



Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ
СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»

И.о. проректора

А.В. Троицкий

« » 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б.1.Б.15.08 «ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Фоминых М.С. Рабочая программа дисциплины: «Экономика информационной безопасности». – Королев МО: «Технологический университет», 2023.

Рецензент: Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО



Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

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

Целью изучения дисциплины является:

1. Привития у обучаемых необходимых знаний и навыков по определению характера влияния мероприятий по защите информации на экономику предприятий и умения рассчитать основные параметры, определяющие экономические эффекты от проводимых мероприятий по информационной безопасности.

2. Вместе с тем, в условиях рынка успешное функционирование любой масштабной информационной системы возможно только на стабильной финансово-экономической базе.

3. В процессе обучения студент приобретает и совершенствует следующие компетенции.

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

ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Основными задачами дисциплины являются:

Следует считать получение студентами системы знаний об экономической безопасности государства, отдельных организаций (предприятий) и показать существующие проблемы экономической оценки проводимых мер по защите информации, в частности:

1. основные подходы к определению экономического ущерба, наносимого защищаемой информации (ресурсу), и определять ожидаемые затраты на ее защиту;
2. определение экономической эффективности защиты информации от реализации выделенных инвестиций в защиту информации;
3. использование механизма страхования защищаемого информационного ресурса как способа экономической защиты информации.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- понимает базовые принципы функционирования экономики и экономического развития, цели формы участия государства в экономике;

- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности
- знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности
- знает как проводится анализ журналов событий средств защиты информации
- знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями
- знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники
- знает основы нормативно-правовых актов в области защиты информации конфиденциального характера
- знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем
- знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации
- знает отечественные и зарубежные стандарты в области информационной безопасности
- знает как разрабатывать технические задания на создание подсистем информационной безопасности открытых информационных систем
- знает правовые нормы, инструкции и стандарты в области организации документооборота
- знает правовые основы организации защиты государственной тайны и конфиденциальной информации
- знает стандарты и критерии в области аудита ИБ
- знает требования законодательства по обеспечению безопасности персональных данных
- знает как составляются политики информационной безопасности в информационной системе персональных данных
- знает принципы организации процесса аудита
- знает теоретическую базу разработки политик безопасности
- знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы
- знает принципы администрирования подсистем информационной безопасности
- знает порядок аттестации объектов информатизации
- знает порядок проведения сертификационных испытаний средств защиты информации

Необходимые умения:

- применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами

(личным бюджетом), контролирует собственные экономические и финансовые риски

- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности.

- умеет реагировать на инциденты информационной безопасности

- умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов

- умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите

- умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов

- умеет разрабатывать инструкции по организации защищённого документооборота и контролировать их исполнение

- умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности

- умеет определять объекты аудита, критерии и область их действия

- умеет применять инструментальные средства мониторинга и аудита безопасности

- умеет составлять программу аудита ИБ

- умеет разрабатывать методики анализа рисков

- умеет собирать и анализировать свидетельства аудита

- умеет формализовать задачи анализа безопасности информационных систем

Трудовые действия:

- умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;

- умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.

- владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ

- владеет навыками сравнения и анализа существующих средств защиты информации

- владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы

- владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации

- владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ

- владеет навыками проведения лицензирования в области защиты информации

- владеет навыками работы с нормативно-правовыми актами

- владеет навыками составления отчётов по результатам выполненного аудита
- владеет навыками проведения аудита ИБ со сбором данных
- владеет навыками по формулированию выводов и заключения по полученным результатам
- владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Экономика информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Экономическая теория», «Основы права», «История», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)» и компетенциях: УК-5,9; ОПК-1,5,6,8,12,13; ДОПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

Таблица 1

Виды занятий	Всего часов	Семестр А	Семестр 8	Семестр ...	Семестр Р ...
Общая трудоемкость	144	144	144		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48		48		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	36		36		
Лабораторные работы (ЛР)	-		-		
Самостоятельная работа	88		60		
Другие виды контактной работы	12		12		
Практическая подготовка	нет		нет		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	T1; T2		T1; T2		
Вид итогового контроля	Экзамен		Экзамен		
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	24	24			
Лекции (Л)	12	12			
Практические занятия (ПЗ)	12	12			
Лабораторные работы (ЛР)					
Другие виды контактной работы	12	12			
Самостоятельная работа	118	118			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Практическая подготовка	8	8			
Вид итогового контроля	Экзамен	Экзамен			

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное/очно-заочное	Практические занятия, час Очное/очно-заочное	Занятия в интерактивной форме, час	Код компетенций
Раздел 1. Экономические основы защиты информации				
Тема 1. Введение в дисциплину и экономические проблемы защиты информационных ресурсов	1/0.5	2/1	-/1	УК-9;
Тема 2. Информация как товар и ее стоимость	0.5/0.5	2/0.5	0.5/1	УК-9;
Тема 3. Анализ экономической информации и целесообразность ее защиты	1/0.5	2/1	0.5/1	УК-9;
Тема 4. Основы экономической безопасности (информационный аспект)	1/0.5	2/1	0.5/1	УК-9;
Тема 5. Взаимозависимость экономической и информационной безопасностей	1/0.5	2/1	0.5/1	ДОПК-2
Тема 6. Бюджетирование деятельности службы информационной безопасности (защиты информации)	0.5/0.5	2/0.5	0.5/1	ДОПК-2
Тема 7. Информационные риски и их страхование	1/0.5	2/1	-/1.5	ДОПК-2
Раздел 2. Экономическая оценка				

