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
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **3**
Семестр: **6**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	44	44	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	72	72	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 6 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 38261

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) 10.05.04 Информационно-аналитические системы безопасности, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Ст. преподаватель каф. КИБЭВС _____ А. И. Гуляев

Доцент каф. КИБЭВС _____ Е. Ю. Костюченко

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. БИС _____ Р. В. Мещеряков

Эксперты:

Доцент каф. КИБЭВС _____ А. А. Конев

Доцент каф. БИС _____ О. О. Евсютин

Согласована на портале № 38261

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Цель – дать основы правового обеспечения информационной безопасности, а также формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

1.2. Задачи дисциплины

– Задачи дисциплины - дать основы:

– - законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;

– -понятий и видов защищаемой информации по законодательству РФ;

– - правовых режимов конфиденциальной информации;

– - правового режим защиты государственной тайны, системы защиты государственной тайны;

– - лицензирования и сертификации в области защиты информации, в том числе государственной тайны;

– -правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);

– -защиты интеллектуальной собственности;

– -правовой регламентации охранной деятельности;

– -правового регулирования взаимоотношений администрации и персонала в области защиты информации;

– - международного законодательства в области защиты информации;

– - знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований.

– -угроз информационной безопасности объекта;

– -организации службы безопасности объекта;

– - подбора и работы с кадрами в сфере информационной безопасности;

– - организации и обеспечения режима конфиденциальности;

– -охраны объектов.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» (Б1.В.ОД.4) относится к блоку 1 (вариативная часть).

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

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Техническая защита информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-16 способностью разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности;

– ПК-18 способностью выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные;

– ПК-20 способностью анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства;

– ПСК-2.2 способностью выполнять анализ корректности и устойчивости

Согласована на портале № 38261

функционирования отдельных компонентов, подсистем и в целом всей национальной системы по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма;

– ПСК-2.3 способностью решать задачи выявления, классификации и последующего предметного анализа информационных объектов с признаками подготовки и/или совершения преступлений в финансовой и экономической сферах деятельности;

В результате изучения дисциплины обучающийся должен:

– **знать** − основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; − правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах.

– **уметь** − применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

– **владеть** − профессиональной терминологией в области информационной безопасности; − навыками работы с нормативными правовыми актами; − навыками организации и обеспечения режима секретности; − методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации.

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
		6 семестр
Аудиторные занятия (всего)	72	72
Лекции	44	44
Практические занятия	28	28
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	36	36
Проработка лекционного материала	13	13
Подготовка к практическим занятиям, семинарам	23	23
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Согласована на портале № 38261

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
6 семестр					
1 Законодательство РФ в области информационной безопасности.	4	0	1	5	ПК-16, ПК-18, ПК-20
2 Правовые основы защиты конфиденциальной информации.	6	4	4	14	ПК-16, ПК-18, ПК-20, ПСК-2.2, ПСК-2.3
3 Правовые основы защиты государственной тайны.	6	4	6	16	ПК-20
4 Лицензирование и сертификация.	4	0	1	5	ПК-20
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	4	4	4	12	ПК-18, ПСК-2.2
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	4	4	5	13	ПК-20
7 Средства и методы физической защиты объектов.	4	4	3	11	ПК-20
8 Организация службы безопасности и работа с кадрами.	4	4	6	14	ПК-20
9 Организация и обеспечения режима секретности.	4	2	3	9	ПК-20
10 Организация пропускного и внутри объектового режима.	4	2	3	9	ПК-20
Итого за семестр	44	28	36	108	
Итого	44	28	36	108	

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
6 семестр			
1 Законодательство РФ в области информационной безопасности.	Понятие и структура информационной безопасности. Основные задачи системы 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	4	ПК-16, ПК-18, ПК-20

Согласована на портале № 38261

	защите информации.		
	Итого	4	
2 Правовые основы защиты конфиденциальной информации.	Конфиденциальная информация. Виды тайн. Коммерческая тайна. Профессиональные тайны. Служебная тайна. Персональные данные. Тайна следствия и судопроизводства. Банковская тайна. Тайна телефонных переговоров и переписки.	6	ПК-16, ПК-18, ПК-20, ПСК-2.2, ПСК-2.3
	Итого	6	
3 Правовые основы защиты государственной тайны.	Государственная тайна, как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Система защиты государственной тайны. Органы защиты государственной тайны и их компетенции. Порядок допуска и доступ к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.	6	ПК-20
	Итого	6	
4 Лицензирование и сертификация.	Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты	4	ПК-20
	Итого	4	
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Уголовно-правовые нормы. Основные принципы и понятия уголовного права. Преступления в сфере компьютерной информации. Экспертиза компьютерных преступлений. Административные правонарушения.	4	ПК-18, ПСК-2.2
	Итого	4	
6 Анализ объекта защиты с позиции организационного обеспечения 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	4	ПК-20

