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

Безопасность информационных и аналитических систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	16	16	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	60	60	часов
5	Из них в интерактивной форме	16	16	часов
6	Самостоятельная работа	48	48	часов
7	Всего (без экзамена)	108	108	часов
8	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 10 семестр

Томск 2017

Согласована на портале № 16895

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 9 » 6 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.04 Информационно-аналитические системы безопасности, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

Ассистент каф. КИБЭВС _____ Н. В. Малахов

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

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

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф.
БИС _____ Р. В. Мещеряков

Эксперт:

Доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 16895

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Раскрыть технологии интеллектуального анализа больших информационных массивов с помощью информационно-аналитических систем.

Дисциплина должна способствовать умению использования информационно-аналитических систем для интеллектуального анализа больших информационных массивов, умению самостоятельно повышать свои знания в области интеллектуального анализа данных, умению применять методы и средства обеспечения информационной безопасности специальных ИАС

1.2. Задачи дисциплины

– Задача дисциплины состоит в том, чтобы ознакомить студентов с современными методами и средствами обеспечения информационной безопасности специальных ИАС, с методами оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность информационных и аналитических систем» (Б1.Б.29) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Базы данных и экспертные системы, Безопасность программного обеспечения, Безопасность систем баз данных, Информатика, Информационные технологии, Криптографические методы защиты информации, Математические методы проектирования финансовых систем (групповое проектное обучение - ГПО 1), Методология и организация информационно-аналитической деятельности, Моделирование информационно-аналитических систем, Основы информационной безопасности, Прикладная криптография, Принципы построения, проектирования и эксплуатации информационно-аналитических систем, Проектирование информационно-аналитических систем (групповое проектное обучение - ГПО 2), Проектирование подсистемы безопасности информационно-аналитических систем в финансовой сфере (групповое проектное обучение - ГПО 3), Распределенные информационно-аналитические системы, Системное программирование, Специальные технологии баз данных и информационных систем, Теоретические основы компьютерной безопасности, Техническая защита информации, Формализованные модели и методы решения аналитических задач.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-7 способностью применять методы и средства обеспечения информационной безопасности специальных ИАС;

– ПК-10 способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;

– ПК-13 способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;

В результате изучения дисциплины студент должен:

– **знать** методы и средства обеспечения информационной безопасности специальных ИАС; технологии, инструментальные средства, средства обеспечения информационной безопасности создаваемых специальных ИАС; методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.

– **уметь** применять методы и средства обеспечения информационной безопасности специальных ИАС; осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС; оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности.

– **владеть** методами и средствами обеспечения информационной безопасности специальных ИАС; методами оценки эффективности специальных ИАС, в том числе средств обеспечения

Согласована на портале № 16895

их информационной безопасности.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Аудиторные занятия (всего)	60	60
Лекции	28	28
Практические занятия	16	16
Лабораторные работы	16	16
Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	48	48
Оформление отчетов по лабораторным работам	16	16
Проработка лекционного материала	8	8
Подготовка к практическим занятиям, семинарам	24	24
Всего (без экзамена)	108	108
Общая трудоемкость ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
10 семестр						
1 Основные понятия информационно-аналитических систем	6	4	4	10	24	ПК-10
2 Методы и средства обеспечения информационной безопасности специальных ИАС	12	4	4	15	35	ОПК-7, ПК-10
3 Технологии и инструментальные средства информационной безопасности создаваемых специальных ИАС	6	4	4	14	28	ПК-10
4 Методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности	4	4	4	9	21	ПК-13

Согласована на портале № 16895

Итого за семестр	28	16	16	48	108	
Итого	28	16	16	48	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Основные понятия информационно-аналитических систем	1. Понятние информационно-аналитической системы, примеры сферы применения2. Технологии применяемые при создании информационно-аналитических систем	6	ПК-10
	Итого	6	
2 Методы и средства обеспечения информационной безопасности специальных ИАС	1. Угрозы информационной безопасности ИАС2. Методы обеспечения информационной безопасности ИАС3. Средства обеспечения информационной безопасности специальных ИАС	12	ОПК-7
	Итого	12	
3 Технологии и инструментальные средства информационной безопасности создаваемых специальных ИАС	1. Создание специальных ИАС2. Технологии и инструментальные средства ИБ ИАС	6	ПК-10
	Итого	6	
4 Методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности	1. Методы оценки эффективности специальных ИАС2. Методы оценки эффективности средств обеспечения информационной безопасности ИАС	4	ПК-13
	Итого	4	
Итого за семестр		28	

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

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

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин			
	1	2	3	4
Предшествующие дисциплины				
1 Базы данных и экспертные системы	+			
2 Безопасность программного обеспечения		+	+	+

