МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

УТВЕРЖДАЮ
Директор Департамента образования
_____ П.Е. Троян
«___» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ КАЧЕСТВОМ И ЗАЩИТА ИНФОРМАЦИИ»

(наименование учебной дисциплины)

Уровень основной образовательной программы Бакалавриат
(бакалавриат, магистратура, специалитет)

Направление(я) подготовки (специальность) 27.03.02 "Управление качеством"
(номер.уровень, полное наименование направления подготовки (специальности))

Профиль(и) «Управление качеством в информационных системах»
(полное наименование профиля направления подготовки (специальности) из ПООП)

Форма обучения очная
(очная, очно-заочная (вечерняя), заочная)

Факультет ФИТ, факультет инновационных технологий
(сокращенное и полное наименование факультета)

Кафедра УИ, кафедра «Управление инновациями»
(сокращенное и полное наименование кафедры)

Курс 4 **Семестр** 7, 8

Учебный план набора 2016 года

Распределение рабочего времени:

№	Виды учебной работы	Семестр 1	Семестр 2	Семестр 3	Семестр 4	Семестр 5	Семестр 6	Семестр 7	Семестр 8	Всего	Единицы
1.	Лекции							18	16	34	часов
2.	Лабораторные работы							36	48	84	часов
3.	Практические занятия										часов
4.	Курсовой проект/работа (КРС) (аудиторная)										часов
5.	Всего аудиторных занятий (Сумма 1-4)							54	64	118	часов
6.	Из них в интерактивной форме							14	14	28	часов
7.	Самостоятельная работа студентов (СРС)							54	80	134	часов
8.	Всего (без экзамена) (Сумма 5,7)							108	144	252	часов
9.	Самост. работа на подготовку, сдачу экзамена								36	36	часов
10.	Общая трудоемкость (Сумма 8,9)							108	180	288	часов
	(в зачетных единицах)							3	5	8	ЗЕТ

Зачет 7 семестр **Диф. зачет** _____ семестр

Экзамен 8 семестр

Томск 2016

Согласована на портале № 8348

Рассмотрена и одобрена на заседании кафедры
протокол № 18 от « 24 » 11 2016 г.

Лист согласований

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 27.03.02 «Управление качеством» (бакалавриат), утвержденного Приказом Министерства образования и науки Российской Федерации № 92 от 09.02.2016 г.

Рассмотрена и утверждена на заседании кафедры « 24 » ноября 2016 г., протокол № 18.

Разработчик

Доцент кафедры УИ _____ П.Н. Дробот
(должность, кафедра) (подпись) (Ф.И.О.)

Ст. диспетчер ФИТ _____ Килина О.В.
(должность, кафедра) (подпись) (Ф.И.О.)

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

Декан ФИТ _____ Г.Н. Нариманова
(название факультета) (подпись) (Ф.И.О.)

Зав. профилирующей и выпускающей
кафедрой УИ _____ Г.Н. Нариманова
(название кафедры) (подпись) (Ф.И.О.)

Эксперты:

доцент каф. УИ, к.ф.-м.н. _____ М.Е. Антипин
(место работы, занимаемая должность) (подпись) (Ф.И.О.)

доцент каф. УИ _____ Е.П. Губин
(место работы, занимаемая должность) (подпись) (Ф.И.О.)

Согласована на портале № 8348

1. Цели и задачи дисциплины *«Информационные технологии в управлении качеством и защита информации»* - формирование у студентов целостного представления о роли современных информационных технологий в управлении качеством организаций и обеспечении безопасности информационных ресурсов предприятий.

Задачи курса:

- ознакомить обучающихся с рядом графических нотаций, применяемых для разработки альбомов бизнес-процессов организаций;
- сформировать у обучающихся навыки работы с рядом современных программных продуктов для визуализации, оценки и анализа эффективности деятельности организаций;
- ознакомить обучающихся с международными стандартами информационной безопасности, российской нормативно-правовой базой в области защиты информации;
- освоить базовые понятия и навыки по разработке политики безопасности компании;
- ознакомить студентов с методологией построения комплексной защиты информационной среды предприятия.

Место дисциплины в структуре ООП:

Дисциплина «Информационные технологии в управлении качеством и защита информации» представляет собой дисциплину базовой части профессионального цикла (Б1), изучается в 7, 8 семестрах в объеме 252 часов (7 ЗЕТ) и 36 часов (1 ЗЕТ) выделяется на проведение экзамена.

Изучение дисциплины базируется на материалах курсов «Информатика», «Информационные технологии», «Теоретические основы информатики», «Статистические методы в управлении качеством», «Информационное обеспечение, базы данных», «Средства и методы управления качеством».

Междисциплинарные связи при параллельном освоении дисциплин устанавливаются с курсами «Управление качеством программных систем», «Управление процессами», «Инструментальные средства моделирования». Поскольку дисциплина «Информационные технологии в управлении качеством и защита информации» изучается в последнем семестре, она является завершающим логически-обобщающим звеном цикла профессиональных дисциплин.

Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3).

В результате изучения дисциплины студент должен:

Знать: *основные информационные технологии в управлении качеством;*

Уметь: *использовать технологии проектирования моделей данных на различных уровнях: концептуальном, логическом и физическом;*

Владеть: *методами защиты информации.*

4. Объем дисциплины и виды учебной работы

Согласована на портале № 8348

Общая трудоемкость дисциплины составляет _____8_____ зачетные единицы.

Вид учебной работы	Всего часов	Семестры							
		1	2	3	4	5	6	7	8
Аудиторные занятия (всего)	118							54	64
В том числе:	-	-	-	-	-	-	-	-	-
Лекции	34							18	16
Лабораторные работы (ЛР)	84							36	48
Практические занятия (ПЗ)									
Семинары (С)									
Коллоквиумы (К)									
Курсовой проект/(работа) (аудиторная нагрузка)									
Другие виды аудиторной работы									
Самостоятельная работа (всего)	134							54	80
В том числе:			-	-	-				
Вид промежуточной аттестации - зачет	36	-							36
Общая трудоемкость час	288							108	180
Зачетные Единицы Трудоемкости	8							3	5

5. Содержание дисциплины

5.1. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции	Лаборат. занятия	Практич. занятия.	Курсовой П/Р (КРС)	Самост. работа студента	Всего час. (без экзам)	Формируемые компетенции (ОК, ПК)
7 семестр								
1.	Модели сложных процессов бизнеса	4	9	-	-	6	19	ОПК-3
2.	Модели и диаграммы графического представления в бизнес-моделировании	2	9	-	-	7	18	ОПК-3
3.	Способы организации источников информации, средств обработки, хранения и передачи данных	4	13	-	-	8	25	ОПК-3
4.	Информационный менеджмент	2	-	-	-	12	14	ОПК-3
5.	Информационные технологии управления проектами	4	3	-	-	8	15	ОПК-3
6.	Интегрированные системы управления предприятием (ИСУП)	2	-	-	-	11	13	ОПК-3
7.	Итоговое тестирование	-	2	-	-	2	4	ОПК-3
	Итого за 7 семестр:	**18**	**36**	**-**	**-**	**54**	**108**	
8 семестр								
8.	Введение. Основные понятия информационной безопасности	2	6	-	-	8	16	ОПК-3
9.	Политика безопасности	2	6	-	-	8	16	ОПК-3
10.	Аудит безопасности и оценка рисков	4	8	-	-	10	22	ОПК-3
11.	Проблемы информационной безопасности сетей	2	6	-	-	12	2	ОПК-3
12.	Идентификация, аутентификация и управление доступом	2	8	-	-	14	24	ОПК-3
13.	Защита электронного документооборота	2	6	-	-	14	22	ОПК-3
14.	Криптографическая защита информации	2	6	-	-	12	2	ОПК-3
15.	Итоговое тестирование	-	2	-	-	2	4	ОПК-3
16.	**Итого за 8 семестр:**	**16**	**48**	**-**	**-**	**80**	**108**	
	ИТОГО	**34**	**84**	**-**	**-**	**134**	**252**	

Согласована на портале № 8348

5.2. Содержание разделов дисциплины (по лекциям)

№ п/п	Наименование разделов	Содержание разделов	Трудоемкость (час.)	Формируемые компетенции (ОК, ПК)
1.	Модели сложных процессов бизнеса.	Понятия о бизнес-моделировании, реинжиниринге бизнеса. Системы управления бизнесом ERP, SCM, CRM, CSRP. Построение комплекса моделей предприятия. Case-средства и case-технологии.	4	ОПК-3
2.	Модели и диаграммы графического представления в бизнес-моделировании.	Технология HIPO. Диаграммы Варнье-Орра. Серия методологий IDEF. Функциональное моделирование. Этапы создания модели IDEF0. Модели «AS IS» и «TO BE». Критерии для определения завершения моделирования. Контекстные IDEFO-диаграммы и диаграммы декомпозиции. Виды связей в IDEF0-моделях.	2	ОПК-3
3.	Способы организации источников информации, средств обработки, хранения и передачи данных	Диаграммы потоков данных (DFD). Диаграммы потоков работ (IDEF3). Объектно-ориентированное моделирование UML. Диаграмма прецедентов. Диаграмма классов. Диаграмма деятельности. Диаграмма вариантов использования. Диаграмма состояний. Диаграмма активности. Диаграмма последовательностей. Диаграмма активности. Диаграмма компонентов. Диаграмма развертывания. Смешанные UML-модели.	4	ОПК-3
4.	Информационный менеджмент.	Понятие информационного менеджмента. Предметная область информационного менеджмента. Роль информационного менеджмента в управлении компанией. Задачи информационного менеджмента. Типовые подходы к решению задач информационного менеджмента. Стандарты ITIL и ITSM.	2	ОПК-3
5.	Информационные технологии управления проектами	Основные понятия управления проектами. Жизненный цикл проекта. Процессы управления проектами. Планирование работ по проекту. Планирование содержания. Определение последовательности работ. Оценка продолжительности работ. Разработка расписания. Представление расписания в виде сетевой диаграммы. Диаграмма контрольных точек. Диаграмма Ганта.	4	ОПК-3
6.	Интегрированные системы управления предприятием (ИСУП)	Основные элементы ИСУП. Функции ИСУП. Стандарты на системы управления. Процесс и этапы внедрения ИСУП.	2	ОПК-3
		Итого за 7 семестр:	**18**	
7.	Введение. Основные понятия информационной безопасности	Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.	2	ОПК-3
8.	Политика безопасности	Основные понятия политики безопасности. Структура политики безопасности организации. Разработка политики безопасности организации.	2	ОПК-3
9.	Аудит безопасности и оценка рисков	Виды и цели аудита. Основные этапы аудита безопасности. Роль оценки рисков в проведении аудита безопасности. Методики оценки рисков CRAMM, OCTAVE, RiskWatch, Microsoft.	4	ОПК-3
10.	Проблемы информационной безопасности сетей	Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP-сетей. Угрозы и уязвимости беспроводных сетей. Пути решения проблем защиты информации в сетях.	2	ОПК-3
11.	Идентификация, аутентификация и управление доступом	Методы аутентификации, использующие пароли. Строгая аутентификация. Биометрическая аутентификация пользователя. Управление идентификацией и доступом.	2	ОПК-3
12.	Защита электронного	Концепция электронного документооборота.	2	ОПК-3