эффективности защиты информации				
Тема 8. Основные положения экономической эффективности защиты информации	1/0.5	2/1	0.5/0.5	ОК-8;ПК-14
Тема 9. Методы оценки экономической эффективности защиты информации	1/0.5	2/1	0.5/0.5	ДОПК-2
Тема 10. Оценка экономических затрат на защиту информации	1/0.5	2/1	-/0.5	ДОПК-3
Тема 11. Экономическая эффективность инвестиций в защиту информации	0.5/0.5	2/0.5	-/0.5	ДОПК-3
Тема 12. Оценка и управление информационными рисками	0.5/0.5	2/0.5	0.5/0.5	ДОПК-3
Тема 13. Оценка защиты интеллектуальной собственности	0.5/0.5	3/0.5	0.5/0.5	ДОПК-4
Тема 14. Оценка предпринимательских информационных рисков (информационная защита бизнес-процессов)	0.5/0.5	3/0.5	0.5/0.5	ДОПК,4
Тема 15. Экономическая оценка эффективности отдельных	0.5/0.5	3/0.5	0.5/0.5	ДОПК-4

подсистем защиты информации				
Тема 16. Интегральная экономическая оценка эффективности комплексной системы защиты информации	0.5/0.5	3/0.5	0.5/0.5	УК-9; ДОПК-2,3,4
Итого:	12/12	36/12	6/12	

4.2. Содержание тем дисциплины

Раздел 1. Экономические основы защиты информации

Тема 1. Введение в дисциплину и экономические проблемы защиты информационных ресурсов

Значение, предмет изучения и краткое содержание курса "Экономика защита информации". Место дисциплины среди других курсов, изучаемых студентами. Методы изучения дисциплины. Названия тем, распределение их по видам аудиторных занятий. Форма проверки знаний. Научная, учебная и периодическая литература по предмету. Знания и умения, которые должны быть приобретены студентами в процессе изучения дисциплины. Раскрытие основных экономических понятий применительно к изучению курса. Законодательные акты, регулирующие экономические вопросы защиты информации.

Структура и факторы общественного производства. Место информации в структуре общественного производства.

Информация как фактор производства и как важнейший ресурс экономики. Влияние развития рыночной экономики на информационные ресурсы.

Тема 2. Информация как товар и ее стоимость

Информация как товар, цена информации. Основные характеристики продукта как товара. Классификация товаров. Особенности товара "информация".

Стоимость товара, принципы ее определения. Составляющие стоимости информационных массивов. Стоимостные оценки результатов интеллектуального труда.

Цена как денежное выражение стоимости товара. Формирование цены на информацию в рыночных условиях. Методы установления цен на информацию.

Тема 3. Анализ экономической информации и целесообразность ее защиты

Понятие, состав и характеристика экономической информации как объекта информационной безопасности. Экономические информационные системы и технологии обработки экономической информации.

Необходимость обеспечения защиты экономической информации.

Тема 4. Основы экономической безопасности (информационный аспект)

Понятие об экономической безопасности государства, общества, личности. Рассмотрение и решение проблем экономической безопасности в России в экономических реформах. Нормативные основы обеспечения экономической безопасности. Основные определения понятий в области экономической безопасности.

Уровни, объекты и методы обеспечения экономической безопасности. Обеспечение экономической безопасности предприятия в рыночных условиях.

Тема 5. Взаимозависимость экономической и информационной безопасностей

Экономические аспекты в информационной безопасности. Общность объектов защиты, угроз и уязвимостей.

Силы и средства информационного противоборства в экономической сфере.

Служба безопасности предприятия и ее функции по экономической и информационной безопасности

Тема 6. Бюджетирование деятельности службы информационной безопасности (защиты информации)

Понятия бюджетирования.

Функции и этапы разработки системы бюджетирования.

Базовые составляющие бюджетирования.

Виды и контроль бюджетирования.

Тема 7. Информационные риски и их страхование

Понятие об информационных рисках и их страховании.

Содержание процесса страхования. Преимущества страхования.

Сущность страхования как метода защиты информации. Принципы страхования информационного ресурса. Виды страхования. Последовательность работ службы защиты информации по реализации страхования информационного ресурса.

Характеристика видов страхования: имущества, ответственности и личное страхование.

Раздел 2. Экономическая оценка эффективности защиты информации

Тема 8. Основные положения экономической эффективности защиты информации

Общий подход к оценке эффективности защиты и страхования информации. Понятие "эффективность"; абсолютная и относительная эффективность. Закон РФ № 149 от 09.08.2006 г. «Об информации, информационных технологиях и защите информации» об экономических задачах защиты информации. Предотвращение ущерба как главная экономическая задача защиты и страхования информации.

