МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	И.о. заведующего кафедрой ИБ
_____И. М. Ажмухамедов	_____Т. Г. Гурская
«06» июня 2024 г.	от «06» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Экономика защиты информации

Составитель(-и):	**Меркулова А. М., старший преподаватель кафедры ИБ**
Направление подготовки	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2021**
Курс	**4**
Семестр	**7**

Астрахань, 2024 г.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цели освоения дисциплины (модуля): изучение основ экономики защиты информации, необходимых специалисту в области информационной безопасности, ознакомление с основными категориями экономической теории применительно к средствам обеспечения защиты информации на объектах информатизации.

1.2. Задачи освоения дисциплины (модуля):

- освоение основ экономической теории информационной безопасности, знакомство с научной терминологией, моделями и концепциями защиты прав на информатизацию государства, общества и личности с использованием экономических методов построения и оптимизации систем защиты информации;
- изучение основных положений экономической политики предприятий и организаций при финансировании затрат на защиту интеллектуальной собственности с учетом современных средств защиты информации и предпринимательского риска;
- применение экономических методов при построении, оценке эффективности и оптимизации систем информационной безопасности.

В результате изучения курса студенты должны:

Знать:

основные подходы к определению затрат на защиту информации, методы оценки эффективности систем защиты, обобщенную систему показателей-индикаторов экономической безопасности, методы экономической оценки ущерба от реализации угроз.

Уметь:

выявить возможные угрозы объекту защиты и провести их ранжирование, оценить возможный ущерб по каждому виду угроз, оценить вероятности возникновения каждой угрозы в течение определенного периода, выбрать способы защиты по каждому виду угроз и оценить их стоимость, сопоставлять стоимости защиты от конкретной угрозы с ущербом от реализации угрозы.

Владеть:

методами проведения расчетов экономических потерь от реализации угроз объекту защиты, методами оценки ущерба по каждому виду угроз, методами выявления состава потенциальных угроз объекту защиты.

Бакалавр, изучив дисциплину «Экономика защиты информации», может быть готов к следующему виду профессиональной деятельности и должен решать следующие профессиональные задачи:

- проектно-технологическая деятельность:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение предварительного технико-экономического обоснования проектных расчетов;
- экспериментально-исследовательская деятельность:
- проведение экспериментов по заданной методике, обработка и анализ их результатов.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Экономика защиты информации» относится части, формируемой участниками образовательных отношений и осваивается в 7 семестре

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки и (или) опыт деятельности, формируемые предшествующими учебными дисциплинами:

1. Математические основы информационных технологий и вычислительной техники.

В результате освоения этой дисциплины, студент должен:

Знать:

• основы математического анализа.

Уметь:

• применять современный математический инструментарий для решения содержательных экономических задач;

Владеть:

• современными методами сбора, обработки и анализа экономических и социальных данных,

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1.Аудит информационной безопасности.

Также дисциплина «Экономика защиты информации» поможет студентам при написании бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) универсальные компетенции:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

б) профессиональных (ПК):

ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
УК-9. .Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	ИУК-9.1. Знать: основные законы и закономерности функционирования экономики; основы экономической теории, необходимые для решения профессиональных и социальных задач.	ИУК-9.2. Уметь применять экономические знания при выполнении практических задач; принимать обоснованные экономические решения в различных областях жизнедеятельности.	ИУК-9.3. Владеть способностью использовать основные положения и методы экономических наук при решении социальных и профессиональных задач
ПК-4 Способен администрировать средства защиты информации в	ИПК-4.1. Знать: источники угроз информационной безопасности в	ИПК-4.2. Уметь: анализировать угрозы безопасности информации в	ИПК-4.3. Владеть навыками управления средствами межсетевого

компьютерных системах и сетях	компьютерных сетях и меры по их предотвращению; принципы функционирования программных средств криптографической защиты информации; виды политик управления доступом и информационными потоками в компьютерных сетях; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	компьютерных системах и сетях; настраивать правила обработки пакетов в компьютерных сетях; настраивать политики безопасности операционных систем, оценивать угрозы безопасности информации в компьютерных системах и сетях, противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем, настраивать антивирусные средства защиты информации в операционных системах	экранирования в компьютерных сетях методикой оценки оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет 4 зачетных единиц, в том числе 36 часов, выделенных на контактную работу обучающихся с преподавателем (из них 36 часов - лабораторные работы), и 108 часов – на самостоятельную работу обучающихся

Таблица 2. Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа(в часах)			Самост. работа		Формы текущего контроля успеваемости *(по неделям семестра).* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	Экономические проблемы информационных ресурсов	7	1-3			4		15	Отчет по лабораторной работе 1.
2	Основные подходы к определению	7	4-5			4		15	Отчет по лабораторной работе

	затрат на защиту информации								2. Контрольная работа 1.
3	Система ресурсообеспечения защиты информации и эффективность ее использования	7	6-7			4		15	Отчет по лабораторной работе 3.
4	Виды ущерба, наносимые информации	7	8-9			4		15	Отчет по лабораторной работе 4. Контрольная работа 2
5	Методы и способы страхования информации	7	10-11			4		15	Отчет по лабораторной работе 5.
6	Формирование бюджета службы защиты информации	7	12-13			4		15	Отчет по лабораторной работе 6.
7	Экономическая эффективность защиты информации	7	14-18			12		18	Контрольная работа 3. Выполнение задания самостоятельной работы. Итоговое тестирование.
ИТОГО		**144**				**36**		**108**	**Экзамен**

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3– Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции (указываются компетенции перечисленные в п.3)*		*Σ общее количество компетенций*
		УК–9	ПК–4	
Экономические проблемы информационных ресурсов	19	+	+	2
Основные подходы к определению затрат на защиту информации	19	+	+	2
Система ресурсообеспечения защиты информации и эффективность ее использования	19	+	+	2
Виды ущерба, наносимые информации	19	+	+	2
Методы и способы страхования информации	19	+	+	2

