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

Разработка и эксплуатация защищенных автоматизированных систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **7, 8, 9**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	8 семестр	9 семестр	Всего	Единицы
1	Лекции	36	46		82	часов
2	Практические занятия	28	10	8	46	часов
3	Лабораторные работы	16	28		44	часов
4	Контроль самостоятельной работы (курсовой проект / курсовая работа)			8	8	часов
5	Всего аудиторных занятий	80	84	16	180	часов
6	Из них в интерактивной форме	22	22		44	часов
7	Самостоятельная работа	28	60	20	108	часов
8	Всего (без экзамена)	108	144	36	288	часов
9	Подготовка и сдача экзамена	36	36		72	часов
10	Общая трудоемкость	144	180	36	360	часов
		4.0	5.0	1.0	10.0	З.Е

Экзамен: 7, 8 семестр
Курсовая работа (проект): 9 семестр

Согласована на портале № 14690

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «10» 2 2017 г.

Томск 2017

Согласована на портале № 14690

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 2016-12-01 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

аспирант каф. КИБЭВС _____ Якимук А. Ю.

Заведующий обеспечивающей каф. КИБЭВС _____ Шелупанов А. А.

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

Декан ФБ _____ Давыдова Е. М.

Заведующий выпускающей каф. КИБЭВС _____ Шелупанов А. А.

Эксперты:

доцент каф. КИБЭВС _____ Конев А. А.

Согласована на портале № 14690

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является: освоение основных методов, использующихся при работе с защищенными автоматизированными системами на этапах их разработки, реализации и эксплуатации.

1.2. Задачи дисциплины

– Задачами изучения дисциплины являются: дать студентам знания о способах проектирования и документального оформления процесса разработки защищенных автоматизированных систем на основе специализированных международных стандартов, развить в них умения и навыки применения специализированных международных стандартов при разработке средств защиты информации, умения и навыки в области разработки защищенных автоматизированных систем в соответствии с требованиями профиля защиты, а также дать знания о методах организации и регламентации процесса эксплуатации защищенных автоматизированных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» (Б1.Б.18) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность программного обеспечения, Программно-аппаратные средства обеспечения информационной безопасности, Распределённые автоматизированные информационные системы, Системное администрирование, Системное программирование, Теоретические основы компьютерной безопасности, Технологии и методы программирования, Управление информационной безопасностью.

Последующими дисциплинами являются: .

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;

– ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;

– ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

– ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы;

– ПК-20 способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;

– ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;

– ПК-28 способностью управлять информационной безопасностью автоматизированной системы;

В результате изучения дисциплины студент должен:

– **знать** − основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; − автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; − методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; − содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; − методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; − основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные,

Согласована на портале № 14690

криптографические, технические); − основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; − основные информационные технологии, используемые в автоматизированных системах.

– **уметь** - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем; - восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.

– **владеть** − профессиональной терминологией в области информационной безопасности; − навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; − методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; − навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; − навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 10.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры		
		7 семестр	8 семестр	9 семестр
Аудиторные занятия (всего)	180	80	84	16
Лекции	82	36	46	
Практические занятия	46	28	10	8
Лабораторные работы	44	16	28	
Контроль самостоятельной работы (курсовой проект / курсовая работа)	8			8
Из них в интерактивной форме	44	22	22	
Самостоятельная работа (всего)	108	28	60	20
Выполнение курсового проекта (работы)	10			10
Оформление отчетов по лабораторным работам	36	6	30	
Проработка лекционного материала	28	10	18	
Подготовка к практическим занятиям, семинарам	34	12	12	10
Всего (без экзамена)	288	108	144	36
Подготовка и сдача экзамена	72	36	36	