Виды ущерба, наносимого информации. Методы оценки степени наносимого информации ущерба. Основные факторы, влияющие на величину ущерба, наносимого владельцу информации вследствие отсутствия или недостаточности ее защиты.

Методы обеспечения сопоставимости расчетных величин при определении эффективности защиты информации. Приведение разновременных результатов и затрат к расчетному году; дисконтирование.

Тема 9. Методы оценки экономической эффективности защиты информации

Существующие методические основы экономической оценки эффективности защиты информации: российские и международные подходы.

Общая характеристика российских подходов оценки экономической эффективности защиты информации: определение экономических затрат на защиту информации и расчет снижения ожидаемых экономических потерь от проводимых мер по защите информации.

Общая характеристика международных подходов оценки экономической эффективности защиты информации: определение совокупной

стоимости владения (сравнительный анализ затрат на защиту информации); оценка возврата инвестиций, выделяемых на защиту информации; оценка и управление информационными рисками.

Тема 10. Оценка экономических затрат на защиту информации

Обзор существующих методов оценки затрат на защиту информации.
Виды затрат на обеспечение информационной безопасности.

Основные положения методики определения затрат на основе метода совокупной стоимости владения (сравнительная оценка экономических расходов, выделенных на защиту информации).

Тема 11. Экономическая эффективность инвестиций в защиту информации

Общие положения об инвестициях, выделяемых на обеспечение информационной безопасности. Обзор существующих методов оценки возврата инвестиций, выделенных на защиту информации (международный опыт).

Основные положения методики оценки инвестиций в защиту информации на основе использования понятия «чистой текущей стоимости» с определением срока окупаемости проводимых мероприятий по защите информации.

Тема 12. Оценка и управление информационными рисками

Анализ, оценка и управления информационными рисками в экономической деятельности предприятия.

Предпринимательский информационный риск и его минимизация.

Управления информационными рисками на различных стадиях жизненного цикла систем защиты информации. Выбор допустимого уровня информационных рисков.

Инструментальные средства оценки информационных рисков.

Тема 13. Оценка защиты интеллектуальной собственности

Понятие интеллектуальная собственность и основы ее защиты.

Существующие методические подходы к экономической оценки защиты интеллектуальной собственности.

Общая характеристика методов оценки эффективности защиты интеллектуальной собственности. Основы методик расчетов упущенной выгоды (наносимого ущерба) в случае нарушения защиты интеллектуальной собственности. Общий подход оценки объектов интеллектуальной собственности и возможных убытков от противоправного их использования

(мировая практика). Частый подход оценки состояния защиты объектов интеллектуальной собственности предприятия (на основе частного функционального критерия защиты интеллектуальной собственности и оценки уровня интеллектуальной защищенности предприятия).

Тема 14. Оценка предпринимательских информационных рисков (информационная защита бизнес-процессов)

Предпринимательская деятельность с позиции защиты экономической информации. Понятие стратегии по безопасности предприятия: стратегии экономической и информационной безопасности. Требуемые уровни (вероятности) защиты экономической информации.

Стратегии экономического развития предприятия. Бизнес-план предприятия как потребитель и источник экономической информации, подлежащей защите.

Технико-экономические задачи по защите информации на предприятии и структура экономических расходов на их реализацию.

Процессно-ориентированный комплексный подход оценки защиты бизнес-процессов как совокупность частных (технического и экономического) подходов.

Тема 15. Экономическая оценка эффективности отдельных подсистем защиты информации

Определение и характеристика отдельных основных подсистем защиты экономической информации на предприятии: пожарной, физической (охранной), компьютерной и инженерно-технической подсистем защиты информационных объектов (ресурса).

Методика расчета экономического риска подсистемы пожарной защиты информационного объекта (ресурса).

Методика расчета экономического риска подсистемы физической (охранной) защиты информационного объекта (ресурса).

Методика расчета экономического риска подсистемы компьютерной безопасности информационного объекта (ресурса).

Тема 16. Интегральная экономическая оценка эффективности комплексной системы защиты информации

Определение и характеристика понятия интегральной оценки экономического ущерба из-за реализации возможных информационных угроз безопасности предприятия.

Методы экономической оценки эффективности систем комплексной безопасности информационных объектов (ресурса).

Основы экономических расчетов по оценке полученной выгоды (прибыли) и упущенной выгоды (недополученной прибыли) в комплексных системах защиты информации на предприятии.

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Экономика информационной безопасности» приведена в Приложении 1.

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

Основная литература:

1. Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/103198> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
2. Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/256274> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3. Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/171525> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
4. Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223223> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5. Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223304> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
6. Малышева Е.Н. Экспертные системы/Издательство: КемГУКИ (Кемеровский государственный университет культуры и искусств), 2010. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7
7. Информационные технологии и системы: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 352 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0376-6
8. Экспертные системы САПР: учебное пособие / А.Л. Ездаков. - М.: ИД ФОРУМ, 2012. - 160 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0398-8
9. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2004.
10. Квашнина Г. А. Донозологический мониторинг комплексной оценки управления адаптивного состояния субъекта в условиях экстремальной ситуации: монография / Г. А. Квашнина, Я. О. Мун. Воронеж: ВГТУ, 2008. 150 с.

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

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. <http://www.academy.it.ru/> – академия АЙТИ.