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции (указываются компетенции перечисленные в п.3)*		*Σ общее количество компетенций*
		УК–9	ПК–4	
Формирование бюджета службы защиты информации	19	+	+	2
Экономическая эффективность защиты информации	30	+	+	2
ИТОГО	**144**			

Содержание дисциплины

Тема 1. Экономические проблемы информационных ресурсов

Предмет и задачи курса. Современные технологии коммерческого распространения информации. «Информационный продукт» и его особенности. «Информационные услуги». Информационные ресурсы. Экономические проблемы информационных ресурсов. Основная причина возникновения понятия «экономическая безопасность». Информация как важнейший ресурс экономики. Информация как товар, цена информации. Наиболее вероятные угрозы. Виды классификации угроз. Обобщенная система показателей-индикаторов экономической безопасности.

Тема 2. Основные подходы к определению затрат на защиту информации

Основные методы определения затрат на информационную безопасность. Определение размера целесообразных затрат на обеспечение безопасности информации. Особенности ценообразования на информационные продукты. Оценка текущего уровня стоимости. Аудит информационной безопасности компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня стоимости владения. Формирование целевой модели совокупности стоимости владения.

Тема 3. Система ресурсообеспечения защиты информации и эффективность ее использования

Управление ресурсами в процессе защиты информации. Классификация предпринимательских рисков. Анализ и оценка риска. Способы минимизации риска.

Тема 4. Виды ущерба, наносимые информации

Виды ущерба, наносимые информации. Виды ущерба от несанкционированного доступа (НСД) к информации. Методы оценки ущерба от НСД. Степень наносимого ущерба информации.Экономическая оценка ущерба от реализации угроз.

Тема 5. Методы и способы страхования информации

Основные принципы защиты информации. Методы защиты информации. Страхование как метод защиты информации. Способы страхования информации.

Тема 6. Формирование бюджета службы защиты информации

Структура службы защиты информации. Расчет численности персонала службы защиты информации. Составляющие бюджета службы защиты информации.

Тема 7. Экономическая эффективность защиты информации

Критерии эффективности систем защиты информации». Методы оценки эффективности систем защиты. Основные положения определения экономической эффективности защиты информации. Оценка экономического эффекта защиты информации. Экономическая эффективность инвестиций в защиту информации. Инвестирование капитала. Основные

источники инвестиций. Объекты инвестирования. Структура инвестиций. Инвестиционный риск в деятельности информационного коммерсанта Финансовый анализ при создании и эксплуатации предприятий по производству и реализации коммерческой информации.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным (семинарским) занятиям необходимо воспользоваться учебно-методической литературой из п.8. Лекции (семинары) необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8, а также пользоваться ресурсами сети Интернет.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер раздела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
1	Подготовка к отчету по лабораторной работе 1.	15	Внеаудиторная, изучение учебных пособий
2	Подготовка к отчету по лабораторной работе 2. Подготовка к контрольной работе 1.	15	Внеаудиторная, изучение учебных пособий
3	Подготовка к отчету по лабораторной работе 3.	15	Внеаудиторная, изучение учебных пособий
4	Подготовка к отчету по лабораторной работе 4. Подготовка к контрольной работе 2	15	Внеаудиторная, изучение учебных пособий
5	Подготовка к отчету по лабораторной работе 5.	15	Внеаудиторная, изучение учебных пособий
6	Подготовка к отчету по лабораторной работе 6. Подготовка к контрольной работе 3	15	Внеаудиторная, изучение учебных пособий
7	Подготовка к итоговому тестированию, подготовка отчета по самостоятельной работе. Подготовка к зачету	18	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно - самостоятельная работа.

Задания для самостоятельной работы

Тема «Экономика и организация защиты от несанкционированного доступа и копирования программного продукта» (*возможные этапы выполнения*):

1. Выбрать объект защиты (если это предприятие, то указать оборот, численность персонала, рентабельность, прибыль).
2. Выявить возможные угрозы объекту защиты и провести их ранжирование (дельфийская процедура – экспертиза).
3. Оценить возможный ущерб по каждому виду угроз – (возможно получение групповой экспертной оценки величины ущерба с использованием дельфийской процедуры и имитационного моделирования).
4. Оценить вероятности возникновения каждой угрозы в течение определенного периода.
5. Оценить математическое ожидание суммарного ущерба.
6. Выбрать способы защиты по каждому виду угроз и оценить их стоимость. Определить последовательность действий по вскрытию системы защиты и оценить затраты времени на реализацию каждого действия (min, max, наиболее вероятное).
7. Сопоставить стоимости защиты от i-й угрозы с ущербом от реализации угрозы. При этом следует учитывать, что затраты на создание системы защиты не должны превышать 5-20% от величины возможного ущерба.
8. Выбрать отдельный элемент объекта защиты – ИС и оценить (условно или с опросом) экономические потери (ущерб) от несанкционированного доступа и от копирования.