Согласована на портале № 14690

Общая трудоемкость ч	360	144	180	36
Зачетные Единицы	10.0	4.0	5.0	1.0

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	Курсовая работа	Всего часов (без экзамена)	Формируемые компетенции
7 семестр							
1 Составление технического задания на автоматизированные информационные системы	4	0	0	2	0	6	
2 Проектирование автоматизированных информационных систем	8	0	0	2	0	10	ПК-9
3 Основные стадии создания автоматизированных информационных систем	8	8	0	6	0	22	ПК-20
4 Содержание работ на этапах создания автоматизированных информационных систем	8	10	0	6	0	24	ПК-8
5 Средства автоматизации проектирования автоматизированных информационных систем	8	10	16	12	0	46	ПК-12, ПК-13, ПК-8, ПК-9
Итого за семестр	36	28	16	28	0	108	
8 семестр							
6 Средства построения пользовательского интерфейса	8	2	0	14	0	24	ПК-20, ПК-8, ПК-9
7 Средства разработки программно-информационного ядра информационных систем	8	4	16	16	0	44	ПК-12, ПК-13, ПК-20, ПК-28, ПК-8, ПК-9
8 Тестирование автоматизированных информационных систем	8	0	12	12	0	32	ПК-25
9 Подготовка приложения к распространению	8	4	0	10	0	22	ПК-20, ПК-25
10 Ввод в эксплуатацию автоматизированных	8	0	0	4	0	12	ПК-20, ПК-25, ПК-28

Согласована на портале № 14690

информационных систем							
11 Эксплуатация автоматизированных информационных систем	6	0	0	4	0	10	ПК-25, ПК-28
Итого за семестр	46	10	28	60	0	144	
9 семестр							
12 Формирование заданий на курсовую работу. Составление технического задания на разработку автоматизированной системы.	0	2	0	6	8	8	ПК-13
13 Проведение предпроектного исследования. Защита результатов научно-исследовательской работы.	0	2	0	4		6	ПК-12, ПК-13
14 Реализация модуля безопасности системы.	0	2	0	8		10	ПК-12, ПК-13, ПК-8, ПК-9
15 Анализ результатов выполнения этапов написания курсовой работы	0	2	0	2		4	ПК-20, ПК-25, ПК-28
Итого за семестр	0	8	0	20	8	36	
Итого	82	46	44	108	8	288	

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
7 семестр			
1 Составление технического задания на автоматизированные информационные системы	Предмет и задачи курса. Краткий обзор изучаемого материала на семестр. Изучение государственных стандартов, содержащих требования к составлению технической документации на этапе планирования работ - ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение», ГОСТ 19.201-78 «ЕСКД Техническое здание. Требование к содержанию и оформлению» и ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».	4	

Согласована на портале № 14690

	Рассмотрение примера технического задания на разработку автоматизированной системы.		
	Итого	4	
2 Проектирование автоматизированных информационных систем	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к построению автоматизированных систем ГОСТ 24.104-85 «Автоматизированные системы управления. Общие требования. Единая система стандартов» и ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». Изучение специфики научно-исследовательской работы.	8	ПК-9
	Итого	8	
3 Основные стадии создания автоматизированных информационных систем	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к стадиям создания автоматизированных систем – ГОСТ 19.102-77 «ЕСПД Стадии разработки», ГОСТ 24.601-86 «Автоматизированные системы. Стадии создания», ГОСТ 24.602-86 «Автоматизированные системы управления. Со-став и содержание работ по стадиям создания» и ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». Рассмотрение вопроса разбиения проекта на этапы и определения ключевых параметров каждого из них. Рассмотрение методики построения IDEF.	8	ПК-20
	Итого	8	
4 Содержание работ на этапах создания автоматизированных информационных систем	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к оформлению документации по этапам разработки – ГОСТ 19.101-77 (СТ СЭВ 1626-79) «ЕСПД Виды программ и программных документов» и ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на	8	ПК-8

Согласована на портале № 14690

	автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем». Ознакомление с ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения без-опасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». Рассмотрение типового комплекта документации.		
	Итого	8	
5 Средства автоматизации проектирования автоматизированных информационных систем	Изучение государственного стандарта, содержащего требования, устанавливаемые российским законодательством к оформлению алгоритмов – ГОСТ 19.701-90 (ИСО 5807-85) «ЕСПД Схемы алгоритмов, программ данных и систем. Рассмотрение вопросов, связанных с построением и реализацией алгоритмов. Ознакомление с содержанием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения». Изучение оценочных уровней доверия и классификации автоматизированных систем.	8	ПК-12, ПК-13, ПК-8, ПК-9
	Итого	8	
Итого за семестр		36	
8 семестр			
6 Средства построения пользовательского интерфейса	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к параметрам пользовательского интерфейса – ГОСТ Р ИСО 9241-11-2010 «Эргономические требования к проведению офисных работ с использованием видеодисплейных терминалов (VDT). Руководство по обеспечению пригодности использования» и ГОСТ Р ИСО 9241-210-2012 «Эргономика взаимодействия человек-система. Человеко-ориентированное проектирование интерактивных систем». Определение ключевых	8	

