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): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **6**
Семестр: **11, 12**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	11 семестр	12 семестр	Всего	Единицы
1	Лекции	4	4	8	часов
2	Практические занятия	4	4	8	часов
3	Лабораторные работы	8	8	16	часов
4	Всего аудиторных занятий	16	16	32	часов
5	Самостоятельная работа	56	47	103	часов
6	Всего (без экзамена)	72	63	135	часов
7	Подготовка и сдача экзамена		9	9	часов
8	Общая трудоемкость	72	72	144	часов
		4.0		4.0	З.Е

Контрольные работы: 12 семестр - 1
Экзамен: 12 семестр

Томск 2017

Согласована на портале № 20972

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от «29» 5 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16 января 2017 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 ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф.
КИБЭВС _____ А. А. Шелупанов

Эксперт:

доцент каф. КИБЭВС _____ Е. Ю. Костюченко

Согласована на портале № 20972

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.5) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность жизнедеятельности, Безопасность операционных систем, Документоведение, Организационное и правовое обеспечение информационной безопасности, Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-2 способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа;

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 систем; 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	
		11 семестр	12 семестр
Аудиторные занятия (всего)	32	16	16

Согласована на портале № 20972

Лекции	8	4	4
Практические занятия	8	4	4
Лабораторные работы	16	8	8
Самостоятельная работа (всего)	103	56	47
Оформление отчетов по лабораторным работам	16	8	8
Проработка лекционного материала	4	2	2
Самостоятельное изучение тем (вопросов) теоретической части курса	62	42	20
Подготовка к практическим занятиям, семинарам	8	4	4
Выполнение контрольных работ	13		13
Всего (без экзамена)	135	72	63
Подготовка и сдача экзамена	9		9
Общая трудоемкость ч	144	72	72
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
11 семестр						
1 Анализ объекта защиты.	2	2	0	3	7	ПСК-2
2 Оценка рисков информационной безопасности.	2	2	8	53	65	ПСК-2
Итого за семестр	4	4	8	56	72	
12 семестр						
3 Система управления информационной безопасностью.	2	2	8	44	56	ПСК-2
4 Управление инцидентами информационной безопасности.	2	2	0	3	7	ПСК-2
Итого за семестр	4	4	8	47	63	
Итого	8	8	16	103	135	

Согласована на портале № 20972

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
11 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.	2	ПСК-2
	Итого	2	
2 Оценка рисков информационной безопасности.	Основные положения стандартов в области управления рисками информационной безопасности. Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.	2	ПСК-2
	Итого	2	
Итого за семестр		4	
12 семестр			
3 Система управления информационной безопасностью.	Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. Организация управления персоналом в контексте обеспечения информационной безопасности.	2	ПСК-2
	Итого	2	
4 Управление инцидентами информационной безопасности.	Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.	2	ПСК-2
	Итого	2	
Итого за семестр		4	
Итого		8	

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.

Согласована на портале № 20972

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
Предшествующие дисциплины				
1 Безопасность жизнедеятельности				
2 Безопасность операционных систем		+		
3 Документоведение	+			
4 Организационное и правовое обеспечение информационной безопасности		+		
5 Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы	+	+		
6 Преддипломная практика	+	+		

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	
ПСК-2	+	+	+	+	Экзамен, Проверка контрольных работ, Отчет по лабораторной работе, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

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
12 семестр			
3 Система управления	Оценка соответствия системы управле-	4	ПСК-2

Согласована на портале № 20972

информационной безопасностью.	ния информационной безопасностью требованиям стандарта СТО БР ИББС 1.0 – 2006.		
	Анализ рисков на основе DigitalSecurity. Кондор.	4	
	Итого	8	
Итого за семестр		8	
11 семестр			
2 Оценка рисков информационной безопасности.	Анализ рисков информационной безопасности на основе построения модели информационных потоков.	4	ПСК-2
	Анализ рисков на основе модели угроз и уязвимостей.	4	
	Итого	8	
Итого за семестр		8	
Итого		16	

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
11 семестр			
1 Анализ объекта защиты.	Формальное описание структуры информационной системы.	2	ПСК-2
	Итого	2	
2 Оценка рисков информационной безопасности.	Составление модели угроз информационной системе.	2	ПСК-2
	Итого	2	
Итого за семестр		4	
12 семестр			
3 Система управления информационной безопасностью.	Формирование требований к системе защиты информации.	2	ПСК-2
	Итого	2	
4 Управление инцидентами информационной безопасности.	Формирование регламента действий при возникновении нештатных ситуаций.	2	ПСК-2
	Итого	2	
Итого за семестр		4	
Итого		8	

