Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

«ОСНОВЫ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Информационно-аналитические системы финансового мониторинга
Квалификация (степень) выпускника: бакалавр
Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Воронов А.Н. Рабочая программа дисциплины: «Основы проектной деятельности». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ООП ВО к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Целью изучения дисциплины является формирование у обучаемых специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества и методики постановки задач концептуального проектирования систем информационной безопасности, приобретение навыков в применении современных технологий при проектировании информационной безопасности объектов различных организаций и предприятий.

В процессе обучения слушатель приобретает и совершенствует следующие компетенции:

Общепрофессиональные компетенции:

- ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;
- ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;
- ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;
- ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

Профессиональные компетенции:

- ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;
- ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

- ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
- ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;
- ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;
- ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;
- ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;
- ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Профессионально - специализированные компетенции:

- ПСК-2: способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур, для информационно-аналитического обеспечения финансового мониторинга;
- ПСК-3: способность участвовать в разработке информационно-аналитических систем финансового мониторинга;
- ПСК-4: способность реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур.

Основными задачами дисциплины являются:

1. Ознакомление обучаемых с методологическими подходами постановки задач при проектировании систем информационной безопасности предприятий, а также с основными методами определения параметров, характеристик и структуры системы информационной безопасности;
2. Формирование у обучаемых способности самостоятельно решать поставленные задачи в области проектирования систем информационной безопасности с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные теоретико-методологические принципы проектирования систем информационной безопасности предприятий;
- структуру проектирования систем информационной безопасности предприятий и технологии её применения;
- методы и последовательность организации проектирования систем информационной безопасности предприятий;
- средства проектирования и модели жизненного цикла систем информационной безопасности предприятий;
- методы оценки эффективности проектируемых систем информационной безопасности предприятий;
- основы моделирования систем информационной безопасности предприятий, особенности проектирования адаптивных систем безопасности;
- основные тенденции развития теории и методологии проектирования систем информационной безопасности предприятий.

Уметь:

- правильно формулировать требования к проектированию систем информационной безопасности предприятий;
- определять основные задачи и функции проектирования систем информационной безопасности предприятий;
- определять структуру системы проектирования и основные периоды жизненного цикла систем информационной безопасности предприятий;
- выполнять основные этапы проектирования систем информационной безопасности предприятий;
- использовать гипотетические модели и методы оценки эффективности проектируемых систем информационной безопасности;
- формулировать рекомендации по совершенствованию методологии проектирования систем информационной безопасности.

Владеть навыками:

- постановки задач по проектированию систем информационной безопасности предприятий;
- построения технологического процесса применения систем информационной безопасности при проектировании;
- применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятий;
- грамотного применения на практике основ проектирования систем информационной безопасности и выбора организационно-методических средств проектирования;

- методики организации и управления качеством проектирования систем информационной безопасности предприятий.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Основы проектной деятельности» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Основы финансового мониторинга» и компетенциях: ОК-3, 5; ОПК-2,4,6 и ПК-1,4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Технико-экономическое обоснование проекта», «Разработка и реализация проекта», «Актуальные проблемы финансов», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Организация информационно-аналитического обеспечения финансового мониторинга», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы обучения составляет 4 зачетные единицы, 144 часа.

Таблица 1

Виды занятий	**Всего часов**	**Семестр 3**	**Семестр 4**	**Семестр …**	**Семестр …**
Общая трудоемкость	144	72	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	16	16		
Лекции (Л)	-	-	-		
Практические занятия (ПЗ)	32	16	16		
Лабораторные работы (ЛР)	-	-	-		
Самостоятельная работа	112	56	56		
КСР	-	-	-		
Курсовые работы (проекты)	-	-	-		
Расчетно-графические ра-	-	-	-		

боты					
Контрольная работа, домашнее задание	-	-	-		
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2	Т1; Т2		
Вид итогового контроля	Зачёт/Зачёт с оценкой	Зачёт	Зачёт с оцен-кой		

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Код компетенций
Третий семестр				
Тема 1. Методология проектирования систем информационной безопасности предприятий.	-	4	1	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9,10, 11,12,13,14,15 ПСК-2,3,4
Тема 2. Особенности проектирования систем защиты информации предприятий.	-	4	1	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9,10, 11,12,13,14,15 ПСК-2,3,4
Тема 3. Основы моделирования систем информационной безопасности предприятий.	-	8	1	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9,10, 11,12,13,14,15 ПСК-2,3,4
Четвёртый семестр				
Тема 4. Методика оценки эффективности проектируемых систем информационной безопасности.	-	8	1	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9,10, 11,12,13,14,15 ПСК-2,3,4.
Тема 5. Особенности проектирования адаптивных систем информационной безопасности.	-	8	2	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9,10, 11,12,13,14,15 ПСК-2,3,4
Итого:	-	32	6	

4.2. Содержание тем дисциплины

Тема 1. Методология проектирования систем информационной безопасности предприятий.

Предметная область проектирования систем информационной безопасности предприятий. Типология систем проектирования и жизненный цикл системы информационной безопасности предприятий. Основные требования к системам проектирования, задачи и функции проектирования систем информационной безопасности предприятий. Краткая характеристика технологий проектирования. Структура методологии проектирования, порядок выбора технологий и логика организации проектирования систем информационной безопасности предприятий. Обзор основных методов проектирования систем информационной безопасности.

Тема 2. Особенности проектирования систем защиты информации предприятий.

Последовательность решения задачи проектирования защиты информационных объектов предприятий. Жизненный цикл систем информационной безопасности, выбор состава оборудования и вариантов информационной защиты объектов предприятий. Основные методические подходы по определению требований к защите информации. Классификация требований по защите объектов предприятий, факторы, влияющие на требуемый уровень защиты. Методы формирования основных функций защиты и выбора средств защиты. Проектирование основных подсистем и элементов системы защиты информационных объектов в соответствии с концепцией полной и эшелонированной защиты.

Тема 3. Основы моделирования систем информационной безопасности предприятий.

Характеристика основных методов и моделей оценки уязвимости проектируемых систем информационной безопасности предприятий. Критерии оценки безопасности информационных технологий, организация требований к проектируемым перспективным продуктам и системам. Понятие модели информационной безопасности. Модель защиты региональных информационных объектов, как модель системы с полным перекрытием. Компьютерные модели оценки эффективности проектируемых систем информационной безопасности и порядок их применения.

