарты в области информационной безопасности	+	+					+	+		

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.3.

Таблица 5.3 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий		Формы контроля
	Прак. зан.	Сам. раб.	

Согласована на портале № 46509

ОПК-1	+	+	Отчет по индивидуальному заданию, Защита отчета, Зачет, Тест
ОПК-2	+	+	Отчет по индивидуальному заданию, Защита отчета, Зачет, Тест
ОПК-3	+	+	Отчет по индивидуальному заданию, Защита отчета, Зачет, Тест
ОПК-4	+	+	Отчет по индивидуальному заданию, Защита отчета, Зачет, Тест
ОПК-5	+	+	Отчет по индивидуальному заданию, Защита отчета, Зачет, Тест

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
2 семестр			
1 Понятие информационной безопасности, ее роль в национальной 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.	2	ОПК-5
	Итого	2	
2 Терминологические основы информационной безопасности.	Понятие информации и смежных с 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	2	ОПК-5
	Итого	2	

Согласована на портале № 46509

3 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.	8	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
	Итого	8	
4 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 непреднамеренные. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Формирование модели нарушителя.	8	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
	Итого	8	
5 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 вычислительные системы, используемые для обработки конфиденциальной информации. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации	4	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
	Итого	4	
6 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	4	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5

Согласована на портале № 46509

	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		
	Итого	4	
7 Правовые основы информационной безопасности.	Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Субъекты и объекты правоотношений в области информационной безопасности. Отрасли законодательства, регламентирующие деятельность по защите информации. Правовые основы защиты конфиденциальной информации. Правовые основы защиты государственной тайны. Лицензирование и сертификация. Нормы ответственности за правонарушения в сфере компьютерных технологий.	4	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
	Итого	4	
8 Организационные основы информационной безопасности.	Задачи организационного обеспечения информационной безопасности. Роль нормативных документов в защите информации. Инвентаризация информационных ресурсов организации. Построение моделей документооборота и информационных систем. Модели нарушителя информационной безопасности. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации. Организация службы безопасности и работа с кадрами. Организация пропускного и внутри объектового режима.	4	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5
	Итого	4	
9 Методология и культура теоретических и экспериментальных	Методы индивидуальных теоретических и экспериментальных исследований, интеграция в научное сообщество, организация работы исследовательского коллектива.	2	ОПК-4

Согласована на портале № 46509

исследований и организация работы исследовательского коллектива в области информационной безопасности	Порядок выполнения научно-исследовательских работ (НИР). Результаты НИР. Паспорта научных специальностей по направлению "Информационная безопасность". Научная этика. Культура научных исследований.		
	Итого	2	
10 Организация преподавательской деятельности по основным образовательным программам высшего образования в области информационной безопасности	Организация преподавательской деятельности (виды контактной работы, организация самостоятельной работы, учебно-методическое обеспечение, педагогика и психология). Источники основных образовательных программ высшего образования в области информационной безопасности. Образовательные стандарты, профессиональные отраслевые стандарты	2	ОПК-5
	Итого	2	
Итого за семестр		40	

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
2 семестр				
1 Понятие информационной безопасности, ее роль в национальной безопасности.	Подготовка к практическим занятиям, семинарам	1	ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	1		
	Итого	2		
2 Терминологические основы информационной безопасности.	Подготовка к практическим занятиям, семинарам	1	ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	1		
	Итого	2		
3 Угрозы. Классификация и анализ угроз информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	2		
	Итого	4		
4 Модель угроз, модель нарушителя.	Подготовка к практическим занятиям, семинарам	2	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивиду-	2		

Согласована на портале № 46509

	альных заданий			
	Итого	4		
5 Модели оценки угроз конфиденциальности, целостности, доступности.	Подготовка к практическим занятиям, семинарам	2	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	2		
	Итого	4		
6 Функции и задачи защиты информации	Подготовка к практическим занятиям, семинарам	2	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Зачет, Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	2		
	Итого	4		
7 Правовые основы информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	2		
	Итого	4		
8 Организационные основы информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5	Защита отчета, Отчет по индивидуальному заданию, Тест
	Выполнение индивидуальных заданий	2		
	Итого	4		
9 Методология и культура теоретических и экспериментальных исследований и организация работы исследовательского коллектива в области информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ОПК-4	Зачет, Тест
	Итого	2		
10 Организация преподавательской деятельности по основным образовательным программам высшего образования в области информационной	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Зачет, Тест
	Итого	2		

Согласована на портале № 46509

безопасности				
Итого за семестр		32		
Итого		32		

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. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: https://e.lanbook.com/book/5171. — Загл. с экрана. — Режим доступа: https://e.lanbook.com/book/5171 (дата обращения: 18.09.2018).
2. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 [Электронный ресурс] [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: https://e.lanbook.com/book/5179. — Загл. с экрана. — Режим доступа: https://e.lanbook.com/book/5179 (дата обращения: 18.09.2018).