Критерии оценки заданий самостоятельной работы:

– оценка «отлично» выставляется обучающемуся, если студент представил задание в соответствии с методическими указаниями, информация в задании сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент представил задание в соответствии с методическими указаниями, информация в задании сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил задание в соответствии с методическими указаниями, информация в задании сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил задание или выполнил ее неверно, без использования методических указаний, обоснования неверные, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут

использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	**Практическое занятие, семинар**	**Лабораторная работа**
Экономические проблемы информационных ресурсов	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Основные подходы к определению затрат на защиту информации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Система ресурсообеспечения защиты информации и эффективность ее использования	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Виды ущерба, наносимые информации	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Методы и способы страхования информации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Формирование бюджета службы защиты информации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Экономическая эффективность защиты информации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Экономика защиты информации» проверяется сформированность у

обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1.	Экономические проблемы информационных ресурсов	УК–9, ПК–4	Отчет по лабораторной работе 1.
2.	Основные подходы к определению затрат на защиту информации	УК–9, ПК–4	Отчет по лабораторной работе 2. Вопросы к контрольной работе 1
3.	Система ресурсообеспечения защиты информации и эффективность ее использования	УК–9, ПК–4	Отчет по лабораторной работе 3.
4.	Виды ущерба, наносимые информации	УК–9, ПК–4	Отчет по лабораторной работе 4. Вопросы к контрольной работе 2
5.	Методы и способы страхования информации	УК–9, ПК–4	Отчет по лабораторной работе 5.
6.	Формирование бюджета службы защиты информации	УК–9, ПК–4	Отчет по лабораторной работе 6. Вопросы к контрольной работе 3
7.	Экономическая эффективность защиты информации	УК–9, ПК–4	Выполнение задания самостоятельной работы Итоговое тестирование. Вопросы к зачету.

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить

	примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1: Экономические проблемы информационных ресурсов

Лабораторная работа №1

Анализ предприятия с точки зрения экономики защиты информации

Цель: изучить модель анализа предприятия с точки зрения экономики защиты информации, получить навыки построения организационных структур в различных приложениях - MS Office (инструментарий SmartArt) и в MS Visio.

Задачи:

1. Изучить виды организационных структур.
2. Описать деятельность выбранной организации.
3. Проанализировать, охарактеризовать и построить организационную структуру выбранной организации.
4. Охарактеризовать и описать все структурные единицы организации согласно организационной структуре (вид деятельности, обязанности, заработная плата).

Порядок выполнения лабораторной работы

1. Изучить существующие типы организационных систем (теоретическая часть)
2. Изучить процессы построения организационных систем в приложениях MS Office, Visio.
3. Провести анализ выбранной организации: вид деятельности, описание нюансов работы организации, организационная структура, функционал и заработная плата каждой организационной ячейки.
4. Оформление отчёта. Отчёт должен содержать титульный лист и основную часть, а именно:
- цель работы,
- описание выбранной организации по всем пунктам,
- построенная организационная структура с помощью описанных программных продуктов или любых других (на выбор студента).
- выводы по лабораторной работе (что было изучено, какие задачи решены и какие получены навыки практической работы).

Контрольные вопросы

1. Что такое организационная структура предприятия? Для чего необходимо разрабатывать организационную структуру?
2. Какие существуют типы организационных структур? Перечислите их преимущества и недостатки.
3. Проведите сравнительный анализ линейно-функциональной структуры управления и проектной? В каких видах бизнеса используются эти структуры?
4. Проведите сравнительный анализ матричной структуры управления и процессной? В каких видах бизнеса используются эти структуры?
5. Проведите сравнительный анализ процессов построения организационных структур в различных программных системах.
6. Какие особенности построения организационных структур в системах моделирования CA ERwin Process Modeler, ARIS и Business Studio?

Тема 2: Основные подходы к определению затрат на защиту информации

Лабораторная работа №2

Моделирование бизнес-процессов в организации

Цель: освоение навыков по моделированию бизнес-процессов конкретной организации.

Задание

1 Определить для каждого отдела или структурной единицы не менее 5 бизнес-процессов. Охарактеризовать их с точки зрения функции (управляющие, операционные, вспомогательные) – доказать, почему.

2 Описать каждый выделенный бизнес-процесс в виде элементарных действий, потоков данных и ролей в графическом виде.

3 Оформить в виде общего отчёта в электронном виде.

Контрольные вопросы

1 Что такое бизнес-процесс?
2 Какие бывают виды бизнес-процессов? Привести примеры, доказать.
3 Какие цели и задачи характеризуют моделирование бизнес-процессов?
4 Какие существуют методы моделирование? В чем их особенность?

Контрольная работа №1

Вопросы к контрольной работе

1. «Информационный продукт» и его особенности. «Информационные услуги».
2. Информационные ресурсы. Экономические проблемы информационных ресурсов.
3. Основная причина возникновения понятия «экономическая безопасность».
4. Информация как важнейший ресурс экономики. Информация как товар, цена информации.
5. Наиболее вероятные угрозы. Виды классификации угроз.
6. Обобщенная система показателей-индикаторов экономической безопасности.
7. Основные методы определения затрат на информационную безопасность.
8. Определение размера целесообразных затрат на обеспечение безопасности информации.
9. Особенности ценообразования на информационные продукты.
10. Оценка текущего уровня стоимости.
11. Аудит информационной безопасности компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня стоимости владения.
12. Формирование целевой модели совокупности стоимости владения.
13. Секретность в рыночной экономике – экономическая категория.
14. Интегральный показатель выбранного режима распространения информации.

Тема 3: Система ресурсообеспечения защиты информации и эффективность ее использования

Лабораторная работа №3

Расчет амортизационных отчислений

Цель: получить навык выполнения расчета амортизационных отчислений. Решить задачи по приведенным алгоритмам.

Порядок формирования индивидуального задания:

Выделенные ***жирным курсивом цифры*** увеличиваются на коэффициент,

соответствующий номеру студента по списку.

$$К = 1 + \frac{№}{100}$$

Если студент имеет порядковый №5, то К=1,05; Если №20, то 1,2, и.т.д.

Задача 1

Восстановительная стоимость станка ***65 тыс. руб***. Норма амортизации 10%. Станок отработал 3 года. Определить его остаточную стоимость (См. пример 1).

Задача 2

Первоначальная стоимость приобретенных токарных станков составляет ***15 млн. руб***. Норма амортизации 10%. Определить годовую сумму амортизационных отчислений. (См. пример 2).

Задача 3

Годовая программа выпуска предприятия 9 0000 штук изделий. Первоначальная стоимость станка, на котором выполняются работы, ***109500 рублей***. Норма амортизации 10%.