Согласована на портале № 38261

	безопасности. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.		
	Итого	4	
7 Средства и методы физической защиты объектов.	Структура системы физической защиты. Система охраны периметра. Система сигнализации, видеонаблюдения, контроля доступа: классификация, сферы применения.	4	ПК-20
	Итого	4	
8 Организация службы безопасности и работа с кадрами.	Служба безопасности объекта. Принципы деятельности службы безопасности. Задачи и функции службы безопасности. Структура службы безопасности. Функции сотрудников службы безопасности. Контроль состояния системы защиты, проведение служебных расследований. Подбор, расстановка и работа с кадрами. Внутренние угрозы информационной безопасности, социальная инженерия. Функции службы безопасности при подборе, увольнении сотрудников и текущей работе с ними. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.	4	ПК-20
	Итого	4	
9 Организация и обеспечения режима секретности.	Основные принципы организации и обеспечения секретного документооборота. Технологические меры поддержания информационной безопасности объектов. Организация совещания и переговоров. Регламентация предоставления сотрудникам допуска к информации ограниченного доступа. Регламентация выдачи (возврата) документов и работы с ними. Регламентация процедуры создания документа ограниченного доступа. Регламентация процедуры снятие грифа с документов ограниченного доступа и их уничтожения. Регламентация обмена документами с другими организациями. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического	4	ПК-20

Согласована на портале № 38261

	сотрудничества. Организация режима и охраны объектов в процессе транспортировки.		
	Итого	4	
10 Организация пропускного и внутри объектового режима.	Проектирование пропускного и внутри объектового режима. Категорирование помещений. Регламентация пропуска лиц в здания. Виды пропусков и порядок их оформления. Порядок пропуска автотранспорта на территорию организации. Регламентация приема и сдачи объекта под охрану. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения. Структура аварийного плана.	4	ПК-20
	Итого	4	
Итого за семестр		44	

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	10
Предшествующие дисциплины										
1 Основы информационной безопасности	+	+					+	+	+	+
2 Правоведение	+	+	+	+	+			+	+	
Последующие дисциплины										
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+					+	+	+	+
2 Техническая защита информации		+	+	+	+				+	+

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.	

Согласована на портале № 38261

ПК-16	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест
ПК-18	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест
ПК-20	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест
ПСК-2.2	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест
ПСК-2.3	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест

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 практические занятия, ч	Интерактивные лекции, ч	Всего, ч
6 семестр			
IT-методы	2	6	8
Работа в команде	2		2
Решение ситуационных задач	4		4
Мини-лекция		6	6
Итого за семестр:	8	12	20
Итого	8	12	20

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
6 семестр			
2 Правовые основы защиты конфиденциальной информации.	Работа с конфиденциальной информацией. Защита коммерческой тайны.	4	ПК-16, ПК-18, ПК-20, ПСК-2.2, ПСК-2.3
	Итого	4	
3 Правовые основы защиты государственной тайны.	Работа с государственной тайной.	4	ПК-20
	Итого	4	
5 Нормы ответственности за	Нарушение законодательства в сфере информационных технологий.	4	ПК-18, ПСК-2.2

Согласована на портале № 38261

правонарушения в сфере компьютерных технологий.	Компьютерные преступления.		
	Итого	4	
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Описание структуры защищаемой организации и видов защищаемой информации.	4	ПК-20
	Итого	4	
7 Средства и методы физической защиты объектов.	Определение угроз автоматизированной системе, обрабатывающей информацию ограниченного доступа, и требований к работе сотрудника с этой информацией.	4	ПК-20
	Итого	4	
8 Организация службы безопасности и работа с кадрами.	Разработка структуры службы безопасности организации.	4	ПК-20
	Итого	4	
9 Организация и обеспечения режима секретности.	Выбор способов и методов защиты информации и автоматизированной системы.	2	ПК-20
	Итого	2	
10 Организация пропускного и внутри объектового режима.	Проектирование пропускного и внутри объектового режима в организации.	2	ПК-20
	Итого	2	
Итого за семестр		28	