Согласована на портале № 8348

	докум е нтооборота	Особенности защиты электронного документооборота. Защита баз данных и корпоративной почты.		
13.	Криптографическая защита информации	Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы. Функция хэширования. Электронная цифровая подпись.	2	ОПК-3
		Итого за 8 семестр:	**16**	
		ИТОГО	**34**	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины из табл.5.1, для которых необходимо изучение обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Предшествующие дисциплины															
1.	Информатика	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2.	Информационные технологии	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4.	Теоретические основы информатики		+	+	+	+	+		+		+				
5.	Информационное обеспечение, базы данных			+		+			+	+			+	+	+
6.	Статистические методы в управлении качеством		+	+	+		+				+	+	+		
7.	Средства и методы управления качеством	+			+	+	+		+	+	+		+		
Дисциплины, изучаемые параллельно															
1.	Управление процессами				+		+							+	
2.	Управление качеством программных систем				+		+			+	+				
3	Инструментальные средства моделирования	+	+	+					+		+		+		

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

Перечень компетенций	Виды занятий					Формы контроля
	Л	Лаб	Пр.	КР/КП	СРС	
ОПК-3	+	+			+	Оценка подготовки и решения кейсов, оценка участия в презентации, оценка разработки политики безопасности

Л – лекция, Пр – практические и семинарские занятия, Лаб – лабораторные работы, КР/КП – курсовая работа/проект, СРС – самостоятельная работа студента

6. Методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах

Методы \ Формы	Лекции (час)	Лабораторные занятия (час)	Практические/семинарские Занятия (час)	Всего
IT-методы		2		2
Работа в команде	2	2		4
Case-study (метод конкретных ситуаций)	2	4		6
Метод круглого стола	2	4		6
Деловая игра		1		1
Работа в малых группах		3		3
Метод презентации	2	4		6

Согласована на портале № 8348

Итого интерактивных занятий	8	20		28

7. Лабораторный практикум

№ п/п	№ раздела дисциплины из табл. 5.1	Тематика практических занятий (семинаров)	Трудо-емкость (час.)	Компетенции ОК, ПК
7 семестр				
1.	1,2	Моделирование бизнес-процесса предприятия с использованием методологии IDEF0	4	ОПК-3
2.	1,2	Применение нотации IDEF0 при проектировании бизнес-процессов	4	ОПК-3
3	3	Построение диаграммы деятельности в нотации UML	4	ОПК-3
4.	3	Построение диаграммы вариантов использования в нотации UML	4	ОПК-3
5.	3	Построение диаграммы последовательностей в нотации UML	4	ОПК-3
6	1,2	Изучение интерфейса программы TIBCO BUSINESS STUDIO и нотации BPMN	4	ОПК-3
7	1,2	Моделирование бизнес-процессов предприятия в нотации BPMN	4	ОПК-3
8	1,2,3,5	Разработка комплекса моделей бизнес-процессов предприятия	6	ОПК-3
9	7	Контроль знаний за семестр по пройденному материалу	2	ОПК-3
		Итого: за 7 семестр	**36**	
8 семестр				
10	8	Изучение Международных и отечественных стандартов в области информационной безопасности	6	ОПК-3
11	10	Изучение существующих методик оценки рисков	6	ОПК-3
12	10	Разработка плана аудита информационной безопасности	8	ОПК-3
13	11	Анализ внутренней сети	6	ОПК-3
14	12	Выявление уязвимостей в компьютерных системах и построение локальной политики паролей	8	ОПК-3
15	12	Исследование надежности системы идентификации пользователя	6	ОПК-3
16	13	Средства защиты и удостоверения подлинности электронных документов на примере пакета Open Office	6	ОПК-3
17	14	Шифрование текста как метод защиты информации.	2	ОПК-3
18	14	Исследование электронной цифровой подписи на основе алгоритма RSA	6	ОПК-3
19	15	Контроль знаний за семестр по пройденному материалу	6	ОПК-3
		Итого: за 8семестр	**48**	
		ИТОГО	**84**	

