МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Управление информационной безопасностью

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **5**
Семестр: **9**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	28	28	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	80	80	часов
5	Из них в интерактивной форме	22	22	часов
6	Самостоятельная работа	28	28	часов
7	Всего (без экзамена)	108	108	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е

Экзамен: 9 семестр

Томск 2017

Согласована на портале № 20666

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от «26» 5 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа 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 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. КИБЭВС _____ А. А. Конев

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф.
БИС _____ Р. В. Мещеряков

Эксперт:

доцент каф. КИБЭВС _____ Е. Ю. Костюченко

Согласована на портале № 20666

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины является овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

1.2. Задачи дисциплины

– Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.

– Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.

– Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление информационной безопасностью» (Б1.В.ОД.16) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность жизнедеятельности, Безопасность операционных систем, Безопасность сетей ЭВМ, Документоведение, Организационное и правовое обеспечение информационной безопасности, Прикладная криптография, Теория вероятностей и математическая статистика.

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-6 способностью готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований;

– ПК-9 способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах;

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

– ПК-17 способностью организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности;

– ПК-19 способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей;

В результате изучения дисциплины студент должен:

– **знать** основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.

– **уметь** оценивать информационные риски в автоматизированных системах; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.

– **владеть** профессиональной терминологией в области информационной безопасности; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами управления информационной безопасностью автоматизированных си-

Согласована на портале № 20666

стем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

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
		9 семестр
Аудиторные занятия (всего)	80	80
Лекции	36	36
Практические занятия	28	28
Лабораторные работы	16	16
Из них в интерактивной форме	22	22
Самостоятельная работа (всего)	28	28
Оформление отчетов по лабораторным работам	8	8
Проработка лекционного материала	6	6
Подготовка к практическим занятиям, семинарам	14	14
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.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
9 семестр						
1 Анализ объекта защиты.	8	6	0	4	18	ПК-19, ПК-9
2 Модель угроз и модель нарушителя.	4	6	0	4	14	ПК-9
3 Оценка рисков информационной безопасности.	4	0	16	9	29	ПК-19, ПК-9
4 Система управления информационной безопасностью.	10	6	0	4	20	ПК-16, ПК-17, ПК-19, ПК-9
5 Политика информационной безопасности.	4	6	0	4	14	ПК-16, ПК-6

Согласована на портале № 20666

6 Управление инцидентами информационной безопасности.	6	4	0	3	13	ПК-16, ПК-17, ПК-9
Итого за семестр	36	28	16	28	108	
Итого	36	28	16	28	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
9 семестр			
1 Анализ объекта защиты.	Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности.	8	ПК-19, ПК-9
	Итого	8	
2 Модель угроз и модель нарушителя.	Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.	4	ПК-9
	Итого	4	
3 Оценка рисков информационной безопасности.	Основные положения стандартов в области управления рисками информационной безопасности.	4	ПК-19, ПК-9
	Итого	4	
4 Система управления информационной безопасностью.	Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. Организация управления персоналом в контексте обеспечения информационной безопасности.	10	ПК-16, ПК-17, ПК-19
	Итого	10	
5 Политика информационной безопасности.	Основные положения стандартов в области регламентации обеспечения информационной безопасности.	4	ПК-16, ПК-6
	Итого	4	
6 Управление инцидентами информационной безопасности.	Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.	6	ПК-16, ПК-17
	Итого	6	

Согласована на портале № 20666

Итого за семестр		36	

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
Предшествующие дисциплины						
1 Безопасность жизнедеятельности						+
2 Безопасность операционных систем		+	+	+	+	
3 Безопасность сетей ЭВМ		+	+	+	+	
4 Документоведение	+					
5 Организационное и правовое обеспечение информационной безопасности			+	+	+	
6 Прикладная криптография		+	+	+	+	
7 Теория вероятностей и математическая статистика			+			
Последующие дисциплины						
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+
2 Преддипломная практика	+	+	+	+	+	+
3 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 и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий				Формы контроля
	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	
ПК-6	+	+		+	Экзамен, Отчет по практическому занятию
ПК-9	+	+		+	Экзамен, Отчет по практическому занятию

Согласована на портале № 20666

ПК-16	+	+		+	Экзамен, Отчет по практическому занятию
ПК-17	+	+		+	Экзамен, Отчет по практическому занятию
ПК-19	+		+	+	Экзамен, Отчет по лабораторной работе

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лабораторные занятия	Интерактивные лекции	Всего
9 семестр				
IT-методы	8	4		12
Презентации с использованием слайдов с обсуждением			10	10
Итого за семестр:	8	4	10	22
Итого	8	4	10	22