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. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

**Фонд оценочных средств для проведения промежуточной аттестации
обучающихся по дисциплине (модулю)**

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

«ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Квалификация (степень) выпускника: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции (В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Тема:1,4.5,6,7,9,10,11	- умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений; - умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.	- применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски	- понимает базовые принципы функционирования экономики и экономического развития, цели формы участия государства в экономике;
2.	ДОП К-2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его	Тема:2,4,,6,,9,11,12,13,14,15,16	- владеет навыками классификации информационных систем и средств вычислительной техники по	- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать	- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности - знает принципы

		<p>информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;</p>		<p>требованиям регуляторов ИБ</p> <ul style="list-style-type: none"> - владеет навыками сравнения и анализа существующих средств защиты информации - владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы - владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации 	<p>предложения по совершенствованию структуры мер и повышению эффективности.</p> <ul style="list-style-type: none"> - умеет реагировать на инциденты информационной безопасности - умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями и руководящих документов - умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите 	<p>разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности</p> <ul style="list-style-type: none"> - знает как проводится анализ журналов событий средств защиты информации - знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями - знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники - знает основы нормативно-правовых актов в области защиты информации конфиденциального характера - знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем
--	--	--	--	---	---	---

3	ДОП К-3	Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	Тема:2,4,,б,, 9,11,12,13,14 ,15,16	- владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ - владеет навыками проведения лицензирования в области защиты информации - владеет навыками работы с нормативно-правовыми актами	- умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями и нормативных документов - умеет разрабатывать инструкции по организации защищённого документооборота и контролировать их исполнение - умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности	- знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации - знает отечественные и зарубежные стандарты в области информационно й безопасности - знает как разрабатывать технические задания на создание подсистем информационно й безопасности открытых информационных систем - знает правовые нормы, инструкции и стандарты в области организации документооборота - знает правовые основы организации защиты государственной тайны и конфиденциальной информации - знает как разрабатывать проекты нормативных материалов,
---	------------	--	--	---	---	--

						<p>регламентирующ их работу по защите информации</p> <ul style="list-style-type: none"> - знает актуальные нормативно-правовые акты и методические документы в области обеспечения информационно й безопасности персональных данных - знает правовые основы организации защиты государственной тайны и конфиденциальн ой информации, задачи органов защиты государственной тайны в соответствии с доктриной ИБ РФ
4	ДОПК-4	Способен проводить аудит защищенност и объекта информатизац ии в соответствии с нормативным и документами	Тема:2,4,,6,,9,11,12,13,14,15,16	<ul style="list-style-type: none"> - владе ет навыками составления отчётов по результатам выполненно го аудита - владе ет навыками проведения аудита ИБ со сбором данных - владе ет навыками по 	<ul style="list-style-type: none"> - умеет определять объекты аудита, критерии и область их действия - умеет применять инструмента льные средства мониторинга и аудита безопасност и - умеет составлять 	<ul style="list-style-type: none"> - знает стандарты и критерии в области аудита ИБ - знает требования законодательств а по обеспечению безопасности персональных данных - знает как составляются политики информационно й безопасности в информационно

				<p>формулированию выводов и заключения по полученным результатам</p> <p>- владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем</p>	<p>программу аудита ИБ</p> <p>- умеет разрабатывать методики анализа рисков</p> <p>- умеет собирать и анализировать свидетельства аудита</p> <p>- умеет формализовать задачи анализа безопасности информационных систем</p>	<p>в системе персональных данных</p> <p>- знает принципы организации процесса аудита</p> <p>- знает теоретическую базу разработки политик безопасности</p> <p>- знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы</p> <p>- знает принципы администрирования подсистем информационной безопасности</p> <p>- знает порядок аттестации объектов информатизации</p> <p>- знает порядок проведения сертификационных испытаний средств защиты информации</p>
--	--	--	--	--	---	---

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

Код компетенции	Инструмент, оценивающий сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
УК-9; ДОПК-2,3,4	Доклад	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; <p>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</p>	<p>Например: Проводится в письменной и/или устной форме. Критерии оценки:</p> <ol style="list-style-type: none"> 1. Соответствие содержания доклада 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 тематике (1 балл). <p>Максимальная сумма баллов - 5 баллов.</p>
УК-9; ДОПК-2,3,4	Выполнение контрольной работы	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; <p>В) не сформирована (компетенция <u>не</u></p>	<p>При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида</p>

		<i>сформирована) – 2 и менее баллов</i>	
--	--	---	--

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. Техничко-экономические задачи по защите информации на предприятии и структура экономических расходов на их реализацию.
2. Процессно-ориентированный комплексный подход оценки защиты бизнес-процессов как совокупность частных (технического и экономического) подходов.
3. Определение и характеристика отдельных основных подсистем защиты экономической информации на предприятии: пожарной, физической (охранной), компьютерной и инженерно-технической подсистем защиты информационных объектов (ресурса).
4. Методика расчета экономического риска подсистемы пожарной защиты информационного объекта (ресурса).
5. Методика расчета экономического риска подсистемы физической (охранной) защиты информационного объекта (ресурса).
6. Методика расчета экономического риска подсистемы компьютерной безопасности информационного объекта (ресурса).
7. Определение и характеристика понятия интегральной оценки экономического ущерба из-за реализации возможных информационных угроз безопасности предприятия.
8. Методы экономической оценки эффективности систем комплексной безопасности информационных объектов (ресурса).
9. Основы экономических расчетов по оценке полученной выгоды (прибыли в комплексных системах защиты информации на предприятии).
10. Основы экономических расчетов по оценке упущенной выгоды (недополученной прибыли) в комплексных системах защиты информации на предприятии.