Согласована на портале № 14690

	параметров для построения пользовательского интерфейса. Рассмотрение примеров документации.		
	Итого	8	
7 Средства разработки программно-информационного ядра информационных систем	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к построению модуля безопасности – ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации» и ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности». Ознакомление с содержанием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения». Изучение технологии работы ядра безопасности, мониторов обращений и прочих компонентов, позволяющих обеспечить безопасность создаваемого программного комплекса. Рассмотрение примеров документации. Рассмотрение типовых про-филей защиты автоматизированных систем.	8	ПК-12, ПК-13, ПК-8, ПК-9
	Итого	8	
8 Тестирование автоматизированных информационных систем	Изучение государственного стандарта, содержащего требования, устанавливаемые российским законодательством к тестированию автоматизированных систем – ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». Изучение видов испытаний и технологию их применения на практике. Рассмотрение примеров документации.	8	

Согласована на портале № 14690

	Итого	8	
9 Подготовка приложения к распространению	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к документации на создаваемую программную продукцию – ГОСТ 19.106-78 (СТ СЭВ 2088-80) «ЕСКД Требования к программным документам, выполненным печатным спосо-бом», РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов» и ГОСТ 19.501-78 «ЕСПД Формуляр. Требования к содержанию и оформлению». Рассмотрение примеров документации. Изучение принципов документального процесса сопровождения автоматизированной системы.	8	ПК-20, ПК-25
	Итого	8	
10 Ввод в эксплуатацию автоматизированных информационных систем	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к рабочей документации на продукцию – ГОСТ 19.504-79 «Руководство программиста. Требования к содержанию и оформлению» и ГОСТ 19.505-79 «Руководство оператора. Требования к содержанию и оформлению». Определение ключевых различий между руководствами программиста и администратора. Рассмотрение примеров документации.	8	ПК-20, ПК-25, ПК-28
	Итого	8	
11 Эксплуатация автоматизированных информационных систем	Обобщение результатов изучения предыдущих этапов. Рассмотрение автоматизированной системы на этапе эксплуатации, условий вывода из эксплуатации. Изучение требований к управлению информационной безопасностью и восстановлению систем после сбоя.	6	ПК-25, ПК-28
	Итого	6	
Итого за семестр		46	
Итого		82	

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 № 14690

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Предшествующие дисциплины															
1 Безопасность программного обеспечения		+	+	+				+	+	+	+				
2 Программно-аппаратные средства обеспечения информационной безопасности				+	+	+	+								
3 Распределённые автоматизированные информационные системы	+	+						+	+		+				
4 Системное администрирование			+	+	+	+	+			+	+				
5 Системное программирование			+	+	+	+	+			+	+				
6 Теоретические основы компьютерной безопасности	+	+		+	+			+	+						
7 Технологии и методы программирования	+	+		+	+	+	+	+							
8 Управление информационной безопасностью		+	+								+				

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

	Виды занятий	Формы контроля

Согласована на портале № 14690

Компетенции	Лекции	Практические занятия	Лабораторные работы	Контроль самостоятельной работы (курсовой проект / курсовая работа)	Самостоятельная работа	
ПК-8	+	+	+		+	Экзамен, Конспект самоподготовки, Компонент своевременности, Отчет по лабораторной работе, Отчет по курсовой работе, Отчет по практике
ПК-9	+	+	+	+	+	Экзамен, Конспект самоподготовки, Компонент своевременности, Отчет по лабораторной работе, Отчет по курсовой работе, Отчет по практике
ПК-12	+	+	+	+	+	Экзамен, Конспект самоподготовки, Компонент своевременности, Отчет по лабораторной работе, Отчет по курсовой работе, Отчет по практике