Определить амортизационные отчисления, включаемые в себестоимость единицы продукции. (См. пример 3).

Задача 4

Первоначальная стоимость оборудования ***210000 руб***. Норма амортизации 8%. Определить, по какой остаточной стоимости объект основных фондов будет реализован через 6 лет. (См. пример 4).

Задача 5

Первоначальная стоимость производственного здания ***70 млн. руб***. Норма амортизации 1%. Определить годовую сумму амортизационных отчислений и продолжительность амортизационного периода. (См. пример 5).

Задача 6

Организация приобрела транспортные средства стоимостью ***175 тыс. руб***. со сроком полезного использования 10 лет. Предполагаемый пробег 900 тыс. км. В отчетном периоде пробег составил 20 тыс. км.

Какова сумма начислений амортизации за отчетный период? (См. пример 6).

Задание

1. Описать и классифицировать основные средства вашей организации
2. Рассчитать для каждого основного средства амортизационные отчисления
3. Если основное средство подлежит ремонту, рассчитать норму отчислений в ремонтный фонд.

Контрольные вопросы

1. Определение основных фондов предприятия
2. Оценка основных фондов
3. Классификационные группы основных фондов
4. Виды износа основных фондов.
5. Что показывает норма амортизации?
6. Что такое амортизация, и на какие цели может использовать предприятие амортизационные отчисления?
7. Как определить амортизационный период?
8. Способы возмещения затрат на ремонт основных фондов
9. Какие существуют методы расчета амортизационных отчислений?

Тема 4: Виды ущерба, наносимые информации

Лабораторная работа №4

Модель определения объектов защиты в условиях независимости ущербов

Здесь можно рассмотреть предприятие, на котором различные отделы взаимосвязаны, и нарушение политики безопасности и защищенности информации в одном из подразделений делает невозможным ведение в полном объеме хозяйственной деятельности в другом отделе.

Целесообразно предположить, что нарушение работы одного из отделов возможно по причинам криминального характера. Например, в силу заинтересованности криминальных структур в ликвидации предприятия как наиболее опасного конкурента или хотя бы в утрате им конкурентных преимуществ.

Предполагается, что средства защиты j-го вида нейтрализуют j-ю стратегию криминальной структуры. Следовательно, ущерб звена объекта защиты будет rij = 0. В остальных случаях ущерб не зависит от того, выполнено ли мероприятие по защите отдельного звена объекта или нет. Для j-й стратегии криминальной структуры положим величину ущерба, который она причиняет предприятию, равной lj. Для удобства будем считать, что $l_1 > l_2 > \ldots > ln$. Кроме того, положим cj = 0. Такая ситуация характерна для моделей конфликтов, в которых затраты на защиту звена (блока) пренебрежимо малы по сравнению с возможным ущербом.

Пусть предприятие включает пять взаимосвязанных отделов, выход из строя одного из которых вследствие возможного повреждения информационной целостности приводит к простою всей производственной системы. Для предотвращения возможных повреждений и простоев производственной системы необходимо, чтобы была обеспечена защита информации в каждом из отделов. Расходы на предупреждение повреждения информационной целостности существенно меньше, чем убытки, которые причиняют всей производственной системе простои отделов предприятия.

Получение значений прямых и косвенных убытков возможно посредством проведения экспертных оценок.

Задание: определить стратегии поведения участника 1 (криминальная структура) и участника 2 (предприятие).

Контрольная работа № 2

Вопросы к контрольной работе

1. Система ресурсообеспечения защиты информации и эффективность ее использования
2. Управление ресурсами в процессе защиты информации.
3. Классификация предпринимательских рисков.
4. Анализ и оценка риска.
5. Способы минимизации риска.
6. Виды ущерба, наносимые информации.
7. Виды ущерба от несанкционированного доступа (НСД) к информации.
8. Методы оценки ущерба от НСД.
9. Степень наносимого ущерба информации.
10. Экономическая оценка ущерба от реализации угроз.

Тема 5: Методы и способы страхования информации

Лабораторная работа №5

Модель определения зон защиты предприятия в условиях ограниченности средств

Пусть одно из исследуемых предприятий, на котором имеется n защитных зон (объектов) и которое может подвергнуться нападению криминальных структур, располагает ограниченным количеством средств, которые могут использоваться для защиты только одной зоны (объекта). Ценность (полезность) зоны (объекта) может быть выражена, например, в ее (его) остаточной стоимости, стоимости хранящейся на складах продукции и составляет величину bi.

Тогда математическое ожидание ущерба, наносимого предприятию, при выборе различными сторонами зон (объектов) i и $j\ (i,j=\overline{1,n})$ можно рассчитать:

$$z_{ij}=\begin{cases} b_i(1-p), если\ i=j(i,j=\overline{1,n}) \\ b_i, если\ i\neq j(i,j=\overline{1,n}) \end{cases},$$

где p – вероятность неуничтожения (незащищенности) зоны (объекта), p>1.

Очевидно, что криминальная структура (участник 1) будет стремиться максимизировать величину zij, а предприятие (участник 2) – минимизировать ее, т.е. интересы сторон прямо противоположны и их взаимодействие составляет содержание антагонистического конфликта.

Задание: Максимальная месячная стоимость продукции и материальных ресурсов, хранимых на складах, составляет: b1 = 150, b2 = 120, b3 = 100 тыс. руб. (здесь b1 – стоимость готовой продукции на первом складе, а b2, b3 – стоимость материальных ресурсов на втором и третьем складах). Предполагается, что вероятность незащищенности объектов-складов составляет p = 50% = 0,5. Определить, 1) с какой вероятностью участник 2 (предприятие) должен защищать склад готовой продукции, второй объект (первый склад материальных ресурсов); 2) с какой вероятностью участник 1 должен угрожать складу готовой продукции, второму объекту (первому складу материальных ресурсов).