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
6 семестр				
1 Законодательство РФ в области информационной безопасности.	Проработка лекционного материала	1	ПК-16, ПК-18, ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Итого	1		
2 Правовые основы защиты конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	2	ПК-16, ПК-18, ПК-20, ПСК-2.2, ПСК-2.3	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	2		
	Итого	4		
3 Правовые основы защиты государственной	Подготовка к практическим занятиям, семинарам	4	ПК-20	Опрос на занятиях, Отчет по индивидуальному

Согласована на портале № 38261

тайны.	Проработка лекционного материала	2		заданию, Тест
	Итого	6		
4 Лицензирование и сертификация.	Проработка лекционного материала	1	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Итого	1		
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Подготовка к практическим занятиям, семинарам	3	ПК-18, ПСК-2.2	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Итого	4		
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	4	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Итого	5		
7 Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	2	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Итого	3		
8 Организация службы безопасности и работа с кадрами.	Подготовка к практическим занятиям, семинарам	4	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	2		
	Итого	6		
9 Организация и обеспечения режима секретности.	Подготовка к практическим занятиям, семинарам	2	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Итого	3		
10 Организация пропускного и внутри объектового режима.	Подготовка к практическим занятиям, семинарам	2	ПК-20	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Итого	3		
Итого за семестр		36		
	Подготовка и сдача	36		Экзамен

Согласована на портале № 38261

	экзамена			
Итого		72		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
6 семестр				
Опрос на занятиях	5	7	8	20
Отчет по индивидуальному заданию		10	10	20
Тест	10	10	10	30
Итого максимум за период	15	27	28	70
Экзамен				30
Нарастающим итогом	15	42	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не	Ниже 60 баллов	F (неудовлетворительно)

Согласована на портале № 38261

зачтено)		

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 1. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 214[2] с. : табл. - ISBN 978-5-91191-053-5 (наличие в библиотеке ТУСУР - 81 экз.)
2. Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 2. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 194[2] с. : табл. - ISBN 978-5-91191-054-5 (наличие в библиотеке ТУСУР - 81 экз.)

12.2. Дополнительная литература

1. Организационное обеспечение информационной безопасности : курс лекций для студентов специальности 090105 "Комплексное обеспечение информационной безопасности АС" / Г. А. Праскурин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005 - . Ч. 1. - Томск : ТУСУР, 2005. - 221 с. (наличие в библиотеке ТУСУР - 83 экз.)
2. Организационное обеспечение информационной безопасности : курс лекций для студентов специальности 090105 "Комплексное обеспечение информационной безопасности АС" / Г. А. Праскурин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005 - . Ч. 2. - Томск : ТУСУР, 2005. - 180 с. : ил. - Библиогр.: с. 179-180. (наличие в библиотеке ТУСУР - 82 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности [Электронный ресурс]: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. — Режим доступа: https://edu.tusur.ru/publications/2506 (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:

Согласована на портале № 38261

– в форме электронного документа;
– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. 1. Справочно-правовая система (СПС) КонсультантПлюс.
2. 2. Справочно-правовая система (СПС) ГАРАНТ.

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

Аудитория информатики, технологий и методов программирования

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard 78" с ПО ActivInspire;
- Проектор ViewSonic PJD5154 DLP;
- Компьютеры класса не ниже M/B ASUS P5LD2 i945P / AMD A8 3.33 GHz / DDR-III DIMM 4096 Mb / Radeon R7 / 1 Gb Seagate (10 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

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

Аудитория Интернет-технологий и информационно-аналитической деятельности

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;

Согласована на портале № 38261

- Компьютеры AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10

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:

Согласована на портале № 38261

14.1.1. Тестовые задания

Вопросы

Вопрос 1

Что такое информация в соответствии с Федеральным законом №149-ФЗ?

1. Сообщения и данные
2. Изображения
3. Сведения об интеллектуальной собственности
4. Сведения (сообщения, данные) независимо от формы их представления

Вопрос 2

Дата принятия Конституции Российской федерации?

1. 01 января 1991
2. 10 декабря 1992
3. 12 декабря 1993
4. 15 ноября 1994

Вопрос 3

Конфиденциальность информации это?