Согласована на портале № 14690

ПК-13	+	+	+	+	+	Экзамен, Конспект самоподготовки, Компонент своевременности, Отчет по лабораторной работе, Защита курсовых проектов (работ), Отчет по курсовой работе, Отчет по практике
ПК-20	+	+	+	+	+	Экзамен, Отчет по лабораторной работе, Отчет по курсовой работе, Отчет по практике
ПК-25	+	+	+		+	Экзамен, Отчет по лабораторной работе, Компонент своевременности, Отчет по курсовой работе
ПК-28	+	+			+	Экзамен, Отчет по лабораторной работе, Отчет по курсовой 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
7 семестр				
Презентации с использованием интерактивной доски с обсуждением			6	6
Выступление студента в роли обучающего			4	4
Case-study (метод конкретных ситуаций)	8			8
Работа в команде		4		4
Итого за семестр:	8	4	10	22
8 семестр				
Презентации с использованием слайдов с обсуждением			6	6
Презентации с			6	6

Согласована на портале № 14690

использованием интерактивной доски с обсуждением				
Работа в команде		8		8
Case-study (метод конкретных ситуаций)	2			2
Итого за семестр:	2	8	12	22
9 семестр				
Итого за семестр:	0	0	0	0
Итого	10	12	22	44

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
7 семестр			
5 Средства автоматизации проектирования автоматизированных информационных систем	Система управления проектами MS Project	8	ПК-12, ПК-13, ПК-8
	Система управления проектами Project Kaiser	8	
	Итого	16	
Итого за семестр		16	
8 семестр			
7 Средства разработки программно-информационного ядра информационных систем	Использование системы контроля версий исходного кода программ Tortoise SVN	4	ПК-20, ПК-9
	Использование системы контроля версий исходного кода программ Fossil	4	
	Использование системы контроля версий исходного кода программ GIT	8	
	Итого	16	
8 Тестирование автоматизированных информационных систем	Использование средства автоматизации тестирования программного обеспечения Bugzilla	4	ПК-25
	Использование средства автоматизации тестирования программного обеспечения Redmine	4	
	Использование средства автоматизации тестирования программного обеспечения Mantis Bagtracker	4	
	Итого	12	

Согласована на портале № 14690

Итого за семестр		28	
Итого		44	

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
7 семестр			
3 Основные стадии создания автоматизированных информационных систем	Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.	8	
	Итого	8	
4 Содержание работ на этапах создания автоматизированных информационных систем	Оценка общих критериев и определение класса защищенности автоматизированной системы.	10	
	Итого	10	
5 Средства автоматизации проектирования автоматизированных информационных систем	Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.	10	
	Итого	10	
Итого за семестр		28	
8 семестр			
6 Средства построения пользовательского интерфейса	Проектирование планируемой автоматизированной системы с учетом государственных стандартов.	2	ПК-8
	Итого	2	
7 Средства разработки программно-информационного ядра информационных систем	Анализ реализации модулей автоматизированных систем	4	ПК-12, ПК-13, ПК-9
	Итого	4	
9 Подготовка приложения к распространению	Анализ полноты проектной документации	4	ПК-20
	Итого	4	
Итого за семестр		10	

Согласована на портале № 14690

9 семестр			
12 Формирование заданий на курсовую работу. Составление технического задания на разработку автоматизированной системы.	Формирование заданий на курсовую работу. Составление технического задания на разработку автоматизированной системы.	2	
	Итого	2	
13 Проведение предпроектного исследования. Защита результатов научно-исследовательской работы.	Проведение предпроектного исследования. Защита результатов научно-исследовательской работы.	2	ПК-12, ПК-13
	Итого	2	
14 Реализация модуля безопасности системы.	Реализация модуля безопасности системы.	2	ПК-12, ПК-13, ПК-8, ПК-9
	Итого	2	
15 Анализ результатов выполнения этапов написания курсовой работы	Анализ результатов выполнения этапов написания курсовой работы	2	ПК-20, ПК-25, ПК-28
	Итого	2	
Итого за семестр		8	
Итого		46	

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
7 семестр				
1 Составление технического задания на автоматизированные информационные системы	Проработка лекционного материала	2		Конспект самоподготовки, Экзамен
	Итого	2		
2 Проектирование автоматизированных информационных систем	Проработка лекционного материала	2	ПК-9	Экзамен
	Итого	2		
3 Основные стадии создания автоматизированных информационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-20	Отчет по практике, Экзамен
	Проработка лекционного материала	2		
	Итого	6		
4 Содержание работ на этапах создания	Подготовка к практическим занятиям,	4	ПК-8	Отчет по практике, Экзамен