Согласована на портале № 16895

3 Безопасность систем баз данных	+			
4 Информатика	+			
5 Информационные технологии	+			
6 Криптографические методы защиты информации		+	+	
7 Математические методы проектирования финансовых систем (групповое проектное обучение - ГПО 1)				+
8 Методология и организация информационно-аналитической деятельности	+	+	+	+
9 Моделирование информационно-аналитических систем	+	+	+	+
10 Основы информационной безопасности	+	+	+	+
11 Прикладная криптография		+	+	
12 Принципы построения, проектирования и эксплуатации информационно-аналитических систем	+	+	+	+
13 Проектирование информационно-аналитических систем (групповое проектное обучение - ГПО 2)	+	+	+	+
14 Проектирование подсистемы безопасности информационно-аналитических систем в финансовой сфере (групповое проектное обучение - ГПО 3)	+	+	+	+
15 Распределенные информационно-аналитические системы	+	+	+	+
16 Системное программирование		+	+	
17 Специальные технологии баз данных и информационных систем	+	+	+	
18 Теоретические основы компьютерной безопасности		+	+	
19 Техническая защита информации			+	
20 Формализованные модели и методы решения аналитических задач	+			

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 № 16895

Компетенции	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	
ОПК-7	+	+	+	+	Домашнее задание, Отчет по лабораторной работе, Опрос на занятиях
ПК-10	+	+	+	+	Домашнее задание, Отчет по лабораторной работе, Опрос на занятиях
ПК-13	+	+	+	+	Домашнее задание, Отчет по лабораторной работе, Опрос на занятиях

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 лекции	Интерактивные лабораторные занятия	Интерактивные практические занятия	Всего
10 семестр				
Выступление студента в роли обучающего	8			8
Презентации с использованием мультимедиа с обсуждением			4	4
Разработка проекта		4		4
Итого за семестр:	8	4	4	16
Итого	8	4	4	16

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
10 семестр			
1 Основные понятия	Выполнение лабораторных работ по	4	ПК-10

Согласована на портале № 16895

информационно-аналитических систем	основам информационно-аналитических систем		
	Итого	4	
2 Методы и средства обеспечения информационной безопасности специальных ИАС	Выполнение лабораторной работы по методам и средствам обеспечения информационной безопасности специальных ИАС	4	ОПК-7
	Итого	4	
3 Технологии и инструментальные средства информационной безопасности создаваемых специальных ИАС	Выполнение лабораторной работы по технологиям и инструментальным средствам информационной безопасности создаваемых специальных ИАС	4	ПК-10
	Итого	4	
4 Методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности	Выполнение лабораторной работы по оценке эффективности специальных ИАС	4	ПК-13
	Итого	4	
Итого за семестр		16	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Основные понятия информационно-аналитических систем	Проверка освоения теоретического материала, разбор возникших вопросов	4	ПК-10
	Итого	4	
2 Методы и средства обеспечения информационной безопасности специальных ИАС	Проверка выполнения практических заданий, их разбор	4	ОПК-7, ПК-10
	Итого	4	
3 Технологии и инструментальные средства информационной безопасности создаваемых специальных ИАС	Проверка практического задания	4	ПК-10
	Итого	4	
4 Методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности	Проверка практического задания	4	ПК-13
	Итого	4	
Итого за семестр		16	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Согласована на портале № 16895

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Основные понятия информационно-аналитических систем	Подготовка к практическим занятиям, семинарам	4	ПК-10	Домашнее задание, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	4		
	Итого	10		
2 Методы и средства обеспечения информационной безопасности специальных ИАС	Подготовка к практическим занятиям, семинарам	8	ОПК-7, ПК-10	Домашнее задание, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	3		
	Оформление отчетов по лабораторным работам	4		
	Итого	15		
3 Технологии и инструментальные средства информационной безопасности создаваемых специальных ИАС	Подготовка к практическим занятиям, семинарам	8	ПК-10	Домашнее задание, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	4		
	Итого	14		
4 Методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности	Подготовка к практическим занятиям, семинарам	4	ПК-13	Домашнее задание, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
Итого за семестр		48		
Итого		48		

Согласована на портале № 16895

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
10 семестр				
Домашнее задание	10	10	15	35
Опрос на занятиях	10	10	10	30
Отчет по лабораторной работе	12	11	12	35
Итого максимум за период	32	31	37	100
Нарастающим итогом	32	63	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. Исаев Д. В. АНАЛИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ. Учебное пособие / Государственный университет – Высшая школа экономики. — М., 2008. — 60с. [Электронный ре-

Согласована на портале № 16895

сурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/book2.pdf

2. Белов В. С. ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ. Основы проектирования и применения: учебное пособие, руководство, практикум / Московский государственный университет экономики, статистики и информатики. — М., 2005. — 111с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/book1.pdf