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
3 Оценка рисков информационной безопасности.	Оценка соответствия системы управления информационной безопасностью требованиям стандарта СТО БР ИББС 1.0 – 2006.	4	ПК-19
	Анализ рисков информационной безопасности на основе построения модели информационных потоков.	4	
	Анализ рисков на основе модели угроз и уязвимостей.	4	
	Анализ рисков на основе DigitalSecurity. Кондор.	4	
	Итого	16	
Итого за семестр		16	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Согласована на портале № 20666

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Анализ объекта защиты.	Формальное описание структуры информационной системы.	6	ПК-9
	Итого	6	
2 Модель угроз и модель нарушителя.	Составление модели угроз информационной системе.	6	ПК-9
	Итого	6	
4 Система управления информационной безопасностью.	Формирование требований к системе защиты информации.	6	ПК-9
	Итого	6	
5 Политика информационной безопасности.	Формирование требований к политике информационной безопасности.	6	ПК-16, ПК-6
	Итого	6	
6 Управление инцидентами информационной безопасности.	Формирование регламента действий при возникновении нештатных ситуаций.	4	ПК-17, ПК-9
	Итого	4	
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
9 семестр				
1 Анализ объекта защиты.	Подготовка к практическим занятиям, семинарам	3	ПК-9, ПК-19	Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	4		
2 Модель угроз и модель нарушителя.	Подготовка к практическим занятиям, семинарам	3	ПК-9	Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		

Согласована на портале № 20666

	Итого	4		
3 Оценка рисков информационной безопасности.	Проработка лекционного материала	1	ПК-19, ПК-9	Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	8		
	Итого	9		
4 Система управления информационной безопасностью.	Подготовка к практическим занятиям, семинарам	3	ПК-9, ПК-16, ПК-17, ПК-19	Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	4		
5 Политика информационной безопасности.	Подготовка к практическим занятиям, семинарам	3	ПК-16, ПК-6	Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	4		
6 Управление инцидентами информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПК-17, ПК-9, ПК-16	Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
Итого за семестр		28		
	Подготовка и сдача экзамена	36		Экзамен
Итого		64		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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
9 семестр				
Отчет по лабораторной работе		20	20	40
Отчет по практическому занятию	12	12	6	30
Итого максимум за период	12	32	26	70

Согласована на портале № 20666

Экзамен				30
Нарастающим итогом	12	44	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 зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью». Выпуск 1 [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. – Электрон. дан. – М.: Горячая линия-Телеком, 2012. – 244 с. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5178

12.2. Дополнительная литература

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=173886

2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2008, 31 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=129018

3. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2014, 106 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183918

4. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М., 2014, 58 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183599

5. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обес-

Согласована на портале № 20666

печения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012, 62 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=179060

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=177398

7. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=175608

8. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187871

9. ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183954

10. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187948

11. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=184904

12. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=179072

13. ГОСТ Р ИСО/МЭК 27033-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187869

14. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187929

15. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187854

16. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]. - http://protect.gost.ru/document1.aspx?control=31&id=204467

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А. Управление информационной безопасностью: презентации по курсу лекций [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/work_progs/kaa1/UIB-lect.zip

2. Конев А.А. Управление информационной безопасностью: методические указания по выполнению практических работ [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/work_progs/kaa1/UIB-pract.pdf

3. Конев А.А. Управление информационной безопасностью: методические указания по выполнению лабораторных работ [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/work_progs/kaa1/UIB-labs.zip

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся

Согласована на портале № 20666

из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. http://protect.gost.ru/

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 808. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Аудиосистема – 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор Optoma – 1 шт.; Компьютер лекционный ASUS ASRock AMD E2-1800/4 ГБ – 1 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 7 SP1; Microsoft Powerpoint Viewer. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 400. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи

Согласована на портале № 20666

учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

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

Согласована на портале № 20666

– представление ответов устно.

Процедура оценивания результатов обучения 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 20666

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Управление информационной безопасностью

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **5**
Семестр: **9**

Учебный план набора 2013 года

Разработчик:
- доцент каф. КИБЭВС А. А. Конев

Экзамен: 9 семестр

Томск 2017

Согласована на портале № 20666

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-19	способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей	Должен знать основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.; Должен уметь оценивать информационные риски в автоматизированных системах; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.; Должен владеть профессиональной терминологией в области информационной безопасности; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами управления информационной безопасностью автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизи-
ПК-17	способностью организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности	
ПК-16	способностью разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности	
ПК-9	способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	
ПК-6	способностью готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований	

Согласована на портале № 20666

		рованных информационных систем.;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-19

ПК-19: способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.	навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;