8. Практические занятия (семинары) не предусмотрены учебным планом.

9. Самостоятельная работа

№ п/п	№ раздела дисциплины из табл. 5.1	Тематика самостоятельной работы *(детализация)*	Трудо-емкость (час.)	Компетенции ОК	Контроль выполнения работы (Опрос, тест, дом.задание, и т.д)
1.	1	Подготовка к опросу на лекции Подготовка к защите лабораторной работы	6	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Решение кейсов
2	2	Ответы на контрольные вопросы Работа с электронными ресурсами Подготовка кейсов по заданной теме	7	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Проверка карты процесса Решение кейсов
3	3	Подготовка к опросу на лекции	8	ОПК-3	Опрос на лекции Защита

Согласована на портале № 8348

		Подготовка к защите лабораторной работы. Ответы на контрольные вопросы Работа с электронными ресурсами Подготовка презентации по теме Составление карты процесса			лабораторной работы. Контрольные вопросы Оценка презентации Проверка карты процесса
4	4	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Подготовка к круглому столу Работа с электронными ресурсами Анализ деятельности предприятия Составление карты процесса Подготовка кейсов по заданной теме	12	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Оценка ответов на круглом столе Проверка карты процесса Решение кейсов
5	5	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Анализ деятельности предприятия Работа с электронными ресурсами Подготовка презентации по теме	8	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Оценка презентации
6	6	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Анализ деятельности предприятия Работа в команде по разработке комплекса моделей бизнес-процессов предприятия Анализ статей по теме Работа с электронными ресурсами	11	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Командная защита комплекса моделей бизнес-процессов предприятия Участие в обсуждение
7	7	Подготовка к тестированию	2	ОПК-3	Тестирование
8	8	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Подготовка доклада по теме Работа с электронными ресурсами	8	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Оценка за доклад
9	9	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Работа с электронными ресурсами Подготовка кейсов по теме	8	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Оценка подготовленности к лабораторной работе Решение кейсов
10	10	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Разработка политики безопасности Работа с электронными ресурсами Подготовка презентации по теме	10	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Проверка политики безопасности Оценка презентации
11	11	Подготовка к опросу на лекции Подготовка к защите	12	ОПК-3	Опрос на лекции Защита лабораторной работы

Согласована на портале № 8348

		лабораторной работы Ответы на контрольные вопросы Разработка политики безопасности Работа с электронными ресурсами Подготовка кейсов по теме			Контрольные вопросы Проверка политики безопасности Решение кейсов
12	12	Подготовка к опросу на лекции. Подготовка к защите лабораторной работы Ответы на контрольные вопросы Разработка политики безопасности Работа с электронными ресурсами Подготовка презентации по теме	14	ОПК-3	Защита лабораторной работы Контрольные вопросы Проверка политики безопасности Оценка презентации
13	13	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Разработка политики безопасности Работа с электронными ресурсами	14	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы
14	14	Подготовка к опросу на лекции Подготовка к защите лабораторной работы Ответы на контрольные вопросы Разработка политики безопасности Подготовка кейсов по теме	12	ОПК-3	Опрос на лекции Защита лабораторной работы Контрольные вопросы Проверка политики безопасности Решение кейсов
15	15	Подготовка к тестированию	2	ОПК-3	Тестирование
16	16	Подготовка и сдача экзамена	36	ОПК-3	Экзамен
		ИТОГО	**134**		

Темы контрольных работ:

1. Основные понятия управления проектами. Жизненный цикл проекта.
2. Концепция электронного документооборота. Особенности защиты электронного документооборота.

10. Примерная тематика курсовых проектов (работ) курсовые работы и проекты не предусмотрены учебным планом.