1. Целостность и доступность информации при ее обработке в автоматизированных системах управления технологическими процессами.
2. Сохранность персональных данных субъекта персональных данных при попытках доступа третьих лиц в информационную систему персональных данных.
3. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
4. Обязательно требование для выполнения лицом, получившим доступа к сведениям, содержащим государственную тайну.

Вопрос 4

Обладатель информации это?

1. Лицо, оформившее права на интеллектуальную собственность в соответствии с законодательством Российской Федерации об интеллектуальной собственности.
2. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
3. Юридическое лицо, оформляющее право на интеллектуальную собственность физических лиц и юридических лиц за исключением резидентов иностранных государств.
4. Юридическое лицо, зарегистрированное за пределами Российской Федерации и регистрирующее право интеллектуальной собственности на территории Российской Федерации.

Вопрос 5

Дата принятия Доктрины информационной безопасности Российской Федерации?

1. 21 июля 1993
2. 09 сентября 2000
3. 27 июня 2006
4. 05 декабря 2016

Вопрос 6

Обеспечение информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации?

1. Совокупность правовых, организационно-технических и экономических методов.
2. Совокупность правовых, организационных и технических методов.
3. Совокупность оперативно-розыскных, научно-технических, информационно-аналитических мер.
4. Совокупность оперативно-розыскных, научно-технических, информационно-

Согласована на портале № 38261

аналитических и иных мер.

Вопрос 7
Основные компоненты справочно-правовой системы?
1. Программная оболочка, экспертная группа юристов.
2. Программная оболочка, информационный банк.
3. Информационный банк, техническая поддержка.
4. Техническая поддержка, экспертная группа правоведов.

Вопрос 8
Каким образом делиться информация по категориям доступа?
1. Государственная тайна и персональные данные.
2. Общедоступная информация и информация ограниченного доступа.
3. Служебная тайна и адвокатская тайна.
4. Конфиденциальная информация и государственная тайна.

Вопрос 9
Пометка коммерческая тайна содержит:
1. Фамилия, имя, отчество индивидуального предпринимателя.
2. Наименование юридического лица.
3. Место нахождения юридического лица.
4. Наименование и место нахождения юридического лица.

Вопрос 10
Режим коммерческой тайны считается установленным?
1. После устного распоряжения генерального директора.
2. После собрания совета директоров юридического лица.
3. После письменного распоряжения уполномоченного лица.
4. После назначения лица, ответственного за защиту коммерческой тайны.

Вопрос 11
Какое количество типов актуальных угроз персональным данным описывается в постановлении Правительства РФ от 01.11.2012 №1119?
1. Один
2. Два
3. Три
4. Четыре

Вопрос 12
Контроль за выполнением требований к защите персональных данных, утвержденный постановлением Правительства РФ от 01.11.2012 №1119 выполняется не реже чем 1 раз в:
1. 1 год
2. 3 года
3. 5 лет
4. На усмотрение оператора персональных данных

Вопрос 13
Постановление Правительства РФ от 01.11.2012 №1119 устанавливает:
1. Классы защищенности персональных данных
2. Уровни защищенности персональных данных
3. Уровни значимости персональных данных
4. Все выше перечисленное

Вопрос 14

Согласована на портале № 38261

Выбор класса средств криптографической защиты информации в соответствии с приказом ФСБ от 10.07.2014 №378 основывается на:

1. Модели актуальных угроз персональных данных
2. Типе актуальных угроз персональных данных
3. Уровне защищенности персональных данных
4. Ни один из выше перечисленных пунктов

Вопрос 15

Какое минимальное число сотрудников устанавливает постановление Правительства от 03.02.2012 №79 соискателю лицензии на деятельность по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну) являющемуся юридическим лицом:

1. 1 сотрудник
2. 2 сотрудника
3. 3 сотрудника
4. 5 сотрудников

Вопрос 16

Какие требования к работникам соискателя лицензии на деятельность по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну) предъявляет постановление Правительства от 03.02.2012 №79:

1. Работа в штате по основному месту работы
2. Работа в штате по внешнему совместительству и высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет
3. Высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности
4. Работа в штате по основному месту работы и высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет

Вопрос 17

Для выполнения работ и услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации лицензиат ФСТЭК должен иметь в наличии:

1. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17 и ГОСТ 2.103-2013 ЕСКД Стадии разработки
2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17 и ГОСТ 2.119-2013 ЕСКД Эскизный проект
3. ГОСТ 2.503-2013 ЕСКД Правила внесения изменений и ГОСТ 2.610-2006 ЕСКД Правила выполнения эксплуатационных документов
4. ГОСТ Р 8.563-2009 Государственная система обеспечения единства измерений. Методики (методы) измерений и ГОСТ 28195-89 Оценка качества программных средств. Общие положения

Вариант 18

Для выполнения работ мониторингу информационной безопасности средств и систем информатизации лицензиат ФСТЭК должен иметь в наличии:

1. Средства управления информацией об угрозах безопасности информации
2. Программные средства контроля целостности
3. Программные средства формирования и контроля полномочий доступа в

Согласована на портале № 38261

информационных (автоматизированных) системах

4. Осциллографы

Вопрос 19

Для какого вида деятельности в соответствии с постановление Правительства от 16.04.2012 №313 не требуется получение лицензии:

1. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем

2. Монтаж шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну

3. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем

4. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств

Вопрос 20

Какое требование предъявляется к руководителю и (или) лицу, уполномоченное руководить работами по модернизации шифровальных (криптографических) средств

1. Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет

2. Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

3. Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

4. Любой из перечисленных пунктов

Вопрос 21

Какое требование предъявляется к руководителю и (или) лицу, уполномоченное руководить работами по передаче шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации

1. Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет

2. Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

3. Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

4. Любой из перечисленных пунктов

Согласована на портале № 38261

Вопрос 22

Какие организации создают свои системы сертификации средств защиты информации?

1. Федеральная служба безопасности Российской Федерации
2. Федеральная служба по техническому и экспортному контролю Российской Федерации
3. Министерство обороны Российской Федерации
4. Все вышеперечисленные

Вопрос 23

Какие из перечисленных функций не входят в перечень компетенций федерального органа по сертификации?

1. выдает сертификаты и лицензии на применение знака соответствия
2. приостанавливает или отменяет действие выданных сертификатов
3. формируют фонд нормативных документов, необходимых для сертификации
4. организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации

Вопрос 24

В компетенцию какого ведомства входит сертификация средств криптографической защиты информации?

1. Федеральная служба безопасности Российской Федерации
2. Федеральная служба по техническому и экспортному контролю Российской Федерации
3. Министерство обороны Российской Федерации
4. Все вышеперечисленные

Вопрос 25

В каком случае аттестация объекта информатизации является добровольной?

1. обработка государственной тайны
2. при защите государственного информационного ресурса
3. управление экологически опасными объектами
4. ведение конфиденциальных переговоров

Вопрос 26

Кто создает организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации

1. Федеральная служба безопасности Российской Федерации
2. Федеральная служба по техническому и экспортному контролю Российской Федерации
3. Министерство обороны Российской Федерации
4. Все вышеперечисленные

Вопрос 27

Какое действие не является обязательным при аттестации объектов информатизации по требованиям безопасности информации

1. подачу и рассмотрение заявки на аттестацию
2. разработка программы и методики аттестационных испытаний
3. испытание несертифицированных средств и систем защиты информации
4. оформление, регистрация и выдача "Аттестата соответствия"

Вопрос 28

Максимальный срок действия аттестата объекта информатизации в соответствии с "Положение по аттестации объектов информатизации по требованиям безопасности информации" утвержденного Гостехкомиссией РФ от 25.11.1994

1. 1 год
2. 2,5 года

Согласована на портале № 38261

3. 3 года
4. 5 лет

Вопрос 29

Какое постановление Правительства РФ регламентирует лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну?

1. Постановление Правительства РФ от 03.02.2012 N 79
2. Постановление Правительства РФ от 16.04.2012 N 313
3. Постановление Правительства РФ от 12.04.2012 N 287
4. Постановление Правительства РФ от 15.04.1995 N 333

Вопрос 30

Чем является защита государственной тайны?

1. видом основной деятельности
2. совокупностью органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях
3. техническими, криптографическими, программными и другими средствами, предназначенными для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средствами контроля эффективности защиты информации
4. процедурой оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений

14.1.2. Экзаменационные вопросы

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Конституционные гарантии прав граждан на информацию и механизм их реализации.
3. Понятие и виды защищаемой информации по законодательству РФ.
4. Государственная тайна как особый вид защищаемой информации.
5. Конфиденциальная информация.
6. Система защиты государственной тайны.
7. Правовой режим защиты государственной тайны.
8. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
9. Правовые режимы конфиденциальной информации.
10. Лицензирование и сертификация в области защиты информации, в том числе государственной тайны.
11. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).
12. Защита интеллектуальной собственности.
13. Правовая регламентация охранной деятельности.
14. Международное законодательство в области защиты информации.
15. Преступления в сфере компьютерной информации.
16. Экспертиза преступлений в области компьютерной информации.
17. Криминалистические аспекты проведения расследований.