Согласована на портале № 14690

автоматизированных информационных систем	семинарам			
	Проработка лекционного материала	2		
	Итого	6		
5 Средства автоматизации проектирования автоматизированных информационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-12, ПК-13, ПК-8, ПК-9	Отчет по лабораторной работе, Отчет по практике, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	6		
	Итого	12		
Итого за семестр		28		
	Подготовка и сдача экзамена	36		Экзамен
8 семестр				
6 Средства построения пользовательского интерфейса	Проработка лекционного материала	4	ПК-20, ПК-9	Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	10		
	Итого	14		
7 Средства разработки программно-информационного ядра информационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-12, ПК-13, ПК-9, ПК-8, ПК-28	Отчет по лабораторной работе, Отчет по практике, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	10		
	Итого	16		
8 Тестирование автоматизированных информационных систем	Проработка лекционного материала	2	ПК-25	Компонент своевременности, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	10		
	Итого	12		
9 Подготовка приложения к распространению	Подготовка к практическим занятиям, семинарам	4	ПК-20, ПК-25	Отчет по практике, Экзамен
	Подготовка к практическим занятиям, семинарам	4		
	Проработка лекционного материала	2		
	Итого	10		
10 Ввод в эксплуатацию	Проработка лекционного	4	ПК-20,	Экзамен

Согласована на портале № 14690

автоматизированных информационных систем	материала		ПК-25, ПК-28	
	Итого	4		
11 Эксплуатация автоматизированных информационных систем	Проработка лекционного материала	4	ПК-25, ПК-28	Экзамен
	Итого	4		
Итого за семестр		60		
	Подготовка и сдача экзамена	36		Экзамен
9 семестр				
12 Формирование заданий на курсовую работу. Составление технического задания на разработку автоматизированной системы.	Подготовка к практическим занятиям, семинарам	2	ПК-13	Отчет по курсовой работе
	Выполнение курсового проекта (работы)	4		
	Итого	6		
13 Проведение предпроектного исследования. Защита результатов научно-исследовательской работы.	Подготовка к практическим занятиям, семинарам	4	ПК-12, ПК-13	Отчет по курсовой работе
	Итого	4		
14 Реализация модуля безопасности системы.	Подготовка к практическим занятиям, семинарам	2	ПК-12, ПК-13, ПК-8, ПК-9	Отчет по курсовой работе
	Выполнение курсового проекта (работы)	6		
	Итого	8		
15 Анализ результатов выполнения этапов написания курсовой работы	Подготовка к практическим занятиям, семинарам	2	ПК-20, ПК-25, ПК-28	Отчет по курсовой работе
	Итого	2		
Итого за семестр		20		
Итого		180		

10. Курсовая работа (проект)

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта) представлены таблице 10.1.

Таблица 10. 1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта)

Наименование аудиторных занятий	Трудоемкость, ч	Формируемые компетенции
9 семестр		

Согласована на портале № 14690

Формирование заданий на курсовую работу. Составление технического задания на разработку автоматизированной системы.	2	ПК-13, ПК-12, ПК-9, ПК-20
Проведение предпроектного исследования. Защита результатов научно-исследовательской работы.	2	
Реализация модуля безопасности системы.	2	
Анализ результатов выполнения этапов написания курсовой работы	2	
Итого за семестр	8	

10.1 Темы курсовых работ

Примерная тематика курсовых работ (проектов):

– Курсовая работа по дисциплине служит для закрепления практических умений и проверки эффективности владения приобретенными навыками. Курсовая работа включает в себя написание программного комплекса, содержащего N модулей из следующего перечня: модуль идентификации/аутентификации, модуль разграничения доступа, модуль журналирования, модуль управления, модуль шифрования. Помимо этого, в рамках курсовой работы от студента потребуется составить комплект документации к разработанному программному комплексу с учетом имеющихся ГОСТов по их оформлению.

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
8 семестр				
Компонент своевременности	5	5	5	15
Конспект самоподготовки	5	5	5	15
Отчет по лабораторной работе	10	10	10	30
Отчет по практике	3	4	3	10
Итого максимум за период	23	24	23	70
Экзамен				30
Нарастающим итогом	23	47	70	100
7 семестр				
Компонент своевременности	5	5	5	15
Конспект самоподготовки	5	5	5	15
Отчет по лабораторной работе		10	10	20
Отчет по практике	10	5	5	20

Согласована на портале № 14690

Итого максимум за период	20	25	25	70
Экзамен				30
Нарастающим итогом	20	45	70	100
9 семестр				
Защита курсовых проектов (работ)			30	30
Компонент своевременности	3	4	3	10
Отчет по курсовой работе	20	20	20	60
Итого максимум за период	23	24	53	100
Нарастающим итогом	23	47	100	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. Комплексная защита информации в корпоративных системах: учебное пособие для вузов / В. Ф. Шаньгин. - М.: ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 592 с. (30 экз.) (наличие в библиотеке ТУСУР - 20 экз.)