11. Рейтинговая система для оценки успеваемости студентов

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 1 КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
7 семестр				
Посещение занятий	4	4	4	12
Выполнение и защита лабораторных работ	3	3	4	10

Согласована на портале № 8348

Выполнение контрольных заданий, самостоятельных работ	2	2	3	7
Компонент своевременности	2	2	2	6
Итого за 7 семестр:	11	11	13	35
8 семестр				
Посещение занятий	4	4	4	12
Выполнение и защита лабораторных работ	3	3	4	10
Выполнение контрольных заданий, самостоятельных работ	2	2	3	7
Компонент своевременности	2	2	2	6
Итого за 8 семестр:	11	11	13	35
Итого максимум за период:	22	22	26	70
Сдача экзамена (максимум)				30
Нарастающим итогом	22	44	70	100

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

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

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

12.Учебно-методическое и информационное обеспечение дисциплины:

12.1 Основная литература

1. Черников Б.В. Информационные технологии управления : учебник для вузов / Б. В. Черников. - 2-е изд., перераб. и доп. - М. : Норма, 2013 ; М. : ИНФРА-М, 2013. - 368 с. (5 экз. в библ. ТУСУР);
2. Елиферов В.Г., Репин В.В. Бизнес-процессы: регламентация и управление: учебное пособие / В. Г. Елиферов, В. В. Репин; Институт экономики и финансов "Синергия". - М.: ИНФРА- М, 2012. - 319 с. (5 экз. в библ. ТУСУР);
3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие для вузов / В. Ф. Шаньгин. - М.: ФОРУМ, 2012; М. : ИНФРА-М, 2012. - 592 с. (30 экз. в библ. ТУСУР).

Согласована на портале № 8348

12.2 Дополнительная литература

1. Макарова Т.В. Основы информационных технологий в рекламе [Текст] : учебное пособие для вузов / Т. В. Макарова, О. Н. Ткаченко, О. Г. Капустина ; ред. Jl. М. Дмитриева. - М. : ЮНИТИ-ДАНА, 2011. - 272 с. (15 экз. в библ. ТУСУР);

2. Советов Борис Яковлевич. Представление знаний в информационных системах [Текст] : учебник для вузов / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. - М. : Академия, 2011. - 144 с. (15 экз. в библ. ТУСУР);

3. Гвоздева, Татьяна Вадимовна. Проектирование информационных систем [Текст] : учебное пособие для вузов / Т. В. Гвоздева, Б. А. Баллод. - Ростов н/Д : Феникс, 2009. - 512 с. (15 экз. в библ. ТУ СУР);

4. Кузовкин Александр Васильевич. Управление данными [Текст] : учебник для вузов / А. В. Кузовкин, А. А. Цыганов, Б. А. Щукин. - М.: Академия, 2010. - 256 с. (25 экз. в библ. ТУСУР);

5. Информационные системы и технологии в экономике и управлении : Учебное пособие для вузов / Санкт-Петербургский государственный университет экономики и финансов ; ред. : В. В. Трофимов. - 2-е изд., перераб. и доп. - М. : Высшее образование, 2007. - 480 с. (20 экз. в библ. ТУСУР);

6. Черников Борис Васильевич. Управление качеством программного обеспечения [Текст] : учебник для вузов / Б. В. Черников. - М. : ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 240 с. (10 экз. в библ. ТУСУР);

7. Куприянов А.И. Основы защиты информации. - М.: Academia, 2006. - 253 с. (50 экз. в библ. ТУСУР);

8. Основы защиты информации: учеб. пособие в 3 ч. Сост. А.А. Шелупанов [и др.]. - Томск: В-Спектр, 2007. - 150 с. (81 экземпляр в библиотеке ТУСУР).

12.3. Учебно-методические пособия и программное обеспечение:

1. Годенова Е.Г. Методические рекомендации к лабораторным работам по дисциплине «Информационные технологии в управлении качеством и защита информации». - ТУСУР: Кафедра «Управление инновациями», 2013 г. - 191 с. Режим доступа URL: http://edu.tusur.ru/training/publications/2917;

2. Годенова Е.Г. Методические рекомендации к организации самостоятельной работе студентов по дисциплине «Информационные технологии в управлении качеством и защита информации». - ТУСУР: Кафедра «Управление инновациями», 2013 г. - 34 с. http://edu.tusur.ru/training/publications/2931.

12.4 Базы данных, информационно-справочные и поисковые системы не предусмотрены

1. Поисковая система Google. [Электронный ресурс] - URL: http://google.com (Дата обращения 18.06.2012 г.);

2. Википедия свободная энциклопедия. [Электронный ресурс] - URL: http://ru.wikipedia.org/wiki. (Дата обращения 18.06.2012 г.)

3. Информационный портал по компьютерной безопасности [Электронный ресурс]. URL: http://www.securitvlab.ru. (дата обращения 11.06.2012 г.)

4. OpenPGP в России. [Электронный ресурс] - URL: http://www.pgpru.com. (Дата обращения 18.06.2012 г.);

5. Microsoft. Центр безопасности. [Электронный ресурс] - URL: http://www.microsoft.com/ru-

Согласована на портале № 8348

ru/securitv/default.aspx. (Дата обращения 18.06.2012 г.);
6. Business Studio. Система бизнес-моделирования. Примеры моделей бизнес процессов. [Электронный ресурс]. Режим доступа: http://www.businessstudio.ru/ (Дата обращения 14.01.2013г.);
7. Стандарты информационной безопасности. [Электронный ресурс] - URL: http://www.leta.ru/librarv/standards/ (Дата обращения 18.06.2012 г.).