12.2. Дополнительная литература

1. Основы защиты информации: учебное пособие / Томский государственный университет систем управления и радиоэлектроники. Изд. 5-е, перераб. и доп. – Томск: В-Спектр, 2011. – 244 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Малахов Н.В. Безопасность информационно-аналитических систем: методические указания по выполнению лабораторных работ / Томский государственный университет систем управления и радиоэлектроники. Томск, 2013. - 5с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/sias/labs.pdf
2. Малахов Н.В. Безопасность информационно-аналитических систем: методические указания по выполнению практических работ / Томский государственный университет систем управления и радиоэлектроники. Томск, 2013. - 5с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/sias/pract.pdf
3. Малахов Н.В. Безопасность информационно-аналитических систем: методические указания по выполнению самостоятельных работ / Томский государственный университет систем управления и радиоэлектроники. Томск, 2013. - 5с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/sias/sam.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. Microsoft Windows 8.1
2. OpenOffice
3. VeraCrypt
4. MySQL Server
5. Microsoft Visual Studio
6. Microsoft Visio

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

Согласована на портале № 16895

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2015 Community; Microsoft Office Visio 2010; Microsoft SQL-Server 2012

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, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2015 Community; Microsoft Office Visio 2010; Microsoft SQL-Server 2012

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 Celeron 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

Согласована на портале № 16895

С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

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

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- 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 № 16895

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

Безопасность информационных и аналитических систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**

Учебный план набора 2012 года

Разработчик:
- Ассистент каф. КИБЭВС Н. В. Малахов

Зачет: 10 семестр

Томск 2017

Согласована на портале № 16895

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-13	способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности	Должен знать методы и средства обеспечения информационной безопасности специальных ИАС; технологии, инструментальные средства, средства обеспечения информационной безопасности создаваемых специальных ИАС; методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.; Должен уметь применять методы и средства обеспечения информационной безопасности специальных ИАС; осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС; оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности.; Должен владеть методами и средствами обеспечения информационной безопасности специальных ИАС; методами оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.;
ПК-10	способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС	
ОПК-7	способностью применять методы и средства обеспечения информационной безопасности специальных ИАС	

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

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

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

Согласована на портале № 16895

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-13

ПК-13: способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности.

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

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Способы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности	Оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности	Способами оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности
Виды занятий	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Практические занятия; • Интерактивные лекции; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Практические занятия; • Интерактивные лекции; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;	• Самостоятельная работа; • Лабораторные работы; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;
Используемые средства оценивания	• Домашнее задание; • Отчет по лабораторной работе; • Опрос на занятиях; • Зачет;	• Домашнее задание; • Отчет по лабораторной работе; • Опрос на занятиях; • Зачет;	• Домашнее задание; • Отчет по лабораторной работе; • Зачет;

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)	• Знать основные и продвинутые способы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности;	• Безошибочно оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;	• способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;
Хорошо (базовый	• Знать основные и	• Оценивать эффектив-	• способностью оцени-

Согласована на портале № 16895

уровень)	продвинутые способы оценки эффективности специальных ИАС;	ность специальных ИАС, в том числе средств обеспечения их информационной безопасности;	вать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;
Удовлетворительно (пороговый уровень)	• Знать основные способы оценки эффективности специальных ИАС;	• Оценивать эффективность специальных ИАС;	• способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;

2.2 Компетенция ПК-10

ПК-10: способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС.

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

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС	осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС	способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС
Виды занятий	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Практические занятия; • Интерактивные лекции; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Практические занятия; • Интерактивные лекции; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;	• Самостоятельная работа; • Лабораторные работы; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;
Используемые средства оценивания	• Домашнее задание; • Отчет по лабораторной работе; • Опрос на занятиях; • Зачет;	• Домашнее задание; • Отчет по лабораторной работе; • Опрос на занятиях; • Зачет;	• Отчет по лабораторной работе; • Домашнее задание; • Зачет;

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

Согласована на портале № 16895

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;	• осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;	• технологиями, инструментальными средствами, средствами вычислительной техники и средствами обеспечения информационной безопасности создаваемых специальных ИАС;
Хорошо (базовый уровень)	• технологии, инструментальные средства, средства вычислительной техники создаваемых специальных ИАС;	• осуществлять выбор технологии, инструментальных средств, средств вычислительной техники создаваемых специальных ИАС;	• технологиями, инструментальными средствами, средствами вычислительной техники создаваемых специальных ИАС;
Удовлетворительно (пороговый уровень)	• технологии и инструментальные средства создаваемых специальных ИАС;	• осуществлять выбор технологии, инструментальных средств создаваемых специальных ИАС;	• технологиями, инструментальными средствами создаваемых специальных ИАС;

2.3 Компетенция ОПК-7

ОПК-7: способностью применять методы и средства обеспечения информационной безопасности специальных ИАС.