Тема 4. Методика оценки эффективности проектируемых систем информационной безопасности.

Методы оценки эффективности проектируемых систем информационной безопасности и их особенности применения. Основные критерии оценки эффективности при проектировании систем информационной безопасности предприятий, качественный и количественный их анализ. Особенности оценки экономической эффективности проектируемых систем информационной безопасности предприятий. Понятие надёжности проектируемых систем и её оценка. Характеристика критериев и показателей эффективности для функций и элементов системы физической защиты региональных объектов, основные правила и процедуры их применения.

Тема 5. Особенности проектирования адаптивных систем информационной безопасности.

Основные тенденции развития теории и методологии проектирования систем информационной безопасности. Направления и тенденции в развитии качества аппаратно-программных средств проектирования в современном мире. Характеристика новых организационно-методических средств развития проектирования систем информационной безопасности. Особенности применения интеллектуальных средств для решения задач проектирования адаптивных систем информационной безопасности. Диалоговая среда моделирования адаптивных систем информационной безопасности.

4. 5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине.

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Основы проектной деятельности» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. Учебное пособие. – М.: Горячая линия-Телеком, 2012.
2. Заботина Н.Н. Проектирование информационных систем. Учебное пособие. – М.: «ИНФРА-М», 2011.
3. Коваленко В.В. Проектирование информационных систем. Учебное пособие. – М.: ФОРУМ, 2012.

Дополнительная литература:

1. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. Учебное пособие. – СПб.: НИУ ИТМО, 2013.
2. Исаев Г.Н. Проектирование информационных систем. Учебное пособие. – М.: Издательство «Омега-Л», 2013.

Рекомендуемая литература:

1. Нестерук Г.Ф., Осовецкий Л.Г., Нестерук Ф.Г. О применении нейро-

нечетких сетей в адаптивных системах информационной защиты // Нейроинформатика-2005: Матер. VII всерос. научно-техн. конф. – М.: МИФИ (ТУ), 2005.
2. Силаенков А.Н. Проектирование системы информационной безопасности. Учебное пособие. – Омск: Издательство ОмГТУ, 2009.
3. Смирнова Г.Н. и др. Проектирование экономических информационных систем. Учебник / под редакцией Тельнова Ю.Ф. – М.: Финансы и статистика, 2003.
4. Тупота В.И. Адаптивные средства защиты информации в вычислительных сетях. Учебное пособие. – М.: Радио и связь, 2002.
5. Юдицкий С.А., Владиславлев П.Н. Основы предпроектного анализа организационных систем. Учебное пособие. – М.: Финансы и статистика, 2005.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. Энциклопедия информационной безопасности. – Публикации, статьи (www.wikIsec.ru).
2. Информационно – справочные (правовые) системы: «Гарант» (garantcenter.ru), «Кодекс» (doskainfo.ru/advert/64804/), «Консультант +» (artiks.ru).

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды.
2. Рабочая программа и методическое обеспечение по дисциплине: «Основы проектной деятельности»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицен-

зионными программно-техническими средствами: операционная система не ниже Windows7; офисные программы MSOffice 13;

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ»
(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач;	Тема:1,2,3,4,5	Основные теоретико-методологические принципы проектирования систем информационной безопасности предприятия; структуру проектирования систем информационной безопасности региона и технологии её применения.	Правильно формулировать требования к проектированию систем информационной безопасности предприятия.	Навыками постановки задач по проектированию систем информационной безопасности предприятия; навыками грамотного применения на практике основ проектирования систем информационной безопасности и выбора организационно-методических средств проектирования.
2.	ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;	Тема:1,2,3,4,5	Основные теоретико-методологические принципы проектирования систем информационной безопасности предприятия; структуру проектирования систем информационной безопасности региона и технологии её применения.	Правильно формулировать требования к проектированию систем информационной безопасности предприятия.	Навыками постановки задач по проектированию систем информационной безопасности предприятия; навыками грамотного применения на практике основ проектирования систем информационной безопасности и выбора организационно-методических средств проектирования.
3.	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;	Тема:1,2,3,4,5	Методы оценки эффективности проектируемых систем информационной безопасности предприятия.	Определять структуру системы проектирования и основные периоды жизненного цикла систем информационной безопасности предприятия.	Навыками применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятия.
4.	ОПК-7	способность определять информационные	Тема:1,2,3,4,5	Методы оценки эффективности проекти-	Определять структуру системы проек-	Навыками применения основных методов анализа и оцен-

		ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.		руемых систем информационной безопасности предприятия.	тирования и основные периоды жизненного цикла систем информационной безопасности предприятия.	ки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятия.
5.	ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты;	Тема:1,2,3,4,5	Методы и последовательность организации проектирования систем информационной безопасности предприятия; средства проектирования и модели жизненного цикла систем информационной безопасности предприятия.	Определять основные задачи и функции проектирования систем информационной безопасности предприятия.	Навыками постановки задач по проектированию систем информационной безопасности предприятия; навыками грамотного применения на практике основ проектирования систем информационной безопасности и выбора организационно-методических средств проектирования.
6.	ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;	Тема:1,2,3,4,5	Методы и последовательность организации проектирования систем информационной безопасности предприятия; средства проектирования и модели жизненного цикла систем информационной безопасности предприятия.	Определять основные задачи и функции проектирования систем информационной безопасности предприятия.	Навыками постановки задач по проектированию систем информационной безопасности предприятия; навыками грамотного применения на практике основ проектирования систем информационной безопасности и выбора организационно-методических средств проектирования.
7.	ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	Тема:1,2,3,4,5	Методы и последовательность организации проектирования систем информационной безопасности предприятия; средства проектирования и модели жизненного цикла	Определять основные задачи и функции проектирования систем информационной безопасности предприятия.	Навыками постановки задач по проектированию систем информационной безопасности предприятия; навыками грамотного применения на практике основ проектирования систем информационной безопасности и выбора

				систем информационной безопасности предприятия.		организационно-методических средств проектирования.
8.	ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	Тема:1,2,3,4,5	Методы и последовательность организации проектирования систем информационной безопасности предприятия; средства проектирования и модели жизненного цикла систем информационной безопасности предприятия.	Определять основные задачи и функции проектирования систем информационной безопасности предприятия.	Навыками постановки задач по проектированию систем информационной безопасности предприятия; навыками грамотного применения на практике основ проектирования систем информационной безопасности и выбора организационно-методических средств проектирования.
9.	ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;	Тема:1,2,3,4,5	Методы оценки эффективности проектируемых систем информационной безопасности предприятия.	Использовать гипотетические модели и методы оценки эффективности проектируемых систем информационной безопасности.	Навыками применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятия.
10.	ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Тема:1,2,3,4,5	Методы оценки эффективности проектируемых систем информационной безопасности предприятия.	Использовать гипотетические модели и методы оценки эффективности проектируемых систем информационной безопасности.	Навыками применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятия.
11.	ПК-9	способность осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения ин-	Тема:1,2,3,4,5	Методы оценки эффективности проектируемых систем информационной безопасности предприятия.	Использовать гипотетические модели и методы оценки эффективности проектируемых систем информационной безопасности.	Навыками применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятия.