13. Материально-техническое обеспечение дисциплины: для организации занятий требуется:
Аппаратное обеспечение (в расчете одно рабочее место на одного или на двух студентов):

1) Компьютер;
2) Мышь;
3) Клавиатура;
4) Монитор;
5) Широкополосный доступ к сети Интернет.

Программное обеспечение (в расчете на один компьютер):

1) Операционная система версии не ниже Windows XP;
2) Пакет программ Microsoft Office или Open Office;
3) Программный продукт Ramus Educational;
4) Программный продукт Tibco Business Studio;
5) Программный продукт Software Ideas Modeler;
6) Программный продукт Microsoft Security Assessment (MSAT);
7) Системная утилита 10-Strike LanState Pro;
8) Программный продукт Microsoft Baseline Security analyzer;
9) Криптографическая программа GnuPG;
10) Программа для создания цифровых сертификатов Abylon Selfcert.

Согласована на портале № 8348

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

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ КАЧЕСТВОМ И ЗАЩИТА ИНФОРМАЦИИ»

Уровень основной образовательной программы: **Бакалавриат**
Направление подготовки (специальность): **27.03.02 "Управление качеством"**
Профиль: **Управление качеством в информационных системах**
Форма обучения: **очная**
Факультет: **ФИТ, Факультет инновационных технологий**
Кафедра: **УИ, Кафедра управления инновациями**
Курс: **4**
Семестр: **7, 8**

Учебный план набора 2016 года

Разработчики:

- к.ф.-м.н., доцент, каф. УИ Дробот П. Н.
- ст. диспетчер ФИТ Килина О.В.

Зачет: 7 семестр
Экзамен: 8 семестр

Томск 2016

Согласована на портале № 8348

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 компетенции
ОПК-3	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Должен знать современные информационно-коммуникационные технологии; Должен уметь применять методы поиска и анализа информации с учетом требований информационной безопасности; Должен владеть библиотечно-библиографическими знаниями, необходимыми для их научной и учебной работы;

2. Реализация компетенций

2.1 Компетенция ОПК-3

ОПК-3: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных 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 2.

Таблица 2– Этапы формирования компетенции и используемые средства оценивания

1. Состав	Знать	Уметь	Владеть
Содержание этапов	Знает современные информационно-коммуникационные технологии	Умеет применять методы поиска и анализа информации с учетом требований информационной безопасности.	Владеет библиотечно-библиографическими знаниями, необходимыми для их научной и учебной работы

Согласована на портале № 8348

Виды занятий	Лекции;	Лабораторные занятия; Самостоятельная работа студентов	Выполнение домашнего задания; Самостоятельная работа студентов
Используемые средства оценивания	Контрольные вопросы	Отчеты по лабораторным работам;	Проверка реферата

Общие характеристики показателей и критериев оценивания компетенции на всех этапах приведены в таблице 3.

Таблица 3 – Общие характеристики показателей и критериев оценивания компетенции 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

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

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	анализирует связи между различными инфокоммуникационными технологиями; представляет способы и результаты использования различных методов	свободно применяет информационно-коммуникационные технологии в незнакомых ситуациях; умеет выражать и аргументированно	способен руководить междисциплинарной командой; свободно владеет разными способами представления библиографической

Согласована на портале № 8348

	поиска; обосновывает выбор программных средств для решения задачи	доказывать положения теории информации	информации
Хорошо (базовый уровень)	понимает связи между различными инфокоммуникационнными технологиями; имеет представление о методах поиска информации; аргументирует выбор программных средств для решения задачи ;	самостоятельно выбирает методы анализа и поиска информации; применяет информационно-коммуникационные технологии в незнакомых ситуациях; умеет сформулировать требования информационной безопасности	критически осмысливает результаты библиографического поиска; владеет разными способами представления результатов поиска
Удовлетворительно (пороговый уровень)	дает определения основных информационно-коммуникационных технологий*;* воспроизводит основные идеи поиска информации; знает основные информационные технологии для управления качеством и умеет их применять на практике	умеет работать со справочной литературой; использует предложенные программные средства; умеет представлять результаты своей работы	владеет библиотечно-библиографической терминологией; способен корректно представить результаты информационного поиска

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 № 8348

3.1 Тематика заданий на домашнюю работу.