Согласована на портале № 20666

Используемые средства оценивания	• Отчет по лабораторной работе; • Экзамен;	• Отчет по лабораторной работе; • Экзамен;	• Отчет по лабораторной работе; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• в полном объеме знает методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;	• в полном объеме умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;	• в полном объеме владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
Хорошо (базовый уровень)	• на продвинутом уровне знает методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;	• на продвинутом уровне умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;	• на продвинутом уровне владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
Удовлетворительно (пороговый уровень)	• на базовом уровне знает методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;	• на базовом уровне умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;	• на базовом уровне владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;

2.2 Компетенция ПК-17

ПК-17: способностью организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	принципы управления персоналом при организации системы защиты информации.	подбирать и организовывать работу сотрудников с информацией ограниченного доступа.	методиками контроля работы персонала при обеспечении информационной безопасности.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические заня-	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические заня-	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная ра-

Согласована на портале № 20666

	тия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	тия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	бота;
Используемые средства оценивания	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• в полном объеме знает принципы управления персоналом при организации системы защиты информации;	• в полном объеме умеет подбирать и организовывать работу сотрудников с информацией ограниченного доступа;	• в полном объеме владеет методиками контроля работы персонала при обеспечении информационной безопасности;
Хорошо (базовый уровень)	• на продвинутом уровне знает принципы управления персоналом при организации системы защиты информации;	• на продвинутом уровне умеет подбирать и организовывать работу сотрудников с информацией ограниченного доступа;	• на продвинутом уровне владеет методиками контроля работы персонала при обеспечении информационной безопасности;
Удовлетворительно (пороговый уровень)	• на базовом уровне знает принципы управления персоналом при организации системы защиты информации;	• на базовом уровне умеет подбирать и организовывать работу сотрудников с информацией ограниченного доступа;	• на базовом уровне владеет методиками контроля работы персонала при обеспечении информационной безопасности;

2.3 Компетенция ПК-16

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

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	типовые нормативные документы по защите информации в информационно-аналитических системах.	составлять типовые нормативные документы по защите информации в информационно-аналитических системах.	методикой составления типовых нормативных документов по защите информации на основе действующих стандартов.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабо-	• Интерактивные практические занятия; • Интерактивные лабо-	• Интерактивные практические занятия; • Интерактивные лабо-

Согласована на портале № 20666

	раторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	раторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	раторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• в полном объеме знает типовые нормативные документы по защите информации в информационно-аналитических системах;	• в полном объеме умеет составлять типовые нормативные документы по защите информации в информационно-аналитических системах;	• в полном объеме владеет методикой составления типовых нормативных документов по защите информации на основе действующих стандартов;
Хорошо (базовый уровень)	• на продвинутом уровне знает типовые нормативные документы по защите информации в информационно-аналитических системах;	• на продвинутом уровне умеет составлять типовые нормативные документы по защите информации в информационно-аналитических системах;	• на продвинутом уровне владеет методикой составления типовых нормативных документов по защите информации на основе действующих стандартов;
Удовлетворительно (пороговый уровень)	• на базовом уровне знает типовые нормативные документы по защите информации в информационно-аналитических системах;	• на базовом уровне умеет составлять типовые нормативные документы по защите информации в информационно-аналитических системах;	• на базовом уровне владеет методикой составления типовых нормативных документов по защите информации на основе действующих стандартов;

2.4 Компетенция ПК-9

ПК-9: способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 9.

Таблица 9 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основные методы управления информационной безопасностью.	оценивать информационные риски в автоматизированных системах.	методами управления информационной безопасностью автоматизированных систем.

Согласована на портале № 20666

Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 10.

Таблица 10 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• в полном объеме знает основные методы управления информационной безопасностью;	• в полном объеме умеет оценивать информационные риски в автоматизированных системах;	• в полном объеме владеет методами управления информационной безопасностью автоматизированных систем;
Хорошо (базовый уровень)	• на продвинутом уровне знает основные методы управления информационной безопасностью;	• на продвинутом уровне умеет оценивать информационные риски в автоматизированных системах;	• на продвинутом уровне владеет методами управления информационной безопасностью автоматизированных систем;
Удовлетворительно (пороговый уровень)	• на базовом уровне знает основные методы управления информационной безопасностью;	• на базовом уровне умеет оценивать информационные риски в автоматизированных системах;	• на базовом уровне владеет методами управления информационной безопасностью автоматизированных систем;

2.5 Компетенция ПК-6

ПК-6: способностью готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 11.

Таблица 11 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	принципы формирования политики информационной безопасности в автоматизированных системах.	разрабатывать частные политики информационной безопасности автоматизированных систем.	методикой формирования политики информационной безопасности на основе действующих стандартов.

Согласована на портале № 20666

Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 12.