Тема 6: Формирование бюджета службы защиты информации

Лабораторная работа №6

Определение размера целесообразных затрат на обеспечение безопасности информации

Определить размер целесообразных затрат на обеспечение безопасности информации можно с помощью следующего подхода. Допустим, что для каждой из возможных неприятностей известны размеры и величины ущерба, если никакое противодействие не предпринимается (ситуация Ro, таблица 1). Величины ущерба в этом случае выписаны в первой строке матрицы. Индекс ноль означает, что неприятность не произошла. В первой колонке этой матрицы стоят затраты на противодействие данной неприятности при разном уровне противодействия. Индекс ноль в этом случае означает, что никаких затрат не производится (V11=0). Считается, что противодействие Ri способно предотвратить все неприятности Sj такие, что i >=j и совсем не способно уменьшить неприятность Sk при i < k.

Таблица 1

Платежная матрица производителя

Противодействие	Событие			
	S_0	S_1	S_2	S_3
R_0	V_{11}	V_{12}	V_{13}	V_{14}
R_1	V_{21}	V_{21}	$V_{21}+V_{13}$	$V_{21}+V_{14}$
R_2	V_{31}	V_{31}	V_{31}	$V_{31}+V_{14}$
R_3	V_{41}	V_{41}	V_{41}	V_{41}

В итоге величины затрат, элементы Vij матрицы, определяются по следующему правилу:

$$V_{ij} = \begin{cases} V_{1i}+V_{j1}, j>i \\ V_{i1}, j \le i \end{cases}$$

Первичный поверхностный анализ позволяет сделать некоторые выводы.

Пусть, например, финансовые возможности производителя ограничены, и он может организовать противодействие степени не больше, чем R2, в то время как ожидать надо неприятность степеней S3.. Из матрицы в таблице 1 видно, что затраты на какое-либо противодействие лишь увеличат потери производителя.

Другой исход имеет место, если подрядчик производителя готов выполнить работу лишь большого объема и высокой степени противодействия, например R3. Если можно ожидать неприятность не более, чем степени S1, то от бездействия ущерб будет меньше, чем от противодействия, которое доступно производителю. В том случае, когда у производителя есть возможность маневра, он обычно может выбирать и путь решения стоящей перед ним задачи.

Выбор способа минимизации затрат зависит от того, какова исходная информация о различных степенях неприятности.

Математическая модель задачи принятия решений определяется множеством состояний {Sj}, множеством стратегий (противодействий) {Ri} и матрицей возможных результатов ||Vij||.

В отдельных задачах рассматривается матрица рисков ||rij||. Риск – мера несоответствия между разными возможными результатами принятия определенных стратегий. Элементы матрицы рисков ||rij|| связаны с элементами платежной матрицы производителя в табл. 1 следующим соотношением:

$$r_{ij} = \begin{cases} \max\limits_i \{V_{ij}\} - V_{ij}, если V - выигрыш \\ V_{ij} - \min\limits_i \{V_{ij}\}, если V - затраты \end{cases}$$

Таким образом, риск – это разность между результатом, который можно получить, если знать действительное состояние внешней среды, и результатом, который будет получен при i-ой стратегии.

Для принятия решения в условиях неопределенности используется ряд критериев: критерий Лапласа, критерий Вальда, критерий Сэвиджа, критерий Гурвица.

Задание: используя перечисленные критерии, определить размер целесообразных затрат на обеспечение безопасности информации для выбранной организации.

Вопросы к контрольной работе 3

1. Основные принципы защиты информации.
2. Способы страхования информации.
3. Структура службы защиты информации. Расчет численности персонала службы защиты информации.
4. Составляющие бюджета службы защиты информации.
5. Критерии эффективности систем защиты информации»
6. Методы оценки эффективности систем защиты.
7. Основные положения определения экономической эффективности защиты информации. Оценка экономического эффекта защиты информации.
8. Экономическая эффективность инвестиций в защиту информации.
9. Инвестирование капитала. Основные источники инвестиций. Объекты инвестирования. Структура инвестиций.
10. Инвестиционный риск в деятельности информационного коммерсанта Финансовый анализ при создании и эксплуатации предприятий по производству и реализации коммерческой информации.

Тема 7: Экономическая эффективность защиты информации

Итоговый тест

1. **Информационными ресурсами являются:**

   А) формализованные идеи, различные данные, методы и средства их накопления, хранения и обмена между источниками и потребителями информации;

   Б) формализованные идеи, технологический процесс производственной системы;

   В) различные данные, методы и средства производства продуктов производственной системы;

   Г) различные данные, методы и средства накопления и хранения продуктов производства.

2. **Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) определяются как:**

   А) информационные процессы;
   Б) информационные системы;
   В) информационные ресурсы;
   Г) информационные технологии.

3. **Совокупность данных, сформированная их производителями для дальнейшего распространения, представляет собой:**

   А) информационную систему;
   Б) информационный продукт;
   В) производственный продукт;
   Г) нет правильного ответа.

4. **К функциям информационного бизнеса относят:**

   А) управление финансами и ведение учёта;
   Б) подготовку кадров и материально-техническое обеспечение;

В) производство и маркетинг

Г) варианты А, Б, В

5. На информационном рынке можно выделить следующих участников:

А) производители баз данных, интерактивные службы, пользователи;

Б) организации, осуществляющие интерактивный доступ к базам данных, шлюзы, или межсистемные интерфейсы, телекоммуникационные службы;

В) все варианты верны;

Г) нет правильного ответа

6. Для отечественного информационного рынка (для его становления и развития) важным является:

А) развитие коммутируемых служб, формирование спроса;

Б) наличие обычных шлюзов, называемых транзитными;

В) статус производителя баз данных

Г) варианты А, Б, В

7. Финансовые расчёты между производителями баз данных и интерактивными службами определяются двумя основными схемами расчётов:

А) арендной и кредитной;

Б) арендной и распределительной;

В) арендной и инвестиционной;

Г) распределительной и кредитной

8. При выборе данной схемы расчётов интерактивная служба платит производителю баз данных некоторую фиксированную сумму за право эксплуатации базы данных, забирая весь возможный доход:

А) арендной;

Б) кредитной;

В) распределительной;

Г) инвестиционной.