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	методы и средства обеспечения информационной безопасности специальных ИАС	применять методы и средства обеспечения информационной безопасности специальных ИАС	способностью применять методы и средства обеспечения информационной безопасности специальных ИАС
Виды занятий	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Практические занятия; • Интерактивные лекции; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;	• Самостоятельная работа; • Лекции; • Лабораторные работы; • Практические занятия; • Интерактивные лекции; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;	• Самостоятельная работа; • Лабораторные работы; • Интерактивные лабораторные занятия; • Интерактивные практические занятия;
Используемые средства оценива-	• Домашнее задание; • Отчет по лаборатор-	• Домашнее задание; • Отчет по лаборатор-	• Домашнее задание; • Отчет по лаборатор-

Согласована на портале № 16895

ния	ной работе; • Опрос на занятиях; • Зачет;	ной работе; • Опрос на занятиях; • Зачет;	ной работе; • Зачет;

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)	• широкий спектр методов и средств обеспечения информационной безопасности специальных ИАС;	• применять широкий спектр методов и средств обеспечения информационной безопасности специальных ИАС;	• способностью применять широкий спектр методов и средств обеспечения информационной безопасности специальных ИАС;
Хорошо (базовый уровень)	• спектр методов и средств обеспечения информационной безопасности специальных ИАС;	• применять спектр методов и средств обеспечения информационной безопасности специальных ИАС;	• способностью применять спектр методы и средства обеспечения информационной безопасности специальных ИАС;
Удовлетворительно (пороговый уровень)	• методы и средства обеспечения информационной безопасности специальных ИАС;	• применять методы и средства обеспечения информационной безопасности специальных ИАС;	• способностью применять методы и средства обеспечения информационной безопасности специальных ИАС;

3 Типовые контрольные задания

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

3.1 Темы домашних заданий

- Подготовить доклад на тему "Информационная система ..."
- Подготовить доклад на тему "Аналитическая система ..."
- Подготовить доклад на тему "Информационная-аналитическая система ..."

3.2 Темы опросов на занятиях

- 1. Понятние информационно-аналитической системы, примеры сферы применения
- 2. Технологии применяемые при создании информационно-аналитических систем
- 1. Угрозы информационной безопасности ИАС
- 2. Методы обеспечения информационной безопасности ИАС
- 3. Средства обеспечения информационной безопасности специальных ИАС
- 1. Создание специальных ИАС
- 2. Технологии и инструментальные средства ИБ ИАС
- 1. Методы оценки эффективности специальных ИАС
- 2. Методы оценки эффективности средств обеспечения информационной безопасности ИАС

3.3 Темы лабораторных работ

- Выполнение лабораторных работ по основам информационно-аналитических систем
- Выполнение лабораторной работы по методам и средствам обеспечения информационной безопасности специальных ИАС
- Выполнение лабораторной работы по технологиям и инструментальным средствам ин-

Согласована на портале № 16895

формационной безопасности создаваемых специальных ИАС

– Выполнение лабораторной работы по оценке эффективности специальных ИАС

3.4 Зачёт

– Применить методы и средства обеспечения информационной безопасности специальных ИАС

– Осуществить выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемой специальных ИАС

– Произвести оценку эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности

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. Исаев Д. В. АНАЛИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ. Учебное пособие / Государственный университет – Высшая школа экономики. — М., 2008. — 60с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/book2.pdf
2. Белов В. С. ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ. Основы проектирования и применения: учебное пособие, руководство, практикум / Московский государственный университет экономики, статистики и информатики. — М., 2005. — 111с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/book1.pdf

4.2. Дополнительная литература

1. Основы защиты информации: учебное пособие / Томский государственный университет систем управления и радиоэлектроники. Изд. 5-е, перераб. и доп. – Томск: В-Спектр, 2011. – 244 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

4.3. Обязательные учебно-методические пособия

1. Малахов Н.В. Безопасность информационно-аналитических систем: методические указания по выполнению лабораторных работ / Томский государственный университет систем управления и радиоэлектроники. Томск, 2013. - 5с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/sias/labs.pdf
2. Малахов Н.В. Безопасность информационно-аналитических систем: методические указания по выполнению практических работ / Томский государственный университет систем управления и радиоэлектроники. Томск, 2013. - 5с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/sias/pract.pdf
3. Малахов Н.В. Безопасность информационно-аналитических систем: методические указания по выполнению самостоятельных работ / Томский государственный университет систем управления и радиоэлектроники. Томск, 2013. - 5с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/mnv1/sias/sam.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Microsoft Windows 8.1
2. OpenOffice
3. VeraCrypt
4. MySQL Server
5. Microsoft Visual Studio
6. Microsoft Visio

Согласована на портале № 16895