		формационной безопасности по профилю своей профессиональной деятельности;				
12.	ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;	Тема:1,2,3,4,5	Методы оценки эффективности проектируемых систем информационной безопасности предприятия.	Использовать гипотетические модели и методы оценки эффективности проектируемых систем информационной безопасности.	Навыками применения основных методов анализа и оценки рисков проектируемых систем, определения размеров возможного ущерба объектам информационной безопасности предприятия.
13.	ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;	Тема:1,2,3,4,5	Основы моделирования систем информационной безопасности предприятия, особенности проектирования адаптивных систем безопасности;	Выполнять основные этапы проектирования систем информационной безопасности предприятия.	Навыками построения технологического процесса применения систем информационной безопасности при проектировании.
14.	ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации;	Тема:1,2,3,4,5	Основы моделирования систем информационной безопасности предприятия, особенности проектирования адаптивных систем безопасности;	Выполнять основные этапы проектирования систем информационной безопасности предприятия.	Навыками построения технологического процесса применения систем информационной безопасности при проектировании.
15.	ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;	Тема:1,2,3,4,5	Основы моделирования систем информационной безопасности предприятия, особенности проектирования адаптивных систем безопасности;	Выполнять основные этапы проектирования систем информационной безопасности предприятия.	Навыками построения технологического процесса применения систем информационной безопасности при проектировании.
16.	ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;	Тема:1,2,3,4,5	Основы моделирования систем информационной безопасности предприятия, особенности проектирова-	Выполнять основные этапы проектирования систем информационной безопасности предприятия.	Навыками построения технологического процесса применения систем информационной безопасности при проектировании.

				ния адаптивных систем безопасности;		
17.	ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Тема:1,2,3,4,5	Основы моделирования систем информационной безопасности предприятия, особенности проектирования адаптивных систем безопасности;	Выполнять основные этапы проектирования систем информационной безопасности предприятия.	Навыками построения технологического процесса применения систем информационной безопасности при проектировании.
18.	ПСК-2	способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур, для информационно-аналитического обеспечения финансового мониторинга;	Тема:1,2,3,4,5	Основные тенденции развития теории и методологии проектирования систем информационной безопасности предприятия.	Формулировать рекомендации по совершенствованию методологии проектирования систем информационной безопасности.	Методикой организации и управления качеством проектирования систем информационной безопасности предприятия.
19.	ПСК-3	способность участвовать в разработке информационно-аналитических систем финансового мониторинга;	Тема:1,2,3,4,5	Основные тенденции развития теории и методологии проектирования систем информационной безопасности предприятия.	Формулировать рекомендации по совершенствованию методологии проектирования систем информационной безопасности.	Методикой организации и управления качеством проектирования систем информационной безопасности предприятия.
20.	ПСК-4	способность реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур.	Тема:1,2,3,4,5	Основные тенденции развития теории и методологии проектирования систем информационной безопасности предприятия.	Формулировать рекомендации по совершенствованию методологии проектирования систем информационной безопасности.	Методикой организации и управления качеством проектирования систем информационной безопасности предприятия.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-2	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-3	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится в письменной форме Критерии оценки: 1.Соответствие содержания реферата заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке работы (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной работы (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов.

			Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-4	Письменное задание	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-7	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-3, ПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру –

		3-4 балла С) не сформирована **2 балла**	10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-5, ПК-6	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится в письменной форме Критерии оценки: 1.Соответствие содержания реферата заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке работы (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной работы (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-7, ПК-8	Письменное задание	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована	1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов).

		2 балла	Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-9, ПК-10	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-11, ПК-12	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится в письменной форме Критерии оценки: 1.Соответствие содержания реферата заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке работы (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной работы (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры

			представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-13, ПК-14	Письменное задание	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-15	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПСК-2	Домашняя работа	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла**	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки:

		С) не сформирована **2 балла**	1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.
ПСК-3	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПСК-4	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла**	Проводится в письменной форме Критерии оценки: 1.Соответствие содержания реферата заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке работы (1

		С) не сформирована **2 балла**	балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной работы (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.

3. 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

Примерная тематика докладов в презентационной форме:

1. Состав и основные характеристики CALS-технологий для реализации стратегии CALS на различных этапах жизненного цикла изделий.
2. Анализ взаимосвязей стандартов управления ресурсами MRP, ERP и CSRP, а также системы управления CRM на этапе маркетинговых исследований.
3. Состав и основные характеристики «Кусочной» автоматизации предприятий и их систем защиты информации.
4. Особенности применения спиральной модели жизненного цикла информационной системы и модели непрерывной разработки таких систем и технологий.
5. Методология проектирования прикладных информационных систем на основе инструментария Oracle CDM.
6. Особенности применения технологии Microsoft Solutions Framework (MSF) корпорации Microsoft для управления проектами разработки информационных систем уровня предприятия.
7. Обзор и особенности применения современных технологий и основных инструментов выработки решений руководителями различных рангов и структур.
8. Состав, основные характеристики и порядок применения малых, средних и крупных средств моделирования информационных систем различных предприятий.
9. Характеристика различных взглядов на применение инструментария Architecture of Integrated Information Systems (ARIS) для описания и проектирования основных бизнес-процессов на предприятии.
10. Особенности реализации CASE-технологий в среде Oracle Designer и других средствах создания и сопровождения прикладных систем.
11. Особенности построения функциональных моделей информационных систем и технологий на основе методологии IDEF0.