9. В зависимости от характера информационной деятельности различают следующие группы пользователей:

А) основные и промежуточные;

Б) главные и промежуточные;

В) текущие и конечные;

Г) промежуточные и конечные

10. Существующий сегодня рынок услуг (особенно отечественный рынок) ориентирован прежде всего на пользователей:

А) конечных;

Б) основных;

В) промежуточных;

Г) текущих

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;

- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.

- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.

- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;

- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Примерный план проведения лабораторно-практического занятия

1. Студенты распределяются по группам. Студентами выбирается одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.
2. Определяются принципы экономики защиты информации организации.
3. Формулируются основные задачи и мероприятия защите информации в организации.
4. Определяются проблемные вопросы, связанные с организацией защиты информации на предприятии по соответствующей теме занятия.
5. Каждой группе студентов выдаются задания (ситуации) и каждая из групп должна в роли руководителя, начальника службы безопасности, специалиста по защите информации и т.д. решать управленческие задачи, связанные с организацией защиты информации на предприятии (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
6. Студентами каждой группы обсуждаются вопросы с целью выработки общих позиций.
7. Руководителями каждой группы излагаются позиции по совершенствованию рекомендуемых мероприятий защиты информации
8. Подводятся итоги занятия с объявлением окончательных оценок участников занятия.

Для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (далее вместе – обучающиеся с ограниченными возможностями здоровья)

предусмотрена система обучения с использованием дистанционных образовательных технологий.

Критерии оценки лабораторных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам экономики.

Перечень вопросов к зачету

1. «Информационный продукт» и его особенности. «Информационные услуги».
2. Информационные ресурсы. Экономические проблемы информационных ресурсов.
3. Основная причина возникновения понятия «экономическая безопасность».
4. Информация как важнейший ресурс экономики. Информация как товар, цена информации.
5. Наиболее вероятные угрозы. Виды классификации угроз.
6. Обобщенная система показателей-индикаторов экономической безопасности.
7. Основные методы определения затрат на информационную безопасность.
8. Определение размера целесообразных затрат на обеспечение безопасности информации.
9. Особенности ценообразования на информационные продукты.
10. Оценка текущего уровня стоимости.
11. Аудит информационной безопасности компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня стоимости владения.
12. Формирование целевой модели совокупности стоимости владения.
13. Секретность в рыночной экономике – экономическая категория.
14. Интегральный показатель выбранного режима распространения информации.
11. Система ресурсообеспечения защиты информации и эффективность ее использования
12. Управление ресурсами в процессе защиты информации.
13. Классификация предпринимательских рисков.
14. Анализ и оценка риска.
15. Способы минимизации риска.
16. Виды ущерба, наносимые информации.
17. Виды ущерба от несанкционированного доступа (НСД) к информации.
18. Методы оценки ущерба от НСД.
19. Степень наносимого ущерба информации.
20. Экономическая оценка ущерба от реализации угроз.
11. Основные принципы защиты информации.