- Анализ применения руководящих документов по системе качества проектирования научно-технической продукции с применением информационно-коммуникационных технологий
- Концепция построения базы знаний системы контроля качества научно-технической продукции с учётом защиты информации
- Этапы проектирования научно-технической продукции с применением современных информационно
- Программное обеспечение, используемое при проектировании научно-технической продукции и защите информации -коммуникационных технологий
- Анализ возможных каналов утечки научно-технической информации при проектировании и влияние её на качество продукции
- Методы и способы защиты научно-технической информации при проектировании продукции с применением информационно-коммуникационных технологий

3.2 Темы лабораторных занятий

1. Изучение Международных и отечественных стандартов в области информационной безопасности
2. Изучение существующих методик оценки рисков
3. Разработка плана аудита информационной безопасности
4. Анализ внутренней сети
5. Выявление уязвимостей в компьютерных системах и построение локальной политики паролей
6. Исследование надежности системы идентификации пользователя
7. Средства защиты и удостоверения подлинности электронных документов на примере пакета Open Office
8. Шифрование текста как метод защиты информации.
9. Исследование электронной цифровой подписи на основе алгоритма RSA
10. Моделирование бизнес-процесса предприятия с использованием методологии IDEF0
11. Применение нотации IDEF0 при проектировании бизнес- процессов
12. Построение диаграммы деятельности в нотации UML
13. Построение диаграммы вариантов использования в нотации UML
14. Построение диаграммы последовательностей в нотации UML
15. Изучение интерфейса программы TIBCO BUSINESS STUDIO и нотации BPMN
16. Моделирование бизнес-процессов предприятия в нотации BPMN
17. Разработка комплекса моделей бизнес-процессов предприятия

3.3 Вопросы к зачету

1. Понятия о бизнес-моделировании, реинжиниринге бизнеса.
2. Системы управления бизнесом ERP, SCM, CRM, CSRP.
3. Построение комплекса моделей предприятия. Case-средства и case-технологии.
4. Технология HIPO. Диаграммы Варнье-Орра. Серия методологий IDEF.
5. Функциональное моделирование. Этапы создания модели IDEF0.
6. Модели «AS IS» и «TO BE». Критерии для определения завершения моделирования. Контекстные IDEFO-диаграммы и диаграммы декомпозиции.
7. Виды связей в IDEF0- моделях.

Согласована на портале № 8348

8. Диаграммы потоков данных (DFD).
9. Диаграммы потоков работ (IDEF3).
10. Объектно-ориентированное моделирование UML. Диаграмма прецедентов. Диаграмма классов. Диаграмма деятельности.
11. Диаграмма вариантов использования.
12. Диаграмма состояний. Диаграмма активности. Диаграмма последовательностей.
13. Диаграмма активности. Диаграмма компонентов.
14. Диаграмма развертывания. Смешанные UML-модели.
15. Понятие информационного менеджмента.
16. Предметная область информационного менеджмента.
17. Роль информационного менеджмента в управлении компанией.
18. Задачи информационного менеджмента.
19. Типовые подходы к решению задач информационного менеджмента.
20. Стандарты ITIL и ITSM.
21. Основные понятия управления проектами. Жизненный цикл проекта.
22. Процессы управления проектами.
23. Планирование работ по проекту.
24. Планирование содержания. Определение последовательности работ.
25. Оценка продолжительности работ. Разработка расписания.
26. Представление расписания в виде сетевой диаграммы.
27. Диаграмма контрольных точек. Диаграмма Ганта.
28. Основные элементы ИСУП.
29. Функции ИСУП. Стандарты на системы управления.
30. Процесс и этапы внедрения ИСУП.

3.4 Вопросы к экзамену

1. Основные понятия защиты информации и информационной безопасности.
2. Анализ угроз информационной безопасности.
3. Основные понятия политики безопасности.
4. Структура политики безопасности организации.
5. Разработка политики безопасности организации.
6. Виды и цели аудита.
7. Основные этапы аудита безопасности.
8. Роль оценки рисков в проведении аудита безопасности.
9. Методики оценки рисков CRAMM, OCTAVE, RiskWatch, Microsoft.
10. Использование сети Интернет.
11. Модель ISO/OSI и стек протоколов TCP/IP.
12. Проблемы безопасности IP-сетей.
13. Угрозы и уязвимости беспроводных сетей.
14. Пути решения проблем защиты информации в сетях.
15. Методы аутентификации, использующие пароли.
16. Строгая аутентификация.
17. Биометрическая аутентификация пользователя.
18. Управление идентификацией и доступом.
19. Концепция электронного документооборота.
20. Особенности защиты электронного документооборота.
21. Защита баз данных и корпоративной почты.
22. Основные понятия криптографической защиты информации.
23. Симметричные и асимметричные криптосистемы.
24. Функция хэширования.
25. Электронная цифровая подпись.

Согласована на портале № 8348

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. Черников Б.В. Информационные технологии управления : учебник для вузов / Б. В. Черников. - 2-е изд., перераб. и доп. - М. : Норма, 2013 ; М. : ИНФРА-М, 2013. -368 с. (5 экз. в библ. ТУСУР);

2. Елиферов В.Г., Репин В.В. Бизнес-процессы: регламентация и управление: учебное пособие / В. Г. Елиферов, В. В. Репин; Институт экономики и финансов "Синергия". - М.: ИНФРА- М, 2012. - 319 с. (5 экз. в библ. ТУСУР);

3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие для вузов / В. Ф. Шаньгин. - М.: ФОРУМ, 2012; М. : ИНФРА-М, 2012. - 592 с. (30 экз. в библ. ТУСУР).