12. Особенности построения интегрированных функциональных моделей ин формационных систем предприятий с использованием пакета BPwin в рамках методологии структурного моделирования.
13. Основные характеристики и особенности применения методологии диаграммы потоков данных (DFD) в нетрадиционном синтаксисе и других визуальных эффектов.
14. Основные понятия и определения технологии создания баз данных логического и физического уровней, порядок их разработки с помощью автоматизированного инструментария.
15. Сравнительный анализ международных и отечественных стандартов по организации создания и использования информационных систем предприятий, основные профили стандартов.
16. Состав, структура и содержание технологической и эксплуатационной документации при проектировании информационных систем и технологий.

Примерная тематика реферата:

1. Основные этапы автоматизации процессов проектирования систем информационной безопасности региона и их характеристика.
2. Стратегия CALS-технологии как средство повышения конкурентноспособности проектируемых систем информационной безопасности предприятий.
3. Общие понятия и методология управления проектом заказанной разработки комплексной системы информационной безопасности с использованием продукта “Oracle”.
4. Применение CASE-технологий и CASE-средств для проектирования систем информационной безопасности региона.
5. Общие сведения о профилях стандартов, применяемых при проектировании систем информационной безопасности.
6. Характеристика интегрированных систем управления предприятием, роль и место проектируемых систем информационной безопасности в деятельности современного холдинга.
7. Применение систем поддержки принятия решений – OLAP-технологий при проектировании и эксплуатации региональных систем информационной безопасности.
8. Методология внедрения систем информационной безопасности в регионе на базе пакетированных решений и модельно-ориентированного проектирования.
9. Современная методология создания перспективных систем информационной безопасности на основе интеллектуальных средств и адаптивных систем, основные особенности её применения.
10. Гибридные средства классификации систем информационной безопасности и особенности их применения для представления знаний в информационном поле.
11. Методика оценки защищённости информационных систем и технологий с применением механизмов нечёткой логики и нейронных сетей.
12. Обзор применяемых перспективных информационных технологий и интел-

лектуальных систем в адаптивных моделях информационной безопасности предприятий.

Примерная тематика письменного задания:

1. Методология построения модели управления городом с использованием технологии “AS IS” (Как есть) и технологии “TO BE” (Как должно быть).
2. Основные цели формирования требований при построении организационной структуры предприятий и диаграмм потоков данных объектного уровня с внешними объектами.
3. Предназначение, состав и методика применения интегрированных систем управления предприятиями на основе управленческого стандарта CSRP.
4. Особенности появления, развития и перспективы дальнейшего применения систем управления взаимоотношениями с клиентами CRM-систем (Customer Relationship Management) в России и за рубежом.
5. Основные понятия, характеристики и методика применения OLAP-технологий (On-Line Analytical Processing) при проектировании информационных систем и защищённых технологий на предприятиях региона.
6. Особенности многомерного представления информации при описании структур данных, основные показатели гиперкуба.
7. Состав и основные характеристики операций манипулирования измерениями, обзор операций формирования среза, иерархических отношений, операций агрегации и вращения.
8. Методика проектирования многомерной базы данных для предприятий и реализация защитных механизмов в ней, порядок использования аналитических функций.
9. Концепция проектирования информационных систем на основе модельно-ориентированной технологии и особенности её применения.
10. Характеристика основных этапов выполнения работ при проектировании информационных систем по каскадной модели жизненных циклов на предприятии.
11. Методика проектирования адаптивных информационных и образовательных систем.
12. Характеристика основных методов и технических приёмов адаптивной гипермедиа.
13. Архитектура адаптивной системы управления информационными и образовательными ресурсами Xite.
14. Методика проектирования адаптивных систем защиты информации на основе использования интеллектуальных средств.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Основы проектной деятельности» являются две текущие аттестации в виде тестов и одна итоговая аттестация в виде зачета/зачёта с оценкой в устной форме.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9, 10,	30 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - 0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9, 10, 11,12,13,14, 15	33 вопроса	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - 0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Зачёт	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9, 10, 11,12,13,14, 15	3 теоретических вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 15 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: «Зачтено»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «Не зачтено»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение

						использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.
Согласно учебному плану	Зачёт с оценкой	ОПК-2,3,4,7, ПК-3,4,5,6,7,8,9, 10, 11,12,13,14, 15 ПСК-2,3,4	3 вопроса	Зачёт с оценкой проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачёта с оценкой	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на большинство вопросов билета «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полу-

						ченные знания на практике; • не работал на практических занятиях; • ответил не на все вопросы билета **«Неудовлетворительно»**: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один или несколько вариантов ответа.

1-е тестирование по дисциплине

1. Жизненный цикл информационной системы – это?

– модель создания информационной системы;
– модель эксплуатации информационной системы;
– модель проектирования информационной системы;
– модель создания и использования информационной системы;

2. Спиральная модель жизненного цикла информационной системы предполагает что?

– делается упор на начальные этапы жизненного цикла, реализуемость технических решений проверяется путём создания прототипов;
– существует наличие циклов, обратной связи между этапами, наличие межэтапных корректировок;
– переход на следующий этап осуществляется после полного окончания работ по предыдущему этапу;
– делается упор на последние этапы жизненного цикла, предполагается

жёсткая детерминация времени исполнения каждого этапа.

3. CASE-средства обеспечивают?

– использование специальным образом организованного хранилища проектных метаданных (репозитария);
– сокращение персонала, связанного с информационной технологией;
– уменьшение степени участия в проектах высшего руководства и менеджеров, а также экспертов предметной области, уменьшение степени участия пользователей в процессе разработки информационных систем;
– немедленное повышение продуктивности деятельности организации.

4. Обозначение IDEF0 это?

– диаграмма ключей;
– диаграммы бизнес-процессов;
– диаграмма потоков данных.

5. Уровнями логической модели данных являются?

– диаграмма сущность-связь;
– модель данных, основанная на ключах;
– полная атрибутная модель.

6. Определённое свойство объекта в ER-диаграмме выражает?

– сущность;
– атрибут;
– связь;
– ключ;

7. Между зависимой и независимой сущностями связь может быть?

– неидентифицирующая;
– многие ко многим;
– идентифицирующая.

8. Что происходит при установлении неидентифицирующей связи?

– миграция атрибутов первичного ключа родительской сущности в состав первичного ключа дочерней сущности;
– атрибуты первичного ключа родительской сущности мигрируют в состав неключевых атрибутов дочерней сущности;
– не происходит миграции ключей.

9. Внешний ключ – это?

– мигрировавший в атрибуты дочерней сущности первичный ключ из родительской сущности;
– первичный ключ родительской сущности;
– первичный ключ данной сущности;
– атрибут, по которому возникает необходимость сортировки данных.