12. Способы страхования информации.
13. Структура службы защиты информации. Расчет численности персонала службы защиты информации.
14. Составляющие бюджета службы защиты информации.
15. Критерии эффективности систем защиты информации»
16. Методы оценки эффективности систем защиты.
17. Основные положения определения экономической эффективности защиты информации. Оценка экономического эффекта защиты информации.
18. Экономическая эффективность инвестиций в защиту информации.
19. Инвестирование капитала. Основные источники инвестиций. Объекты инвестирования. Структура инвестиций.
20. Инвестиционный риск в деятельности информационного коммерсанта Финансовый анализ при создании и эксплуатации предприятий по производству и реализации коммерческой информации.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности				
1.	Задание закрытого типа	Какие виды вкладов вы знаете? 1. Потребительский 2. Ипотечный 3. Срочный 4. Сверхсрочный 5. До востребования	3, 5	2
2.		Что такое Агентство по страхованию вкладов? 1. организация, которая отвечает за функционирование системы страхования банковских вкладов, в том числе обеспечивает осуществление страховых выплат при отзыве лицензии банка или его банкротстве 2. организация, осуществляющая надзор за деятельностью страховых компаний 3. банк, через который страховые компании выплачивают страховые возмещения клиентам 4. государственный орган, в задачи которого входит обеспечение устойчивости национальной валюты и платежной системы	1	2
3.		Прибыль банка – это: 1. Процент по кредитам 2. Процент по депозитам 3. Разница всех доходов и расходов	4	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		4. Разница между ставками процента по кредитам и депозитам		
4.		Срочные вклады в банковских учреждениях 1. могут быть сняты со счета после предварительного уведомления 2. служат для накопления денежных сбережений 3. используются для осуществления текущих расчетов 4. удобные для банковского прогнозирования	2	2
5.		К пассивным банковским операциям относится 1. предоставление ссуд 2. прием вкладов 3. операции с ценными бумагами 4. сделки с недвижимостью	2	2
6.	Задание открытого типа	Задачи, для решения которых используется оценка интеллектуальной собственности:	внесение и определение стоимости вклада в Уставной капитал предприятия; уступка прав на объект интеллектуальной собственности и выдача лицензий на их использование; определение стоимости лицензий на использование ОИС; приватизация или продажа бизнеса, в хозяйственной деятельности которого используются объекты интеллектуальной собственности и права на них; подготовка к переговорам с потенциальными партнерами, инвесторами и кредиторами; разрешение конфликтов в суде и определение размера ущерба от нарушения исключительных прав на объекты интеллектуальной собственности;	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			определение размеров авторского вознаграждения за создание и использование объекта интеллектуальной собственности; постановка нематериальных активов, включающих права интеллектуальной собственности, на баланс предприятия (введение ОИС в хозяйственный оборот).	
7.		Этапы расчета стоимости объектов интеллектуальной собственности (ОИС) методом освобождения от роялти	Расчет стоимости ОИС методом освобождения от роялти производится в несколько этапов: 1) составляется прогноз объема продаж, по которым ожидаются выплаты по роялти (учитывая жизненный цикл продукции); 2) определяется ставка роялти. Ставка роялти колеблется, как правило, в пределах 1-12%; 3) определяется экономический срок службы патента или лицензии; 4) рассчитываются ожидаемые выплаты по роялти как процент от прогнозируемого объема продаж; 5) из ожидаемых выплат по роялти вычитают все расходы, связанные с обеспечением патента или лицензии; 6) рассчитываются дисконтированные потоки прибыли от выплат по роялти; 7) определяются суммы текущих стоимостей потоков прибыли от выплат по роялти.	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
8.		Способы минимизации риска	К наиболее распространенным методам снижения риска на предприятии относятся следующие. 1. Избежание риска, то есть уклонение от сомнительных проектов, связанных с высоким риском, отказ от работы с ненадежными партнерами. 2. Страхование – представляет собой систему возмещения убытков страховщиками при наступлении страховых случаев из специальных фондов, формируемых за счет страховых взносов, уплачиваемых страхователями. 3. Самострахование – это создание специального резервного фонда (фонда риска) за счет отчислений на случай возникновения непредвиденной ситуации. 4. Диверсификация производственной деятельности (увеличение числа используемых или готовых к использованию технологий, расширению ассортимента выпускаемой продукции, ориентация на различные сегменты потребителей), рынка сбыта, закупок материалов – является эффективным способом снижения рисков и обретения экономической устойчивости и самостоятельности. 5. Хеджирование используется для минимизации рисков	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			снабжения в условиях высоких инфляционных ожиданий и отсутствия надежных каналов закупок.	
9.		Затраты на обеспечение должного качества информационных технологий и их соответствия требованиям стандартов включают в себя:	затраты на обеспечение соответствия требованиям качества информационных технологий; затраты на обеспечение соответствия принятым стандартам и требованиям достоверности информации, действенности средств защиты; затраты на доставку и обмен конфиденциальной информации; затраты на удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов.	2
10.		Затраты, возникающие в результате потери новаторства включают в себя:	затраты на проведение дополнительных исследований и разработки новой рыночной стратегии для предприятия в связи с отказом от организационных, научно-технических, коммерческих решений, ставших неэффективными в результате утечки сведений; затраты, возникшие из-за снижение приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.	2
ПК-4. Способен администрировать средства защиты информации в компьютерных				

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
системах и сетях безопасности				
1.	Задание закрытого типа	Совокупная стоимость затрат на создание (приобретение) программного продукта складывается из следующих составляющих: 1. Затраты на приобретение программных средств, 2. Затраты на внедрение, 3. Эксплуатационные затраты. 4. Затраты на материалы 5. Отчисления на социальные нужды	1, 2, 3	2
2.		Период времени, который начинается с момента принятия решения о необходимости создания программного продукта и заканчивается в момент его полного изъятия из эксплуатации 1. Жизненный цикл программного продукта 2. Круговорот программного продукта 3. Документооборот программного продукта 4. Жизненный процесс программного продукта	1	2
3.		Автоматизированное проектирование это 1. процесс постепенного приближения к выбору окончательного проектного решения 2. процесс проектирования, происходит при взаимодействии человека с компьютером 3. процесс проектирования осуществляется компьютером без участия человека 4. процесс проектирования, происходит без применения вычислительной техники	2	2
4.		Технико-экономические показатели сложной технической системы это 1. совокупность используемых для достижения эффекта финансовых, материальных, трудовых и временных ресурсов 2. изменение результатов процесса проектирования при замене	3	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		неавтоматизированного способа его исполнения автоматизированным 3. составляющие эффекта, имеют техническое и экономическое выражение 4. сопоставления эффекта от применения САПР и полных затрат на ее создание и эксплуатацию		
5.		Критерием оценки готовности является коэффициент готовности, который равен: 1. доле времени пребывания системы в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии 2. доле объема трафика системы в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии 3. количеству запросов в системе в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии 4. количеству отказов в системе в работоспособном состоянии и не может интерпретироваться как вероятность нахождения системы в работоспособном состоянии	1	2
6.	Задание открытого типа	Основные предметные области, представляющие интерес для коммерческой разведки	Основными предметными областями, представляющими интерес для коммерческой разведки, являются: показатели объема сбыта продукции, уровень прибыли, сведения о заказчиках, поставщиках, заключаемых сделках, маркетинговая политика конкурентов, деловая стратегия руководителей фирм-конкурентов, их личные качества; научно-исследовательские и конструкторские работы, технологические	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			процессы при производстве новой продукции, системы защиты информации конкурентов.	
7.		Что включают в себя затраты на ликвидацию последствий нарушения режима информационной безопасности?	Затраты на ликвидацию последствий нарушения режима информационной безопасности: затраты на восстановление системы безопасности до соответствия требованиям политики безопасности. затраты на приобретение новых технических средств; затраты на утилизацию пришедших в негодность ресурсов; затраты на восстановление баз данных и прочих информационных ресурсов; затраты на проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность; затраты на проведение дополнительных испытаний и проверок информационных систем; затраты на проведение расследований нарушений политики безопасности; затраты на юридические споры и выплаты компенсаций; затраты, возникшие вследствие разрыва деловых отношений с партнерами	2
8.		Что включают в себя затраты на обслуживание системы информационной безопасности?	Затраты на обслуживание системы информационной безопасности: затраты на осуществление	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			технической поддержки производственного персонала при внедрении средств защиты информации; затраты на организацию системы допуска исполнителей и сотрудников конфиденциального делопроизводства; затраты на обслуживание и настройку программно-технических средств защиты, операционных систем, сетевого оборудования; затраты на организацию безопасного использования информационных систем; затраты на обеспечение бесперебойной работы системы защиты информации.	
9.		Что может выступать в качестве объектов страхования, как одного из методов защиты информации	В качестве объектов страхования могут выступать: 1. Электронное оборудование разветвленных вычислительных, информационных систем; телекоммуникационных систем, систем связи и телефонии; систем хранения информации; систем бесперебойного питания; систем управления доступом и систем технической безопасности; другого подобного оборудования 2. Информационные ресурсы информация в любом виде (базы данных, библиотеки, архивы в электронной форме и	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			т.д.) программные средства и комплексы, находящиеся в разработке или эксплуатации. 3. Финансовые активы денежные средства в электронной форме в виде записей на счетах (системы клиент-банк); ценные бумаги в электронном виде.	
10.		Какие направления включает в себя деятельность по обеспечению экономической безопасности предприятия	Деятельность по обеспечению экономической безопасности предприятия включает в себя следующие направления: 1. Обоснование уровня приемлемого риска при принятии управленческих решений. Если потери можно заранее предвидеть и предусмотреть, то они должны рассматриваться как неизбежные расходы. Поэтому управление риском представляет собой прогнозную оценку возможных потерь ресурсов при наступлении неблагоприятных обстоятельств и отклонении от намеченной стратегии и разработку мер, направленных на их предотвращение и обеспечение экономической безопасности предприятия. 2. Разработку стратегии и тактики ведения производственно-хозяйственной деятельности, позволяющих минимизировать	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			хозяйственный риск и обеспечить экономическую безопасность. 3. Защиту материальных, финансовых и информационных ресурсов. Данное направление предусматривает предотвращение несанкционированного доступа к ресурсам предприятия, их использования не по назначению, хищения. 4. Защиту персонала. Люди являются наиболее слабым звеном в обеспечении безопасности, например, в системе защиты коммерческой тайны. Данное направление предусматривает охрану персонала от преступных посягательств, обеспечение нормальных условий для эффективной работы персонала, стимулирование персонала в поиске эффективных решений	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;