4.2. Дополнительная литература

1. Макарова Т.В. Основы информационных технологий в рекламе [Текст] : учебное пособие для вузов / Т. В. Макарова, О. Н. Ткаченко, О. Г. Капустина ; ред. Jl. М. Дмитриева. - М. : ЮНИТИ-ДАНА, 2011. - 272 с. (15 экз. в библ. ТУСУР);

2. Советов Борис Яковлевич. Представление знаний в информационных системах [Текст] : учебник для вузов / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. - М. : Академия, 2011. - 144 с. (15 экз. в библ. ТУСУР);

3. Гвоздева, Татьяна Вадимовна. Проектирование информационных систем [Текст] : учебное пособие для вузов / Т. В. Гвоздева, Б. А. Баллод. - Ростов н/Д : Феникс, 2009. - 512 с. (15 экз. в библ. ТУ СУР);

4. Кузовкин Александр Васильевич. Управление данными [Текст] : учебник для вузов / А. В. Кузовкин, А. А. Цыганов, Б. А. Щукин. - М.: Академия, 2010. - 256 с. (25 экз. в библ. ТУСУР);

5. Информационные системы и технологии в экономике и управлении : Учебное пособие для вузов / Санкт-Петербургский государственный университет экономики и финансов ; ред. : В. В. Трофимов. - 2-е изд., перераб. и доп. - М. : Высшее образование, 2007. - 480 с. (20 экз. в библ. ТУСУР);

6. Черников Борис Васильевич. Управление качеством программного обеспечения [Текст] : учебник для вузов / Б. В. Черников. - М. : ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 240 с. (10 экз. в библ. ТУСУР);

7. Куприянов А.И. Основы защиты информации. - М.: Academia, 2006. - 253 с. (50 экз. в библ. ТУСУР);

8. Основы защиты информации: учеб. пособие в 3 ч. Сост. А.А. Шелупанов [и др.]. - Томск: В-Спектр, 2007. - 150 с. (81 экземпляр в библиотеке ТУСУР).

4.3. Учебно-методическое пособие и программное обеспечение

1. Годенова Е.Г. Методические рекомендации к лабораторным работам по дисциплине «Информационные технологии в управлении качеством и защита информации». - ТУСУР: Кафедра «Управление инновациями», 2013 г. - 191 с. Режим доступа URL: http://edu.tusur.ru/training/publications/2917;

2. Годенова Е.Г. Методические рекомендации к организации самостоятельной работе

Согласована на портале № 8348

студентов по дисциплине «Информационные технологии в управлении качеством и защита информации». - ТУСУР: Кафедра «Управление инновациями», 2013 г. - 34 с. http://edu.tusur.ru/training/publications/2931.

4.4. Базы данных, информационно справочные и поисковые системы

1. Поисковая система Google. [Электронный ресурс] - URL: http://google.com (Дата обращения 18.06.2012 г.);
2. Википедия свободная энциклопедия. [Электронный ресурс] - URL: http://ru.wikipedia.org/wiki. (Дата обращения 18.06.2012 г.)
3. Информационный портал по компьютерной безопасности [Электронный ресурс]. URL: http://www.securitvlab.ru. (дата обращения 11.06.2012 г.)
4. OpenPGP в России. [Электронный ресурс] - URL: http://www.pgpru.com. (Дата обращения 18.06.2012 г.);
5. Microsoft. Центр безопасности. [Электронный ресурс] - URL: http://www.microsoft.com/ru-ru/securitv/default.aspx. (Дата обращения 18.06.2012 г.);
6. Business Studio. Система бизнес-моделирования. Примеры моделей бизнес процессов. [Электронный ресурс]. Режим доступа: http://www.businessstudio.ru/ (Дата обращения 14.01.2013г.);
7. Стандарты информационной безопасности. [Электронный ресурс] - URL: http://www.leta.ru/librarv/standards/ (Дата обращения 18.06.2012 г.).

4.5 Материально-техническое обеспечение дисциплины: для организации занятий требуется:

Аппаратное обеспечение (в расчете одно рабочее место на одного или на двух студентов):

1) Компьютер;
2) Мышь;
3) Клавиатура;
4) Монитор;
5) Широкополосный доступ к сети Интернет.

Программное обеспечение (в расчете на один компьютер):

1) Операционная система версии не ниже Windows XP;
2) Пакет программ Microsoft Office или Open Office;
3) Программный продукт Ramus Educational;
4) Программный продукт Tibco Business Studio;
5) Программный продукт Software Ideas Modeler;
6) Программный продукт Microsoft Security Assessment (MSAT);
7) Системная утилита 10-Strike LanState Pro;
8) Программный продукт Microsoft Baseline Security analyzer;
9) Криптографическая программа GnuPG;
10) Программа для создания цифровых сертификатов Abylon Selfcert.

Согласована на портале № 8348