2. 2. Технология разработки программных систем: учебное пособие / И. Г. Боровской ; Том-ский государственный университет систем управления и радиоэлектроники (Томск). -

Согласована на портале № 14690

Электрон. текстовые дан. - Томск : [б. и.], 2012. - 260 с. [Электронный ресурс]. - http://edu.tusur.ru/training/publications/2436

12.2. Дополнительная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем : Монография / Р. В. Мещеряков, А. А. Шелупанов. - Томск : В-Спектр, 2007. - 349с. (26 экз.) (наличие в библиотеке ТУСУР - 26 экз.)
2. Стандарты информационной безопасности. Учебное пособие/ В.А. Галатенко. — М.: ИНТУИТ, 2006. — 264 с. Доступ из локальной сети каф. КИБЭВС. – Систем. Требования: DjvuReader. [Электронный ресурс]. - http://cesir/aos/yay/Library/Galatenko.djvu

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Методические указания к курсовой работе, практическим занятиям и самостоятельной работе. 2017. 6 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/yay/Metodichka_Po_Praktike.docx
2. Методические указания к лабораторным работам. 2015 г. 186 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/yay/Laboratorny_Praktikum_Riezas.pdf

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://portal.tusur.ru; http://www.lib.tusur.ru – образовательный портал университета;
2. http://protect.gost.ru; http://gostexpert.ru – база государственных стандартов.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Мультимедийная лекционная аудитория. Дисплейный класс с локальной вычислительной сетью. Интерактивная доска с лицензионным программным обеспечением и мультимедиа-проектор.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, расположенная по адресу 634034, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 407. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 - 2 штуки по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForse GT240 PCI-E. с широкополосным доступом в Internet, – 6 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP3; Visual Studio 2010; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

Согласована на портале № 14690

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. 407. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 - 2 штуки по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForse GT240 PCI-E. с широкополосным доступом в Internet, – 6 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP3; Visual Studio 2010; 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)

Согласована на портале № 14690

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;
- 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 № 14690

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

Разработка и эксплуатация защищенных автоматизированных систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **7, 8, 9**

Учебный план набора 2012 года

Разработчики:

- аспирант каф. КИБЭВС Якимук А. Ю.

Экзамен: 7, 8 семестр
Курсовая работа (проект): 9 семестр

Томск 2017

Согласована на портале № 14690

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-28	способностью управлять информационной безопасностью автоматизированной системы	Должен знать − основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; − автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; − методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; − содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; − методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; − основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); − основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; − основные информационные технологии, используемые в автоматизированных системах. ; Должен уметь - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем; -
ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
ПК-20	способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	
ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	
ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
ПК-8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	

Согласована на портале № 14690

		восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем. ; Должен владеть − профессиональной терминологией в области информационной безопасности; − навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; − методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; − навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; − навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных 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	Обладает фактическими	Обладает диапазоном	Контролирует работу,

Согласована на портале № 14690

уровень)	и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	практических умений, требуемых для развития творческих решений, абстрагирования проблем	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-28

ПК-28: способностью управлять информационной безопасностью автоматизированной системы.

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	основные информационные технологии, используемые в автоматизированных системах	администрировать подсистемы информационной безопасности автоматизированных систем	поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);

Согласована на портале № 14690

	проект / курсовая работа);	проект / курсовая работа);	
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Экзамен; • Курсовая работа (проект);

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)	• знает в полном объеме основные информационные технологии, используемые в автоматизированных системах;	• в полном объеме умеет администрировать подсистемы информационной безопасности автоматизированных систем;	• в полном объеме владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне основные информационные технологии, используемые в автоматизированных системах;	• на продвинутом уровне умеет администрировать подсистемы информационной безопасности автоматизированных систем;	• на продвинутом уровне владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне основные информационные технологии, используемые в автоматизированных системах;	• на базовом уровне умеет администрировать подсистемы информационной безопасности автоматизированных систем;	• на базовом уровне владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