Таблица 12 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• в полном объеме знает принципы формирования политики информационной безопасности в автоматизированных системах;	• в полном объеме умеет разрабатывать частные политики информационной безопасности автоматизированных систем;	• в полном объеме владеет методикой формирования политики информационной безопасности на основе действующих стандартов;
Хорошо (базовый уровень)	• на продвинутом уровне знает принципы формирования политики информационной безопасности в автоматизированных системах;	• на продвинутом уровне умеет разрабатывать частные политики информационной безопасности автоматизированных систем;	• на продвинутом уровне владеет методикой формирования политики информационной безопасности на основе действующих стандартов;
Удовлетворительно (пороговый уровень)	• на базовом уровне знает принципы формирования политики информационной безопасности в автоматизированных системах;	• на базовом уровне умеет разрабатывать частные политики информационной безопасности автоматизированных систем;	• на базовом уровне владеет методикой формирования политики информационной безопасности на основе действующих стандартов;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Экзаменационные вопросы

– 1. Цель и этапы анализа объектов защиты.

– 2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.

Согласована на портале № 20666

– 3. Идентификация и классификация объектов защиты.

– 4. Типизация информационных систем. Данные об информационной системе, необходимые для построения модели документооборота.

– 5. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.

– 6. Подходы к построению модели нарушителя.

– 7. Классификация нарушителей (ФСТЭК).

– 8. Классификация угроз безопасности персональных данных (ФСТЭК).

– 9. Методика определения актуальных угроз (ФСТЭК).

– 10. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.

– 11. Угрозы, источником которых является персонал организации.

– 12. Методы «социальной инженерии» и способы защиты от них.

– 13. Обязанности сотрудников Службы безопасности при приёме сотрудников на работу.

– 14. Нормативная документация, обязательная к ознакомлению и подписанию при приёме на работу.

– 15. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.

– 16. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.

– 17. Упрощённая модель классификации субъектов.

– 18. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.

– 19. Основные положения регламента контроля использования технических средств обработки и передачи информации.

– 20. Основные положения инструкции по организации парольной защиты.

– 21. Основные положения документов, регламентирующих использование средств аутентификации и носителей ключевой информации.

– 22. Основные положения инструкции по организации антивирусной защиты.

– 23. Основные положения инструкции по работе с электронной почтой.

– 24. Типы чрезвычайных ситуаций. Структура аварийного плана. Причины изменения аварийного плана.

– 25. Классификация объектов при составлении аварийного плана.

– 26. Требования к различным классам объектов и их резервированию.

– 27. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.

– 28. Приведите примеры источников информации об инцидентах информационной безопасности.

– 29. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.

– 30. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

3.2 Вопросы для подготовки к практическим занятиям, семинарам

– Формальное описание структуры информационной системы.

– Составление модели угроз информационной системе.

– Формирование требований к системе защиты информации.

– Формирование требований к политике информационной безопасности.

– Формирование регламента действий при возникновении нештатных ситуаций.

3.3 Темы лабораторных работ

– Оценка соответствия системы управления информационной безопасностью требованиям

Согласована на портале № 20666

стандарта СТО БР ИББС 1.0 – 2006.

– Анализ рисков информационной безопасности на основе построения модели информационных потоков.

– Анализ рисков на основе модели угроз и уязвимостей.

– Анализ рисков на основе DigitalSecurity. Кондор.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью». Выпуск 1 [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. – Электрон. дан. – М.: Горячая линия-Телеком, 2012. – 244 с. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5178

4.2. Дополнительная литература

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=173886

2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2008, 31 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=129018

3. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2014, 106 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183918

4. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М., 2014, 58 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183599

5. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012, 62 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=179060

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=177398

7. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=175608

8. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187871

9. ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=183954

10. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187948

11. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных техноло-

Согласована на портале № 20666

гий к обеспечению непрерывности бизнеса. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=184904

12. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=179072

13. ГОСТ Р ИСО/МЭК 27033-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187869

14. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187929

15. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. [Электронный ресурс]. - http://protect.gost.ru/document.aspx?control=7&id=187854

16. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]. - http://protect.gost.ru/document1.aspx?control=31&id=204467

4.3. Обязательные учебно-методические пособия

1. Конев А.А. Управление информационной безопасностью: презентации по курсу лекций [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/work_progs/kaa1/UIB-lect.zip

2. Конев А.А. Управление информационной безопасностью: методические указания по выполнению практических работ [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/work_progs/kaa1/UIB-pract.pdf

3. Конев А.А. Управление информационной безопасностью: методические указания по выполнению лабораторных работ [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/work_progs/kaa1/UIB-labs.zip

4.4. Базы данных, информационно справочные и поисковые системы

1. http://protect.gost.ru/

Согласована на портале № 20666