- неполный ответ для теоретический заданий;

- небрежное выполнение;

- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Критерии оценки зачета:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам экономики.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине отводится 100 баллов (90 баллов на текущие формы контроля и до 10 баллов отводится на бонусы), которые накапливаются студентом в течение всего семестра изучения дисциплины.

Оценивание студентов на зачете осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий/ баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	6/10	60	По расписанию
2.	*Выполнение контрольной работы*	2/5	10	
3.	*Тест*	1/10	10	
4.	*Выполнение самостоятельной работы*	1/10	10	
Всего			**90**	-
Блок бонусов				
5.	*Посещение занятий без пропусков*	1	3	
6.	*Своевременное выполнение всех заданий*	1	3	
7.	*Активность студента на занятии*	1	4	
Всего			**10**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2

Показатель	Балл
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Экономика и управление производством [Электронный ресурс] : учеб. пособие / Богомолова И.П., Филатова М.В., Слепокурова Ю.И. Лебедева Л.В., Стукало О.Г., Струков Г.Н., Черников В.В. - Воронеж : ВГУИТ, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785000321553.html. ЭБС «Консультант студента»).
2. Репин, В.В. Бизнес-процессы. Моделирование, внедрение, управление. - 2-е изд. - М. : Манн, Иванов и Фербер, 2014. - 512 с. - ISBN 978-5-91657-907-9: 1498-20 : 1498-20. (25 экз.)
3. Риск-менеджмент [Электронный ресурс] : Учебник для бакалавров / А. Н. Фомичев. - 4-е изд. - М. : Дашков и К, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785394026768.html ЭБС «Консультант студента»).
4. Бизнес-безопасность / И.Н. Кузнецов. - 4-е изд. - М. : Дашков и К, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785394026546.html ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб.пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ; стер. - М. : Академия, 2009. – 336 с. (45 экз.)

2. Защита предпринимательства (экономическая и информационная безопасность) : учебное пособие / Одинцов А.А. - М. : Международные отношения, 2003. - URL: http://www.studentlibrary.ru/book/ISBN5713311694.html ЭБС «Консультант студента»).

3. Математические основы теории риска : Учебн. пособ. / Королев В.Ю., Бенинг В.Е., Шоргин С.Я. - 2-е изд., перераб. и доп. - М. : ФИЗМАТЛИТ, 2011. - http://www.studentlibrary.ru/book/ISBN9785922112673.html ЭБС «Консультант студента»).

4. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М. : ЦИПСиР, 2011. - http://www.studentlibrary.ru/book/ISBN9785961413649.html ЭБС «Консультант студента»).

5. Основы организационного обеспечения информационной безопасности объектов информатизации : Доп. УМО по образованию в области ИБ качестве учеб. пособ. по специальностям в области ИБ / С.Н. Семкин [и др.].. : Гелиос АРВ, 2005. - 192 с. (55 экз.)

6. Основы информационного менеджмента : учеб. пособие / А.В. Костров. - 2-е изд., перераб. и доп. - М. : Финансы и статистика, 2009. - URL: http://www.studentlibrary.ru/book/ISBN9785279030200.html ЭБС «Консультант студента»).

7. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А. - М. : ДМК Пресс, 2004. - (Информационные технологии для инженеров). - URL: http://www.studentlibrary.ru/book/ISBN5940742467.html ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).