2.2 Компетенция ПК-25

ПК-25: способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования

Согласована на портале № 14690

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	методы, способы и средства обеспечения отказоустойчивости автоматизированных систем	восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях	навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Экзамен; • Курсовая работа (проект);

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)	• знает в полном объеме методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;	• в полном объеме умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;	• в полном объеме владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств

Согласована на портале № 14690

			автоматизированных систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;	• на продвинутом уровне умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;	• на продвинутом уровне владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;	• на базовом уровне умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;	• на базовом уровне владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

2.3 Компетенция ПК-20

ПК-20: способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований 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	основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;

Согласована на портале № 14690

	• Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);

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)	• знает в полном объеме основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;	• в полном объеме умеет исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;	• в полном объеме владеет навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;	• на продвинутом уровне умеет исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;	• на продвинутом уровне владеет навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне основные криптографические методы, алгоритмы, протоколы,	• на базовом уровне умеет исследовать эффективность создаваемых средств автоматизации,	• на базовом уровне владеет навыками использования программно-аппаратных средств

Согласована на портале № 14690

	используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;	проводить технико-экономическое обоснование проектных решений;	обеспечения информационной безопасности автоматизированных систем;

2.4 Компетенция ПК-13

ПК-13: способностью участвовать в проектировании средств защиты информации автоматизированной системы.

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 меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)	разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен;	• Отчет по лабораторной работе; • Защита курсовых проектов (работ); • Конспект самоподготовки; • Отчет по курсовой работе;	• Отчет по лабораторной работе; • Защита курсовых проектов (работ); • Отчет по курсовой работе; • Отчет по практике; • Экзамен;

Согласована на портале № 14690

	• Курсовая работа (проект);	• Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Курсовая работа (проект);

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)	• знает в полном объеме основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);	• в полном объеме умеет разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;	• в полном объеме владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);	• на продвинутом уровне умеет разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;	• на продвинутом уровне владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);	• на базовом уровне умеет разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;	• на базовом уровне владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;

2.5 Компетенция ПК-12

ПК-12: способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы.

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	автоматизированную	определять	методами и

Согласована на портале № 14690

этапов	систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);

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)	• знает в полном объеме как оценить автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной	• в полном объеме умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	• в полном объеме владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных

Согласована на портале № 14690

	безопасности;		систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне как оценить автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;	• на продвинутом уровне умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	• на продвинутом уровне владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне как оценить автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;	• на базовом уровне умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	• на базовом уровне владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;

2.6 Компетенция ПК-9

ПК-9: способностью участвовать в разработке защищенных автоматизированных систем 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 13.

Таблица 13 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль

Согласована на портале № 14690

	работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 14.

Таблица 14 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• знает в полном объеме каковы методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;	• в полном объеме умеет разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;	• в полном объеме владеет навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне каковы методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;	• на продвинутом уровне умеет разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;	• на продвинутом уровне владеет навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне каковы методы, способы, средства, последовательность и содержание этапов разработки	• на базовом уровне умеет разрабатывать и исследовать аналитические и компьютерные модели автоматизированных	• на базовом уровне владеет навыками анализа и синтеза структурных и функциональных схем защищенных

Согласована на портале № 14690

	автоматизированных систем и подсистем безопасности автоматизированных систем;	систем и подсистем безопасности автоматизированных систем;	автоматизированных информационных систем;

2.7 Компетенция ПК-8

ПК-8: способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 15.

Таблица 15 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основные угрозы безопасности информации и принципы построения модели нарушителя в автоматизированных системах	разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен;	• Отчет по лабораторной работе; • Конспект самоподготовки; • Отчет по курсовой работе; • Отчет по практике; • Экзамен;	• Отчет по лабораторной работе; • Отчет по курсовой работе; • Отчет по практике; • Экзамен; • Курсовая работа (проект);

Согласована на портале № 14690

	• Курсовая работа (проект);	• Курсовая работа (проект);	

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 16.