10. Мощность связи обозначает?

– число дочерних сущностей у родительской;
– количество экземпляров дочерней сущности, связанных с одним экземпляром родительской сущности;
– число мигрировавших ключей.

11. Имя роли (функциональное имя) в логической модели данных – это?

– синоним атрибута внешнего ключа в дочерней сущности;
– отображаемое имя связи на диаграмме;
– имя внешнего ключа в дочерней сущности.

12. Миграция атрибутов в логической модели данных происходит при установлении?

– идентифицирующей связи;
– неидентифицирующей связи;
– в любом из вышеперечисленных случаев.

13. БНФ-нотация используется?

– для описания механизмов;
– для описания данных;
– для задания мини-спецификаций процессов.

14. Правилами нормализации существование в одной сущности двух атрибутов с одинаковыми именами?

– запрещено;
– разрешено;
– разрешается при установлении определённых типов связи.

15. Вторая нормальная форма логической модели данных имеет смысл?

– только для сущностей, имеющих сложный ключ;
– только при хранении в одном атрибуте разных по смыслу значений;
– при наличии зависимости неключевого атрибута от части ключа.

16. Вторая нормальная форма логической модели данных предполагает отсутствие взаимосвязи между неключевыми атрибутами?

– да;
– нет;

17. Ошибкой нормализации является?

– хранение в одном атрибуте разных по смыслу значений;
– разделение сложных атрибутов на атомарные;
– независимость неключевых атрибутов от других неключевых атрибутов.

18. Одним из требований, предъявляемых к первичному ключу, является следующее?

– два экземпляра не должны иметь одинаковых значений возможного ключа;
– ключ не должен быть составным;
– атрибуты ключа должны иметь нулевые значения.

19. Вторичный ключ это потенциальный ключ, не ставший первичным?

– да;
– нет.

20. Внешние ключи создаются автоматически?

– когда любая связь соединяет сущности;

– только при установлении идентифицирующей связи;
– только при установлении связи «многие ко многим»;
– нет верного ответа.

21. Согласны ли Вы, что зависимые сущности?

– могут иметь один и тот же внешний ключ из нескольких родительских сущностей;
– не могут получить один и тот же внешний ключ несколько раз через разные связи;
– справедливы оба ответа.

22. Верно ли утверждение, что информация обладает свойствами, отражающими её природу и особенности использования: кумулятивностью, эмержентностью, неассоциативностью?

– да;
– нет.

23. По какому признаку информационные системы делят на одиночные, групповые, корпоративные?

– по масштабу;
– по сфере применения;
– по способу организации.

24. Системы обработки транзакций подразделяются на:

– пакетные ИС;
– оперативные ИС;
– комбинированные ИС;
– структурные ИС.

25. Что представляет из себя OLTP (Online Transaction Processing)?

– режим оперативной обработки транзакций;
– режим пакетной обработки транзакций;
– режим обработки запроса пользователя;
– время обработки транзакций.

26. Какой из перечисленных пунктов не входит в классификацию информационных систем по способу их организации?

– системы на основе архитектуры файл–сервер;
– системы на основе архитектуры клиент–сервер;
– системы на основе многоуровневой архитектуры;
– корпоративные информационные системы.

27. Информационные системы, ориентированные на коллективное использование информации членами рабочей группы чаще всего?

– одиночные;
– групповые;
– корпоративные;
– комбинированные.

28. Какие из перечисленных информационных систем основаны на использовании гипертекстовых документов и функций мультимедиа?

– системы поддержки принятия решений;
– информационно-справочные системы;

– офисные информационные системы;
– расчётно-логические системы.

29. По какому признаку классификации информационных систем они объединяют в себе: системы обработки транзакций, системы поддержки принятия решений, информационно-справочные и офисные информационные системы?

– по сфере применения;
– по масштабу;
– по способу организации;
– по составу.

30. Выберите требования, предъявляемые к информационным системам:

– гибкость;
– надёжность;
– эффективность;
– безопасность.

2-е тестирование по дисциплине

1. Информационно-поисковые системы входят в состав документальных информационных систем?

– да;
– нет.

2. Какими специальными навигационными конструкциями оснащаются документы, помещаемые в хранилища в семантически-навигационных системах?

– гиперссылками;
– тегами;
– маркерами;
– ключами.

3. Как называются связи в базе данных, когда одна и та же запись может входить в отношения со многими другими записями?

– «один к одному»;
– «один ко многим»;
– «многие ко многим».

4. Существует ли связь «один ко многим» в реляционной структуре данных?

– да;
– нет.

5. Как называется модель данных, в которой информация представлена в виде древовидной структуры с реализацией логических отношений «целое-часть»?

– реляционной;
– иерархической;
– сетевой;

– полярной.

6. В каких моделях отношения представляются в виде двумерной таблицы с подмножеством декартовых произведений доменов?

– в сетевых;
– в детерминированных;
– в реляционных;
– в бинарных.

7. Выберите стандартные методы организации файловой системы на магнитном диске в соответствии с методами доступа к ним:?

– последовательные файлы;
– индексно-последовательные файлы;
– графические файлы;
– индексно-произвольные файлы.

8. Алфавит – это система знаков, используемых для записи слов и выражений?

– да;
– нет.

9. В какой классификации объектов вся предметная область разбивается на ряд исходных рубрик по семантическому принципу, отражающему её специфику?

– в фасетной;
– в иерархической;
– в спиральной;
– в каскадной.

10. Непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы (ИС) и заканчивающийся в момент полного изъятия её из эксплуатации называют?

– разработкой ИС;
– проектированием ИС;
– жизненным циклом ИС;
– испытаниями ИС.

11. Жизненный цикл разрабатываемого программного обеспечения по методологии RAD включает в себя фазу оценки его эффективности?

– да;
– нет.

12. Новые сведения, которые могут быть использованы человеком для совершенствования своей деятельности и пополнения знаний называют?

– информацией;
– информационной системой;
– информационной технологией;
– системотехникой.

13. Кто предложил реляционную модель данных, основанную на представлении объектов в виде двумерных таблиц?

– С. Морзе;
– К. Шеннон;

– Э. Кодд;
– П. Чен.

14. Понятия кортеж и атрибут относятся к какой модели данных?

– сетевой;
– реляционной;
– каскадной;
– спиральной.

15. Множество атомарных значений одного и того же типа называют?