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

Формой контроля знаний по дисциплине «Экономика информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оцениваемых знаний, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	УК-9; ДОПК-2,3,4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.</i>
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	УК-9; ДОПК-2,3,4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.</i>
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	Зачет	УК-9; ДОПК-2,3,4	2 теоретических вопроса	экзамен проводится	Результаты предоставляются	Критерии оценки: «Отлично»:

<p>овленные графики образовательного процесса</p>			<p>+ практическое задание</p>	<p>письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.</p>	<p>яются в день проведения экзамена</p>	<ul style="list-style-type: none"> • 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. <p>«Хорошо»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание <p>«Удовлетворительно»:</p> <ul style="list-style-type: none"> • демонстриру
---	--	--	-------------------------------	--	---	---

						<p>ет частичные знания по темам дисциплин;</p> <ul style="list-style-type: none"> • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; <p>«Неудовлетворительно»:</p> <ul style="list-style-type: none"> • 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.
--	--	--	--	--	--	--

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Вопрос №1. Принципы защиты информации можно разделить на (выберите лишнее):
 - -экономические
 - -правовые
 - -организационные

-используемые при защите информации от технических средств разведки и в средствах вычислительной техники

2. Вопрос №2. К основным правовым принципам защиты информации НЕ относится:

- -принцип приоритета международного права над внутригосударственным
- -принцип законности
- -принцип персональной ответственности
- -принцип собственности и экономической целесообразности

3. Вопрос №3. Персональная ответственность за сохранность доверенных секретов относится к

- -правовым принципам
- -организационным принципам
- -техническим принципам
- - другим принципам защиты информации.

1.2. Типовые вопросы, выносимые на экзамен

1. Структура и факторы общественного производства.
2. Место информации в структуре общественного производства.
3. Информация как фактор производства и как важнейший ресурс экономики.
4. Влияние развития рыночной экономики на информационные ресурсы.
5. Информация как товар, цена информации.
6. Основные характеристики продукта как товара. Классификация товаров. Особенности товара "информация".
7. Стоимость товара, принципы ее определения. Составляющие стоимости информационных массивов.
8. Стоимость оценки результатов интеллектуального труда.
9. Цена как денежное выражение стоимости товара. Формирование цены на информацию в рыночных условиях. Методы установления цен на информацию.
10. Понятие, состав и характеристика экономической информации как

- объекта информационной безопасности.
11. Экономические информационной системы и технологии обработки экономической информации.
 12. Необходимость обеспечения защиты экономической информации.
 13. Понятие об экономической безопасности государства, общества, личности.
 14. Рассмотрение и решение проблем экономической безопасности в России в экономических реформах.
 15. Нормативные основы обеспечения экономической безопасности. Основные определения понятий в области экономической безопасности.
 16. Уровни, объекты и методы обеспечения экономической безопасности. Обеспечение экономической безопасности предприятия в рыночных условиях.
 17. Предпринимательский информационный риск и его минимизация.
 18. Экономические аспекты в информационной безопасности. Общность объектов защиты, угроз и уязвимостей.
 19. Силы и средства информационного противоборства в экономической сфере.
 20. Служба безопасности предприятия и ее функции по экономической и информационной безопасности.
 21. Понятия бюджетирования службы информационной безопасности. Функции и этапы разработки системы бюджетирования. Базовые составляющие бюджетирования. Виды и контроль бюджетирования.
 22. Понятие о страховании защищаемого информационного ресурса. Содержание процесса страхования. Преимущества страхования.
 23. Сущность страхования как метода защиты информации. Принципы страхования информационного ресурса. Виды страхования.
 24. Последовательность работ службы защиты информации по реализации страхования информационного ресурса.
 25. Характеристика видов страхования: имущества, ответственности и личное страхование.
 26. Страхование информационных рисков.
 27. Общий подход к оценке эффективности защиты и страхования информации.
 28. Понятие "эффективность"; абсолютная и относительная эффективность.
 29. Закон РФ № 149 от 09.08.2006 г. «Об информации, информационных технологиях и защите информации» об экономических задачах защиты информации.
 30. Предотвращение ущерба как главная экономическая задача защиты и страхования информации.
 31. Виды ущерба, наносимого информации.
 32. Методы оценки степени наносимого информации ущерба.