12.2. Дополнительная литература

1. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] [Электронный ресурс]: учебное пособие / Ю.И. Коваленко. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: https://e.lanbook.com/book/5163. — Загл. с экрана. — Режим доступа: https://e.lanbook.com/book/5163 (дата обращения: 18.09.2018).
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, Э.Р. Газизова ; под ред. А.А.Шелупанова, С.Л.Груздева, Ю.С.Нахаева. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: https://e.lanbook.com/book/5114. — Загл. с экрана. — Режим доступа: https://e.lanbook.com/book/5114 (дата обращения: 18.09.2018).

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 — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf (дата обращения: 18.09.2018).

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;

Согласована на портале № 46509

– 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. eLIBRARY.RU – российская научная электронная библиотека, интегрированная с Российским индексом научного цитирования (РИНЦ).
2. Scopus – библиографическая и реферативная база данных.
3. SpringerLink – хранилище электронных копий научных книг и журналов, издаваемых компанией Springer.
4. IEEE Xplore – электронная платформа, содержащая полные тексты публикаций из журналов, материалов конференций, стандартов, издаваемых IEEE и IEE (Institution of Electrical Engineers).
5. http://fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования.
6. http://www.nark-rspp.ru – Национальный реестр профессиональных стандартов.

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 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:

– Microsoft Windows 7 Pro

13.1.2. 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;

Согласована на портале № 46509

- 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);

Согласована на портале № 46509

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:

Согласована на портале № 46509

a) Аттестация;
b) Аудит;
c) Сертификация;
d) Пентест.

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

11. 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.

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

13. 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.

14. Какая угроза безопасности информации является преднамеренной?
a) Ошибки персонала;
b) Сбой программного обеспечения;
c) Фальсификация, подделка документов;
d) Открытие электронного письма, содержащего вирус.

15. 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.

16. Угроза диверсии относится к …
a) Субъективной преднамеренной причине нарушения целостности информации;
b) Субъективной непреднамеренной причине нарушения целостности информации;

Согласована на портале № 46509

c) Объективной непреднамеренной причине нарушения целостности информации;
d) Объективной преднамеренной причине нарушения целостности информации.

17. Перехват данных является угрозой:
a) Доступности;
b) Конфиденциальности;
c) Целостности;
d) Достоверности.

18. 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.

19. 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.

20. 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.

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

22. 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.

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

24. Защита информации это:

Согласована на портале № 46509

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.

25. Какой вид информации не относится к категории конфиденциальной информации?

a) Коммерческая тайна;

b) Тайна судопроизводства;

c) Персональные данные;

d) Государственная тайна.

14.1.2. Зачёт

1. Теория защиты информации. Основные направления
2. Обеспечение информационной безопасности и направления защиты
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
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 Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных
15. Методологические подходы к оценке уязвимости информации
16. Модель защиты системы с полным перекрытием
17. Рекомендации по использованию моделей оценки уязвимости информации Допущения в моделях оценки уязвимости информации Методы определения требований к защите информации
18. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации
19. Классификация требований к средствам защиты информации
20. Требования к защите, определяемые структурой автоматизированной системы обработки данных
21. Требования к защите, обуславливаемые видом защищаемой информации
22. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации
23. Анализ существующих методик определения требований к защите информации
24. Классы защищенности средств вычислительной техники от несанкционированного доступа
25. Функции защиты информации
26. Стратегии защиты информации
27. Способы и средства защиты информации
28. Способы «абсолютной системы защиты»
29. Архитектура систем защиты информации. Требования
30. Общеметодологических принципов архитектуры системы защиты информации
31. Построение средств защиты информации
32. Ядро системы защиты
33. Семирубежная модель защиты

Согласована на портале № 46509

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

35. Регуляторы в области защиты информации

36. Методы индивидуальных теоретических и экспериментальных исследований, интеграция в научное сообщество, организация работы исследовательского коллектива.

37. Порядок выполнения научно-исследовательских работ (НИР).

38. Результаты НИР.

39. Паспорта научных специальностей по направлению «Информационная безопасность».

40. Научная этика.

41. Культура научных исследований.

42. Организация преподавательской деятельности (виды контактной работы, организация самостоятельной работы, учебно-методическое обеспечение, педагогика и психология).

43. Источники основных образовательных программ высшего образования в области информационной безопасности.

44. Образовательные стандарты, профессиональные отраслевые стандарты.

14.1.3. 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)

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

14.2. 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.

Согласована на портале № 46509

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.

Согласована на портале № 46509