– записью;
– ключом;
– кортежем;
– доменом.

16. Как называется ключ, в который включены значимые атрибуты с соответствующей информацией об объекте?

– естественный;
– искусственный;
– суррогатный;
– составной.

17. Как называется ключ, созданный самой СУБД или пользователем с помощью определённой процедуры, но сам по себе не содержащий информации?

– естественный;
– искусственный;
– суррогатный;
– составной.

18. Какой знак представляет собой указатель на данные, размещённые в реляционной таблице?

– номер;
– индекс;
– метка;
– ссылка.

19. Как называется процесс организации данных путём ликвидации повторяющихся групп с целью приведения таблиц к виду непротиворечивого и корректного редактирования их?

– консолидация данных;
– конкатенация данных;
– нормализация данных;
– инкапсуляция данных.

20. Выберите формы представления числовых данных в таблицах:

– целочисленные;
– вещественные с фиксированной точкой;
– вещественные с плавающей точкой;
– даты и времени.

21. Как называют уровни полномочий пользователей базы данных?

– правами;

– привилегиями;
– свойствами;
– способами.

22. Выберите правильные разновидности документальных информационных систем при их классификации:

– информационно-поисковые;
– фактографические;
– полнотекстовые;
– расчётно-логические.

23. Какие операции с данными возможны при создании отчётов в СУБД?

– сортировка данных;
– группировка данных;
– изменение данных;
– вычисление итогов.

24. Совокупность действий со строго определёнными правилами их выполнения это?

– система;
– алгоритм;
– закон;
– матрица.

25. Единая система данных, организованная по определённым правилам, которые предусматривают общие принципы описания, хранения и обработки их называется?

– сводом законов;
– базой данных;
– базой знаний;
– методикой.

26. Формализованная система сведений о некоторой предметной области, содержащая данные о свойствах объектов, закономерностях и правилах использования их в задаваемых ситуациях для принятия актуальных решений называется?

– сводом законов;
– базой данных;
– базой знаний;
– методикой.

27. В чём заключается цель информатизации общества в нашей стране?

– в справедливом распределении материальных благ;
– в удовлетворении духовных потребностей человека;
– в удовлетворении информационных потребностей граждан, их групп предприятий и организаций за счёт внедрения компьютеров и средств коммуникаций;
– в привлечении граждан к активной познавательной и созидательной деятельности.

28. С помощью какого инструмента рекомендуется формировать решение в условиях риска?

– дерево вывода;
– дерево решений;
– дерево целей;
– нечёткие множества.

29. Что предусматривает термин «Информатизация общества»?

– увеличение избыточной информации, циркулирующей в обществе;
– изучение информатики во всех учебных заведениях страны;
– организацию свободного доступа каждого человека к информационным ресурсам, накопленным человеческой цивилизацией;
– целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных технологий.

30. Что такое генерализация?

– то же самое, что и ассоциация;
– отношение между суперклассом и подклассом;
– отношение между объектами внутри класса;
– то же самое, что и наследование.

31. Что такое полиморфизм?

– принцип, позволяющий разным объектам выполнять одни и те же операции, вести себя одинаково;
– то же, что и генерализация;
– принцип, основанный на совпадении метода с сигнатурой, описанной в интерфейсе;
– принцип инкапсуляции объектов.

32. Композиция – это более строгая разновидность агрегации?

– да;
– нет.

33. Начало какого этапа жизненного цикла информационной системы знаменует собой создание диаграммы классов?

– тестирования;
– анализа;
– проектирования;
– внедрения.

4.2. Типовые вопросы, выносимые на зачёт

1. Характеристика предметной области проектирования систем информационной безопасности предприятия.
2. Основные понятия проектирования систем информационной безопасности и их характеристика.
3. Типология и жизненный цикл проектирования систем информационной бебезопасности предприятия.
4. Основные требования к проектированию систем информационной безопас-

ности, цель их проектирования.
5. Универсальные и специальные задачи и функции проектирования систем информационной безопасности предприятия.
6. Структура проектирования систем информационной безопасности и её функциональная и обеспечивающая части.
7. Организационно-правовое обеспечение проектирования систем информационной безопасности, характеристика проектно-технической документации проетируемых систем.
8. Состав и основные элементы принципиальной схемы функционирования проектируемой системы информационной безопасности предприятия.
9. Краткая характеристика методологии проектирования систем информационной безопасности и требования к ней, выбор технологии проектирования.
10. Основные методы проектирования систем информационной безопасности, логика организации проектирования.
11. Характеристика современных средств проектирования систем информационной безопасности, особенности их применения.
12. Понятие модели жизненного цикла системы информационной безопасности, основные разновидности моделей и особенности их применения.
13. Содержание и характеристика предпроектной стадии создания системы информационной безопасности предприятия.
14. Содержание и характеристика стадии разработки технического задания проектируемой системы.
15. Содержание и характеристика эскизного и технического проектирования системы информационной безопасности предприятия.
16. Содержание и характеристика рабочего проектирования системы информационной безопасности предприятия, состав комплекта проектной документации.

4.4 Типовые вопросы, выносимые на зачёт с оценкой

1. Выбор состава оборудования для системы физической защиты различных объектов и их предварительная оценка.
2. Организация требований к системам безопасности в рамках документа «Общие критерии».
3. Основные характеристики эффективной системы физической защиты (СФЗ) региональных объектов и основные критерии её проектирования.
4. Архитектура системы защиты информации и объектов, порядок её построения, понятие ядра СФЗ.
5. Порядок обеспечения безопасности защищаемых объектов с помощью средств физической защиты информации, последовательность решения задачи.
6. Оборудование центрального поста персонала охраны и интегрального комплекса физической защиты охраняемых объектов.
7. Последовательность анализа и оценки эффективности проектирования систем информационной безопасности.
8. Методы оценки эффективности функционирования систем безопасности.