33. Основные факторы, влияющие на величину ущерба, наносимого владельцу информации вследствие отсутствия или недостаточности ее защиты.
34. Методы обеспечения сопоставимости расчетных величин при определении эффективности защиты информации (приведение разновременных результатов и затрат к расчетному году; дисконтирование).
35. Методические основы экономической оценки эффективности защиты информации: российские подходы.
36. Методические основы экономической оценки эффективности защиты информации: международные подходы.
37. Общая характеристика российских подходов оценки экономической эффективности защиты информации. Определение экономических затрат на защиту информации.
38. Общая характеристика российских подходов оценки экономической эффективности защиты информации. Расчет снижения ожидаемых экономических потерь от проводимых мер по защите информации.
39. Общая характеристика международных подходов оценки экономической эффективности защиты информации. Определение совокупной стоимости владения (сравнительный анализ затрат на защиту информации).
40. Общая характеристика международных подходов оценки экономической эффективности защиты информации: оценка возврата инвестиций, выделяемых на защиту информации.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

**Методические указания для обучающихся по освоению дисциплины
(модуля)**

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

«ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Квалификация (степень) выпускника: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

– Привития у обучаемых необходимых знаний и навыков по определению характера влияния мероприятий по защите информации на экономику предприятий и умения рассчитать основные параметры, определяющие экономические эффекты от проводимых мероприятий по информационной безопасности.

– Вместе с тем, в условиях рынка успешное функционирование любой масштабной информационной системы возможно только на стабильной финансово-экономической базе.

– В процессе обучения студент приобретает и совершенствует следующие компетенции.

Задачами дисциплины являются:

1. Теоретические основы подготовки студентов в области экономической безопасности

2. Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области экономической безопасности

2. Указания по проведению практических занятий

Общая продолжительность практических занятий составляет 36 часов для очной формы обучения и 12 часов для очно-заочной формы обучения.

Раздел 1. Экономические основы защиты информации

Тема 1. Введение в дисциплину и экономические проблемы защиты информационных ресурсов

Практическое занятие 1.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Информация как товар, цена информации.
2. Основные характеристики продукта как товара.
3. Классификация товаров. Особенности товара "информация".
4. Стоимость товара, принципы ее определения. Составляющие стоимости информационных массивов.
5. Стоимостные оценки результатов интеллектуального труда.
6. Цена как денежное выражение стоимости товара.
7. Формирование цены на информацию в рыночных условиях. Методы установления цен на информацию.

Продолжительность занятия: 2/2 ч.

Тема 2. Информация как товар и ее стоимость

Практическое занятие 2.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Понятие, состав и характеристика экономической информации как объекта информационной безопасности.
2. Экономические информационные системы.
3. Технологии обработки экономической информации.
4. Необходимость обеспечения защиты экономической информации.

Продолжительность занятия: 2/2 ч.

Тема 3. Анализ экономической информации и целесообразность ее защиты

Практическое занятие 3.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Понятие об экономической безопасности государства, общества, личности.
2. Рассмотрение и решение проблем экономической безопасности в России в экономических реформах.
3. Нормативные основы обеспечения экономической безопасности. Основные определения понятий в области экономической безопасности.
4. Уровни, объекты и методы обеспечения экономической безопасности.
5. Обеспечение экономической безопасности предприятия в рыночных условиях.

Продолжительность занятия: 2/2 ч.

Тема 4. Основы экономической безопасности (информационный аспект)

Практическое занятие 4.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Экономические аспекты в информационной безопасности. Общность объектов защиты, угроз и уязвимостей.
2. Силы и средства информационного противоборства в экономической сфере.
3. Служба безопасности предприятия и ее функции по экономической и информационной безопасности.

Продолжительность занятия: 2/2 ч.

Тема 5. Взаимозависимость экономической и информационной безопасностей

Практическое занятие 5.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Понятия бюджетирования.
2. Функции и этапы разработки системы бюджетирования.
3. Базовые составляющие бюджетирования.
4. Виды и контроль бюджетирования.

Продолжительность занятия: 2/2 ч.

Тема 6. Бюджетирование деятельности службы информационной безопасности (защиты информации)

Практическое занятие 6.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Понятие об информационных рисках и страховании защищаемого информационного ресурса.
2. Содержание процесса страхования. Преимущества страхования.
3. Сущность страхования как метода защиты информации.
4. Принципы страхования информационного ресурса.
5. Виды страхования.
6. Последовательность работ службы защиты информации по реализации страхования информационного ресурса.
7. Особенности страхования информационных рисков.

Продолжительность занятия: 2/2 ч.

Тема 7. Информационные риски и их страхование

Практическое занятие 7.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Теоретические основы оценки экономической эффективности подсистемы пожарной защиты информационных объектов.

2. Ознакомление с исходными данными и выполнение расчетов по оценке экономической эффективности подсистемы пожарной защиты выбранных информационных объектов

3. Анализ полученных результатов оценки экономической эффективности подсистемы пожарной защиты выбранных информационных объектов и формулирование выводов и предложений по текущему состоянию информационной безопасности.

Продолжительность занятия: 2/2 ч.

Раздел 2. Экономическая оценка эффективности защиты информации

Тема 8. Основные положения экономической эффективности защиты информации

Практическое занятие 8.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Теоретические основы оценки экономической эффективности подсистемы физической защиты информационных объектов.

2. Ознакомление с исходными данными и выполнение расчетов по оценке экономической эффективности подсистемы физической защиты выбранных информационных объектов

3. Анализ полученных результатов оценки экономической эффективности подсистемы физической защиты выбранных информационных объектов и формулирование выводов и предложений по текущему состоянию информационной безопасности.