14.1.3. Темы индивидуальных заданий

Задание №1.

Каждый студент для своего индивидуального задания по дисциплине «Комплексное обеспечение информационной безопасности» должен представить обоснование использования или разработки выбранной системы.

Должны быть рассмотрены следующие вопросы:

Согласована на портале № 38261

1) Перечень нормативно-правовых актов:
1.1) перечень законов;
1.2) перечень подзаконных актов.
2) Лицензирование и сертификация:
2.1) обоснование проведения лицензирования и сертификации (аттестации);
2.2) перечень контролирующих, сертифицирующих, аттестующих организаций;
3) Нормы ответственности за нарушение нормативно-правовых актов:
3.1) перечень статей;
3.2) перечень санкций согласно статьям.

Задание №2.

Индивидуальное задание №2 включает в себя самостоятельное изучение раздела курса, посвященного компьютерным правонарушениям. В задании необходимо привести не менее 4-5 примеров преступлений в сфере компьютерной информации, как в РФ, так и в зарубежных странах. Привести признаки и элементы состава преступления, расследование компьютерного преступления, особенности основных следственных действий. Описать какие статьи каких законов были нарушены, какую ответственность понесло лицо или группа лиц, совершивших преступление. Дать свои оценки преступлениям. Оценить проблемы судебного преследования за преступления в сфере компьютерной информации.

Задание №3

Индивидуальное задание №3 включает в себя разработку проектов нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

Каждый студент для своего индивидуального задания по дисциплине «Комплексное обеспечение информационной безопасности» должен представить в дополнение к Индивидуальному заданию №1

следующий перечень документов:

1) Перечень сведений конфиденциального характера.
2) Перечень лиц допущенных к сведениям конфиденциального характера.
3) Матрица разграничения доступа.
4) Регламент доступа лиц к сведениям ограниченного доступа.

14.1.4. Темы опросов на занятиях

Понятие и структура информационной безопасности. Основные задачи системы 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.

Конфиденциальная информация. Виды тайн. Коммерческая тайна. Профессиональные тайны. Служебная тайна. Персональные данные. Тайна следствия и судопроизводства. Банковская тайна. Тайна телефонных переговоров и переписки.

Государственная тайна, как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Система защиты государственной тайны. Органы защиты государственной тайны и их компетенции. Порядок допуска и доступ к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.

Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты

Уголовно-правовые нормы. Основные принципы и понятия уголовного права. Преступления в сфере компьютерной информации. Экспертиза компьютерных преступлений. Административные правонарушения.

Задачи организационного обеспечения информационной безопасности. Роль нормативных

Согласована на портале № 38261

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.

Структура системы физической защиты. Система охраны периметра. Система сигнализации, видеонаблюдения, контроля доступа: классификация, сферы применения.

Служба безопасности объекта. Принципы деятельности службы безопасности. Задачи и функции службы безопасности. Структура службы безопасности. Функции сотрудников службы безопасности. Контроль состояния системы защиты, проведение служебных расследований. Подбор, расстановка и работа с кадрами. Внутренние угрозы информационной безопасности, социальная инженерия. Функции службы безопасности при подборе, увольнении сотрудников и текущей работе с ними. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.

Основные принципы организации и обеспечения секретного документооборота. Технологические меры поддержания информационной безопасности объектов. Организация совещания и переговоров. Регламентация предоставления сотрудникам допуска к информации ограниченного доступа. Регламентация выдачи (возврата) документов и работы с ними. Регламентация процедуры создания документа ограниченного доступа. Регламентация процедуры снятие грифа с документов ограниченного доступа и их уничтожения. Регламентация обмена документами с другими организациями. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества. Организация режима и охраны объектов в процессе транспортировки.

Проектирование пропускного и внутри объектового режима. Категорирование помещений. Регламентация пропуска лиц в здания. Виды пропусков и порядок их оформления. Порядок пропуска автотранспорта на территорию организации. Регламентация приема и сдачи объекта под охрану. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения. Структура аварийного плана.

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 № 38261

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 № 38261