9. Основные характеристики и показатели эффективности датчиков охранной сигнализации.
10. Особенности эмпирического подхода к оценке уязвимости информации.
11. Характеристика основных показателей эффективности проектируемой СФЗ их количественный и качественный анализ.
12. Порядок оценки и управления рисками при проектировании систем информационной безопасности.
13. Критерии оценки безопасности информационных технологий, стратегия защиты информации.
14. Основные инструменты для проведения количественного анализа систем информационной безопасности, характеристика компьютерных моделей.
15. Основные методы и модели оценки уязвимости информации.
16. Рекомендации по использованию моделей оценки уязвимости информации.
17. Характеристика семирубежной модели защиты информации, особенности использования модели с полным перекрытием.
18. Трёхмерная модель системы защиты информации, как составная часть комплексной системы безопасности.
19. Основные тенденции развития теории и методологии проектирования систем информационной безопасности на современном этапе развития науки и общества.
20. Основные тенденции развития качества, применяемых аппаратно-программных средств проектирования систем безопасности.
21. Организационно-методические средства развития проектирования систем информационной безопасности.
22. Применение современных интеллектуальных средств для решения задач проектирования систем информационной безопасности предприятия.
23. Понятие адаптивных систем информационной безопасности и методы их моделирования.
24. Методика формирования базы знаний для адаптивных систем информационной безопасности с использованием средств искусственного интеллекта.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ОСНОВЫ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ»

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

– приобретение обучающимися знаний и представлений по проектированию технологий обеспечения информационной безопасности;

– приобретение обучающимися практических навыков и умений по применению современных технологий обеспечения информационной безопасности.

Задачи дисциплины:

– ознакомление обучающихся с основными методологическими подходами проектирования систем информационной безопасности предприятия;

– освоение обучаемыми основных методов определения параметров, характеристик и структуры системы информационной безопасности;

– формирование у обучаемых способности самостоятельно решать поставленные задачи в области проектирования систем информационной безопасности с помощью современных принципов, методов и средств в различных организационных структурах предприятий.

2. Указания по проведению практических занятий

Тема: Методология проектирования систем информационной безопасности предприятия.

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по методологии проектирования систем информационной безопасности.

Основные положения темы занятия:

1. Основные требования к системам проектирования, задачи и функции проектирования систем информационной безопасности предприятия.

2. Структура методологии проектирования, порядок выбора технологий и логика организации проектирования систем информационной безопасности предприятия.

Вопросы для обсуждения:

1. Определение структуры проектирования систем информационной безопасности предприятия.
2. Обеспечивающая часть структуры системы проектирования информационной безопасности.
3. Функциональная структура системы проектирования информационной безопасности.
4. Средства проектирования системы информационной безопасности предприятия.

Продолжительность занятия – 4 ч.

Тема: Особенности проектирования систем защиты информации предприятий.

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по особенностям проектирования систем защиты информации предприятий.

Основные положения темы занятия:

1. Методы формирования основных функций защиты и выбора средств защиты.

2. Проектирование основных подсистем и элементов системы защиты информационных объектов в соответствии с концепцией полной и эшелонированной защиты.

Вопросы для обсуждения:

1. Формирование требований к системе защиты объектов предприятия.
2. Особенности проектирования подсистем защиты охраняемых объектов.
3. Характеристика элементов классической системы обеспечения безопасности информационных объектов предприятия.
4. Пример организации информационной защиты ситуационного вычислительного центра, как типового объекта информационной безопасности объединеия предприятий.

Продолжительность занятия – 4 ч.

Тема: Основы моделирования систем информационной безопасности предприятия.

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по основам моделирования систем информационной безопасности.

Основные положения темы занятия:

1. Понятие модели информационной безопасности. Модель защиты различных информационных объектов, как модель системы с полным перекрытием.

2. Компьютерные модели оценки эффективности проектируемых систем информационной безопасности и порядок их применения.

Вопросы для обсуждения:

1. Характеристика семирубежной модели защиты информационных объектов предприятия и других моделей информационной безопасности.
2. Компьютерные модели, как инструменты количественного анализа проектируемых систем информационной безопасности и их оценки.
3. Методика применения инструментальных средств для анализа эффективности проектируемых систем информационной безопасности предприятий.

Продолжительность занятия – 8 ч.

Тема: Методика оценки эффективности проектируемых систем информационной безопасности.

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по оценке эффективности проектируемых систем информационной безопасности.

Основные положения темы занятия:

1. Особенности оценки экономической эффективности проектируемых систем информационной безопасности предприятия. Понятие надёжности проектируемых систем и её оценка.

2. Характеристика критериев и показателей эффективности для функций и элементов системы физической защиты охраняемых объектов, основные правила и процедуры их применения.

Вопросы для обсуждения:

1. Характеристика критериев и показателей оценки эффективности проектируемых систем информационной безопасности предприятия.
2. Методика оценки уязвимости проектируемых систем безопасности предприятия.
3. Основные подходы к управлению рисками и оценки рисков при проектировании.

Продолжительность занятия – 8 ч.

Тема: Особенности проектирования адаптивных систем информационной безопасности.

Практическое занятие 5.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по проектированию адаптивных систем информационной безопасности.

Основные положения темы занятия:

1. Особенности применения интеллектуальных средств для решения задач проектирования адаптивных систем информационной безопасности.

2. Диалоговая среда моделирования адаптивных систем информационной безопасности и методика её применения.

Вопросы для обсуждения:

1. Применение нейронных сетей при проектировании адаптивных систем информационной безопасности.
2. Выбор алгоритма обучения нейронных сетей на основе генетических алгоритмов и других инструментов искусственного интеллекта.
3. Интеллектуальные средства для решения задач классификации систем информационной безопасности предприятия и особенности их применения.
4. Гибридные средства классификации и комплементарность представления

информации в адаптивных системах информационной безопасности.

Продолжительность занятия – 8 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрен учебным планом.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить обучающихся к самостоятельному научному творчеству.

Задачи самостоятельной работы:

– расширить представление в области проектирования информационных технологий обеспечения информационной безопасности;

– систематизировать знания в области оценки предварительной защищённости информационных систем и применению методики их защиты;

– овладеть некоторыми навыками решения нетривиальных задач в области организации проектирования защищённых информационных систем и технологий.