Продолжительность занятия: 2/2 ч.

Тема 9. Методы оценки экономической эффективности защиты информации

Практическое занятие 9.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Теоретические основы оценки экономической эффективности подсистемы компьютерной защиты информационных объектов.

2. Ознакомление с исходными данными и выполнение расчетов по оценке экономической эффективности подсистемы компьютерной защиты выбранных информационных объектов

3. Анализ оценки экономической эффективности подсистемы компьютерной защиты информационных объектов, формулирование выводов и предложений по текущему состоянию информационной безопасности.

Продолжительность занятия: 2/2 ч.

Тема 10. Оценка экономических затрат на защиту информации

Практическое занятие 10.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Теоретические основы экономической эффективности комплексной системы защиты информации.

2. Ознакомление с исходными данными и выполнение расчетов по оценке экономической эффективности комплексной системы защиты информации.

3. Анализ оценки экономической эффективности комплексной системы защиты информации, формулирование выводов и предложений по текущему состоянию информационной безопасности.

Продолжительность занятия: 2/2 ч.

Тема 11. Экономическая эффективность инвестиций в защиту информации

Практическое занятие 11.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Экономические проблемы информационных ресурсов.
2. Информация как товар и ее стоимость.
3. Анализ экономической информации и целесообразность ее защиты.

Продолжительность занятия: 2/2 ч.

Тема 12. Оценка и управление информационными рисками

Практическое занятие 12.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основы экономической безопасности (информационный аспект).
2. Взаимозависимость экономической и информационной безопасностей.
3. Бюджетирование деятельности службы информационной безопасности (защиты информации).
4. Страхование как экономический метод защиты информации.

Продолжительность занятия: 2/2ч.

Тема 13. Оценка защиты интеллектуальной собственности

Практическое занятие 13.

Вид практического занятия: *подготовка доклада*.
Образовательные технологии: *групповая дискуссия*.

Вид практического занятия: *смешанная форма практического занятия*.

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основные положения экономической эффективности защиты информации.
2. Методы оценки экономической эффективности защиты информации.
3. Оценка экономических затрат на защиту информации.
4. Экономическая эффективность инвестиций в защиту информации.
5. Оценка информационных рисков.

Продолжительность занятия: 2/2 ч.

Тема 14. Оценка предпринимательских информационных рисков (информационная защита бизнес-процессов)

Практическое занятие 14.

Вид практического занятия: *подготовка доклада*.

Образовательные технологии: *групповая дискуссия*.

Вид практического занятия: *смешанная форма практического занятия*.

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основные положения экономической эффективности защиты информации.
2. Методы оценки экономической эффективности защиты информации.
3. Оценка экономических затрат на защиту информации.
4. Экономическая эффективность инвестиций в защиту информации.
5. Оценка информационных рисков.

Продолжительность занятия: 2/2 ч.

Тема 15. Экономическая оценка эффективности отдельных подсистем защиты информации

Практическое занятие 15.

Вид практического занятия: *подготовка доклада*.

Образовательные технологии: *групповая дискуссия*.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Оценка защиты интеллектуальной собственности.
2. Оценка предпринимательских информационных рисков (информационная защита бизнес-процессов).

Продолжительность занятия: 2/2ч.

Тема 16. Интегральная экономическая оценка эффективности комплексной системы защиты информации

Практическое занятие 16.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

3. Экономическая оценка эффективности отдельных подсистем защиты информации.
4. Интегральная экономическая оценка эффективности комплексной системы защиты информации.

Продолжительность занятия: 6/6 ч.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Тема. Оценка и управление информационными рисками	<i>Подготовка докладов по темам:</i> 1. Общая характеристика международных подходов оценки экономической эффективности защиты информации. Оценка и управление информационными рисками. 2. Обзор существующих методов оценки затрат на защиту информации.

		<ol style="list-style-type: none"> 3. Виды затрат на обеспечение информационной безопасности. 4. Основные положения методики определения затрат на основе метода совокупной стоимости владения (сравнительная оценка экономических расходов, выделенных на защиту информации). 5. Общие положения об инвестициях, выделяемых на обеспечение информационной безопасности. 6. Обзор существующих методов оценки возврата инвестиций, выделенных на защиту информации (международный опыт). 7. Основные положения методики оценки инвестиций в защиту информации на основе использования понятия «чистой текущей стоимости» с определением срока окупаемости проводимых мероприятий по защите информации. 8. Понятия об информационных рисках, их анализ (оценка). 9. Управления информационными рисками в экономической деятельности предприятия (общие положения). 10. Управления информационными рисками на различных стадиях жизненного цикла систем защиты информации.
2.	Тема. Оценка защиты интеллектуальной собственности	<p><i>Подготовка докладов по темам:</i></p> <ol style="list-style-type: none"> 1. Выбор допустимого уровня информационных рисков. 2. Инструментальные средства оценки информационных рисков. 3. Понятие интеллектуальная собственность и основы ее защиты. 4. Существующие методические подходы к экономической оценке защиты интеллектуальной собственности. 5. Методика оценки эффективности защиты интеллектуальной собственности: расчет упущенной выгоды (наносимого ущерба) в случае нарушения защиты интеллектуальной собственности – общий подход. 6. Методика оценки эффективности защиты интеллектуальной собственности: оценка объектов интеллектуальной собственности и