Таблица 16 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• знает в полном объеме основные угрозы безопасности информации и принципы построения модели нарушителя в автоматизированных системах;	• в полном объеме умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	• в полном объеме владеет навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
Хорошо (базовый уровень)	• знает на продвинутом уровне основные угрозы безопасности информации и принципы построения модели нарушителя в автоматизированных системах;	• на продвинутом уровне умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	• на продвинутом уровне владеет навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне основные угрозы безопасности информации и принципы построения модели нарушителя в автоматизированных системах;	• на базовом уровне умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	• на базовом уровне владеет навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

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.

Согласована на портале № 14690

3.1 Вопросы на самоподготовку

– Оценка общих критериев и определение класса защищенности автоматизированной системы.

– Анализ средства защиты информации на предмет оценочных уровней доверия.

3.2 Экзаменационные вопросы

– Назначение ЕСПД. Классификация и обозначение стандартов ЕСПД

– Виды программ и программных документов. Стадии разработки.

– Виды программ и программных документов. Обозначения программ и программных документов.

– Виды программ и программных документов. Основные надписи. Общие требования к программной документации. Требования по оформлению и содержанию технического задания.

– Виды программ и программных документов. Программа и методика испытаний.

– Общие требования к программной документации. Текст и описание программы. Требования к содержанию и оформлению.

– Виды программ и программных документов. Общие требования к программной документации. Пояснительная записка. Требования к содержанию и оформлению.

– Руководство системного программиста. Руководство программиста. Руководство оператора. Руководство по техническому обслуживанию. Требования к содержанию и оформлению.

– Виды программ и программных документов. Описание языка. Требования к содержанию и оформлению.

3.3 Вопросы для подготовки к практическим занятиям, семинарам

– Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.

– Оценка общих критериев и определение класса защищенности автоматизированной системы.

– Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.

– Проектирование планируемой автоматизированной системы с учетом государственных стандартов.

– Анализ реализации модулей автоматизированных систем

– Анализ полноты проектной документации

3.4 Темы лабораторных работ

– Система управления проектами MS Project

– Система управления проектами Project Kaiser

– Использование системы контроля версий исходного кода программ Tortoise SVN

– Использование системы контроля версий исходного кода программ Fossil

– Использование системы контроля версий исходного кода программ GIT

– Использование средства автоматизации тестирования программного обеспечения Bugzilla

– Использование средства автоматизации тестирования программного обеспечения Redmine

– Использование средства автоматизации тестирования программного обеспечения Mantis Bagtracker

3.5 Темы курсовых проектов (работ)

– Создание автоматизированной системы в сфере образования

– Создание автоматизированной системы в банковской организации

Согласована на портале № 14690

– Создание автоматизированной системы в сфере здравоохранения
– Создание автоматизированной системы по продаже ж/д билетов
– Создание автоматизированной системы по продаже авиа-билетов

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. Комплексная защита информации в корпоративных системах: учебное пособие для вузов / В. Ф. Шаньгин. - М.: ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 592 с. (30 экз.) (наличие в библиотеке ТУСУР - 20 экз.)
2. 2. Технология разработки программных систем: учебное пособие / И. Г. Боровской ; Том-ский государственный университет систем управления и радиоэлектроники (Томск). - Электрон. текстовые дан. - Томск : [б. и.], 2012. - 260 с. [Электронный ресурс]. - http://edu.tusur.ru/training/publications/2436

4.2. Дополнительная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем : Монография / Р. В. Мещеряков, А. А. Шелупанов. - Томск : В-Спектр, 2007. - 349с. (26 экз.) (наличие в библиотеке ТУСУР - 26 экз.)
2. Стандарты информационной безопасности. Учебное пособие/ В.А. Галатенко. — М.: ИНТУИТ, 2006. — 264 с. Доступ из локальной сети каф. КИБЭВС. – Систем. Требования: DjvuReader. [Электронный ресурс]. - http://cesir/aos/yay/Library/Galatenko.djvu

4.3. Обязательные учебно-методические пособия

1. Методические указания к курсовой работе, практическим занятиям и самостоятельной работе. 2017. 6 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/yay/Metodichka_Po_Praktike.docx
2. Методические указания к лабораторным работам. 2015 г. 186 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/yay/Laboratorny_Praktikum_Riezas.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. http://portal.tusur.ru; http://www.lib.tusur.ru – образовательный портал университета;
2. http://protect.gost.ru; http://gostexpert.ru – база государственных стандартов.

Согласована на портале № 14690