Объём времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**112**
Вопросы, выносимые на самостоятельное изучение	48
Подготовка к практическим занятиям	32
Подготовка докладов	16
Выполнение практических заданий	16

Вопросы, выносимые на самостоятельное изучение:

1. Методология построения модели управления городом с использованием технологии “AS IS” (Как есть) и технологии “TO BE” (Как должно быть).
2. Основные цели формирования требований при построении организационной структуры предприятий и диаграмм потоков данных объектного уровня с внешними объектами.
3. Предназначение, состав и методика применения интегрированных систем управления предприятиями на основе управленческого стандарта CSRP.
4. Особенности появления, развития и перспективы дальнейшего применения систем управления взаимоотношениями с клиентами CRM-систем (Customer Relationship Management) в России и за рубежом.
5. Основные понятия, характеристики и методика применения OLAP-техноло-

гий (On-Line Analytical Processing) при проектировании информационных систем и защищённых технологий на предприятиях региона.
6. Особенности многомерного представления информации при описании структур данных, основные показатели гиперкуба.
7. Состав и основные характеристики операций манипулирования измерениями, обзор операций формирования среза, иерархических отношений, операций агрегации и вращения.
8. Методика проектирования многомерной базы данных для предприятий и реализация защитных механизмов в ней, порядок использования аналитических функций.
9. Концепция проектирования информационных систем на основе модельно-ориентированной технологии и особенности её применения.
10. Характеристика основных этапов выполнения работ при проектировании информационных систем по каскадной модели жизненных циклов на предприятии.
11. Методика проектирования адаптивных информационных и образовательных систем.
12. Характеристика основных методов и технических приёмов адаптивной гипермедиа.
13. Архитектура адаптивной системы управления информационными и образовательными ресурсами Xite.
14. Методика проектирования адаптивных систем защиты информации на основе использования интеллектуальных средств.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	48	Изучение открытых источников
2.	Подготовка к практическим занятиям	32	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Тематика докладов	16	1. Методология внедрения систем информационной безопасности в регионе на базе пакетированных решений и модельно-ориентированного проектирования. 2. Характеристика интегрированных систем управления предприятием, роль и место проектируемых систем информационной безопасности в деятельности современного холдинга. 3. Гибридные средства классифи-

			кации систем информационной безопасности и особенности их применения для представления знаний в информационном поле. 4. Методика оценки защищённости информационных систем и технологий с применением механизмов нечёткой логики и нейронных сетей.
4.	Выполнение практических заданий	16	1. Характеристика основных этапов выполнения работ при проектировании информационных систем по каскадной модели жизненных циклов на предприятии. 2. Особенности многомерного представления информации при описании структур данных, основные показатели гиперкуба. 3. Характеристика основных методов и технических приёмов адаптивной гипермедиа. 4. Состав и основные характеристики операций манипулирования измерениями, обзор операций формирования среза, иерархических отношений, операций агрегации и вращения.

Примерные темы докладов

1. Особенности применения спиральной модели жизненного цикла информационной системы и модели непрерывной разработки таких систем и технологий.
2. Методология проектирования прикладных информационных систем на основе инструментария Oracle CDM.
3. Особенности применения технологии Microsoft Solutions Framework (MSF) корпорации Microsoft для управления проектами разработки информационных систем уровня предприятия.
4. Обзор и особенности применения современных технологий и основных инструментов выработки решений руководителями различных рангов и структур.
5. Состав, основные характеристики и порядок применения малых, средних и крупных средств моделирования информационных систем различных предприятий.
6. Характеристика различных взглядов на применение инструментария Architecture of Integrated Information Systems (ARIS) для описания и проектирования основных бизнес-процессов на предприятии.
7. Особенности реализации CASE-технологий в среде Oracle Designer и других средствах создания и сопровождения прикладных систем.
8. Особенности построения функциональных моделей информационных сис-

тем и технологий на основе методологии IDEF0.
9. Особенности построения интегрированных функциональных моделей ин формационных систем предприятий с использованием пакета BPwin в рамках методологии структурного моделирования.
10. Основные характеристики и особенности применения методологии диаграммы потоков данных (DFD) в нетрадиционном синтаксисе и других визуальных эффектов.
11. Основные понятия и определения технологии создания баз данных логического и физического уровней, порядок их разработки с помощью автоматизированного инструментария.
12. Методология внедрения систем информационной безопасности на предприятии на базе пакетированных решений и модельно-ориентированного проектирования.

5. Указания по проведению контрольных работ

Не предусмотрены учебным планом.

6. Указания по проведению курсовых работ

Не предусмотрены учебным планом.

7. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. Учебное пособие. – М.: Горячая линия-Телеком, 2012.
2. Заботина Н.Н. Проектирование информационных систем. Учебное пособие. – М.: «ИНФРА-М», 2011.
3. Коваленко В.В. Проектирование информационных систем. Учебное пособие. – М.: ФОРУМ, 2012.

Дополнительная литература:

1. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. Учебное пособие. – СПб.: НИУ ИТМО, 2013.
2. Исаев Г.Н. Проектирование информационных систем. Учебное пособие. – М.: Издательство «Омега-Л», 2013.

Рекомендуемая литература:

1. Нестерук Г.Ф., Осовецкий Л.Г., Нестерук Ф.Г. О применении нейронечетких сетей в адаптивных системах информационной защиты // Нейроинформатика-2005: Матер. VII всерос. научно-техн. конф. – М.: МИФИ (ТУ), 2005.
2. Силаенков А.Н. Проектирование системы информационной безо-

пасности. Учебное пособие. – Омск: Издательство ОмГТУ, 2009.
3. Смирнова Г.Н. и др. Проектирование экономических информационных систем. Учебник / под редакцией Тельнова Ю.Ф. – М.: Финансы и статистика, 2003.
4. Тупота В.И. Адаптивные средства защиты информации в вычислительных сетях. Учебное пособие. – М.: Радио и связь, 2002.
5. Юдицкий С.А., Владиславлев П.Н. Основы предпроектного анализа организационных систем. Учебное пособие. – М.: Финансы и статистика, 2005.

Электронные книги:

1. Обеспечение безопасности персональных данных. Методическое пособие. Издательский дом «Афина», 2010: **www.inside-zi.ru**
2. Краткий энциклопедический словарь информационной безопасности. Издатель: Энергия, 2010: **www.biblioclub.ru**
3. ЭБС «Руконт»: **www.rucont.ru**

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – Научно-образовательный портал;
2. **www.wikIsec.ru** – Энциклопедия информационной безопасности. – Публикации, статьи;
3. **http://www.fsb.ru/** – Официальный сайт Федеральной службы безопасности РФ;
4. **http://www.fstec.ru/** – Официальный сайт Федеральной службы по техническому экспортному контролю РФ.

9. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice*.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Технологического Университета.
2. Рабочая программа и методическое обеспечение по дисциплине «Основы проектной деятельности».
3. Информационно – справочные (правовые) системы:
   – «Гарант» (**garantcenter.ru**);
   – «Кодекс» (**doskainfo.ru/advert/64804/**);
   – «Консультант +» (**artiks.ru**).