		<p>возможных убытков от противоправного их использования (мировая практика) – частый подход.</p> <p>7. Методика оценки эффективности защиты интеллектуальной собственности: оценка уровня интеллектуальной защищенности предприятия.</p> <p>8. Предпринимательская деятельность с позиции защиты экономической информации.</p> <p>9. Понятие стратегии по безопасности предприятия: стратегии экономической и информационной безопасности. Требуемые уровни (вероятности) защиты экономической информации.</p>
3	<p>Тема. Оценка предпринимательских информационных рисков (информационная защита бизнес-процессов)</p>	<p>Подготовка докладов по темам:</p> <p>1. Экономические проблемы в области защиты информации (информационного ресурса).</p> <p>2. Определения эффективности хозяйственно-экономической деятельности предприятия (информационный аспект).</p> <p>3. Роль информации в структуре общественного производства (как ресурса экономики и фактора производства).</p> <p>4. Основы обеспечения экономической безопасности государства (уровни и объекты экономической безопасности, методы ее обеспечения).</p> <p>5. Основы обеспечения экономической безопасности предприятия (уровни и объекты экономической безопасности, методы ее обеспечения).</p>
4	<p>Тема . Экономическая оценка эффективности отдельных подсистем защиты информации</p>	<p>Подготовка докладов по темам:</p> <p>1. Основы обеспечения экономической безопасности личности (уровни и объекты экономической безопасности, методы ее обеспечения)</p> <p>2. Правовые основы и базовые положения определения экономической эффективности защиты информации.</p> <p>3. Особенности информации как товар.</p> <p>4. Основные факторы, определяющие величину ущерба, нанесенного владельцу информации (вследствие отсутствия или недостаточной защиты информации).</p>

		5. Хозяйственно-экономическое значение инвестиций в защиту информации.
--	--	--

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объем контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. Экономические проблемы в области защиты информации (информационного ресурса).

2. Определения эффективности хозяйственно-экономической деятельности предприятия (информационный аспект).

3. Роль информации в структуре общественного производства (как ресурса экономики и фактора производства).

4. Основы обеспечения экономической безопасности государства (уровни и объекты экономической безопасности, методы ее обеспечения).

5. Основы обеспечения экономической безопасности предприятия (уровни и объекты экономической безопасности, методы ее обеспечения).

6. Основы обеспечения экономической безопасности личности (уровни и объекты экономической безопасности, методы ее обеспечения)

7. Правовые основы и базовые положения определения экономической эффективности защиты информации.
8. Особенности информации как товар.
9. Основные факторы, определяющие величину ущерба, нанесенного владельцу информации (вследствие отсутствия или недостаточной защиты информации).
10. Хозяйственно-экономическое значение инвестиций в защиту информации.
11. Методы оценки эффективности инвестиций в защиту информации (с обоснованием целесообразного метода).
12. Производственно-хозяйственная деятельность организаций как источник экономической информации, подлежащей защите.
13. Виды и управление рисками при защите информации (с обоснованием целесообразного вида).
14. Основы страхования и использование его в целях защиты информации.
15. Анализ состояния экономической безопасности организации (с определением роли защиты информации в ее обеспечении).
16. Выбор методов определения экономического ущерба (наносимого владельцу информации в результате противоправного ее использования).
17. Расчетные (аналитические) методы стоимостных оценок ущерба, наносимого владельцу информации (с обоснованием целесообразного метода).
18. Экспертные методы стоимостных оценок ущерба, наносимого владельцу информации (с обоснованием целесообразного метода).
19. Анализ экономической информации, возникающий в процессе производственно-хозяйственной деятельности (с выработкой рекомендаций по экономической целесообразности ее защиты).
20. Методы сопоставительного анализа эффективности инвестиционных проектов в защиту информации (с обоснованием целесообразного метода).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/103198> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
2. Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: <https://e.lanbook.com/book/256274> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3. Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/171525> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4. Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223223> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5. Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223304> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

6. Малышева Е.Н. Экспертные системы/Издательство: КемГУКИ (Кемеровский государственный университет культуры и искусств), 2010.

Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7

7. Информационные технологии и системы: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 352 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0376-6

8. Экспертные системы САПР: учебное пособие / А.Л. Ездаков. - М.: ИД ФОРУМ, 2012. - 160 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0398-8

9. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. — М.: Горячая линия – Телеком, 2004.

10. Квашнина Г. А. Донозологический мониторинг комплексной оценки управления адаптивного состояния субъекта в условиях экстремальной ситуации: монография / Г. А. Квашнина, Я. О. Мун. Воронеж: ВГТУ, 2008. 150 с.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. www.wiklsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн.
 5. www.rucont.ru - ЭБС «Руконт».
 6. <http://www.academy.it.ru/> – академия АЙТИ.
 7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
 8. [http://www.gov.ru/](http://www.gov.ru) - Официальный сервер органов государственной власти Российской Федерации.
 9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
- <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *Msoffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Экономика информационной безопасности»