Согласована на портале № 20972

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
11 семестр				
1 Анализ объекта защиты.	Подготовка к практическим занятиям, семинарам	2	ПСК-2	Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
2 Оценка рисков информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПСК-2	Отчет по лабораторной работе, Отчет по практическому занятию, Экзамен
	Самостоятельное изучение тем (вопросов) теоретической части курса	42		
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	8		
	Итого	53		
Итого за семестр		56		
12 семестр				
3 Система управления информационной безопасностью.	Выполнение контрольных работ	13	ПСК-2	Отчет по лабораторной работе, Отчет по практическому занятию, Проверка контрольных работ, Экзамен
	Подготовка к практическим занятиям, семинарам	2		
	Самостоятельное изучение тем (вопросов) теоретической части курса	20		
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	8		
	Итого	44		
4 Управление инцидентами информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПСК-2	Отчет по практическому занятию, Экзамен
	Проработка лекционного	1		

Согласована на портале № 20972

	материала			
	Итого	3		
Итого за семестр		47		
	Подготовка и сдача экзамена	9		Экзамен
Итого		112		

9.1. Темы контрольных работ

1. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации политики информационной безопасности.
2. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации распределения обязанностей в сфере информационной безопасности организации.
3. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации взаимодействия со сторонними организациями.
4. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления активами организации.
5. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации классификации защищаемой информации.
6. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления персоналом при работе с защищаемой информацией.
7. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации физической безопасности организации и её оборудования.
8. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управлению информационными системами (в т.ч. телекоммуникационными).
9. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления доступом к информации и информационным системам.
10. Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления инцидентами информационной безопасности и непрерывностью бизнеса.

9.2. Темы для самостоятельного изучения теоретической части курса

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
3. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
4. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.
5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
6. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

Не предусмотрено

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-

Согласована на портале № 20972

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 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 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

Согласована на портале № 20972

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 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/

Согласована на портале № 20972

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 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	Тесты, письменные самостоятельные работы, вопросы к зачету,	Преимущественно проверка методами, исходя из состояния

Согласована на портале № 20972

показаниям	контрольные работы, устные ответы	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;
- 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 № 20972

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): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **6**
Семестр: **11, 12**

Учебный план набора 2013 года

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

Экзамен: 12 семестр

Томск 2017

Согласована на портале № 20972

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
ПСК-2	способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа	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-

Согласована на портале № 20972

		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 ПСК-2

ПСК-2: способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа.

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.	оценивать информационные риски в автоматизированных системах.	методами выявления угроз информационной безопасности и оценки информационных рисков.
Виды занятий	• Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по практическому занятию; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практическому занятию; • Экзамен;	• Отчет по лабораторной работе; • Отчет по практическому занятию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в та-

Согласована на портале № 20972

блице 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 оценивать информационные риски в автоматизированных системах;	• в полном объеме владеет методами выявления угроз информационной безопасности и оценки информационных рисков;
Хорошо (базовый уровень)	• на продвинутом уровне знает методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;	• на продвинутом уровне умеет оценивать информационные риски в автоматизированных системах;	• на продвинутом уровне владеет методами выявления угроз информационной безопасности и оценки информационных рисков;
Удовлетворительно (пороговый уровень)	• на базовом уровне знает методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;	• на базовом уровне умеет оценивать информационные риски в автоматизированных системах;	• на базовом уровне владеет методами выявления угроз информационной безопасности и оценки информационных рисков;

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 Темы контрольных работ

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации политики информационной безопасности.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации распределения обязанностей в сфере информационной безопасности организации.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации взаимодействия со сторонними организациями.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления активами организации.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации классификации защищаемой информации.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления персоналом при работе с защищаемой информацией.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации физической безопасности организации и её оборудования.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управлению информационными системами (в т.ч. телекоммуникационными).

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления доступом к информации и информационным системам.

– Сформулируйте разделы документа (-ов), содержащего рекомендации по реализации управления инцидентами информационной безопасности и непрерывностью бизнеса.

Согласована на портале № 20972

3.2 Экзаменационные вопросы

– 1. Цель и этапы анализа объектов защиты. 2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем. 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.

3.3 Вопросы для подготовки к практическим занятиям, семинарам

– Формальное описание структуры информационной системы.
– Составление модели угроз информационной системе.
– Формирование требований к системе защиты информации.
– Формирование регламента действий при возникновении нештатных ситуаций.

3.4 Темы лабораторных работ

– Оценка соответствия системы управления информационной безопасностью требованиям 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 /

Согласована на портале № 20972

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 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]. -

Согласована на портале № 20972

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 № 20972