МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Экономика и управление бизнес процессами в информационной безопасности

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
Безопасность открытых информационных систем

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2025 г.

Разработчик:

Доцент кафедры «Информационная безопасность», к.т.н., доцент,

/ К.В. Пителинский /

Ст. преподаватель кафедры «Информационная безопасность»

/ В.В. Осьмин /

Преподаватель кафедры «Информационная безопасность»

/ С.О. Маковей /

Согласовано:
Зав. кафедрой «Информационная безопасность»,

/И.В. Калуцкий/

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Управление информационной безопасностью» следует отнести:

- обучение навыкам экономического, организационного и психологического анализа управленческих отношений, основам деловой этики и культуры управленческого труда.
- получение студентами специальных знаний и навыков в области управления различными объектами информатизации, подлежащими защите
- изучение методов проектирования, моделирования и оптимизации отдельных частей системы управления и построение комплексной системы управления.
- формирование практических навыков воздействия на социально-психологический климат, разрешение конфликтных ситуаций, разработки и принятия управленческих решений.

К **основным задачам** освоения дисциплины «Управление информационной безопасностью» следует отнести:

- приобретение знаний о человеческом факторе в управлении, поведении людей в организации, их взаимодействии. Знакомство с психологической характеристикой трудовой группы и процессом её развития.
- овладение знаниями об организации, её формах и законах, внутренней и внешней среде организации.
- приобретение знаний об управленческих структурах и полномочиях, путях совершенствования организации управления.
- приобретение навыков выработки рационального управленческого решения и его реализации.
- овладение принципами проведения качественного аутсорсинга и аутстаффинга в ИТ-сфере и в сфере безопасности.

В результате освоения дисциплины «Управление информационной безопасностью» у обучающихся формируются следующие компетенции и должны быть достигнуты следующиерезультаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.	**Знать:** • основы экономики функционирования предприятия; **Уметь:** • принимать обоснованные экономические решения в различных областях жизнедеятельности; • обосновать актуальность использования ценностных систем при социальном и профессиональном взаимодействии **Владеть:** • инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности.
ПК-5. Способен проводить	**Знать:**

анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	• основные подходы к определению экономического ущерба, нанесенного информационным ресурсам предприятия; **Уметь:** • проводить анализ, предлагать и обосновывать выбор решений по обеспечению экономической и информационной безопасности в сфере профессиональной деятельности **Владеть:** • инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности.

2. Место дисциплины в структуре ООП специалитета

Дисциплина относится к обязательной части блока Б1 «Дисциплины (модули)».

Дисциплина «Экономика и управление бизнес-процессами в информационной безопасности» взаимосвязана логическии содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное правовое обеспечение информационной безопасности», «Управление информационной безопасностью».

Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности», «Теория принятия решений» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

3.1 Виды учебной работы и трудоемкость

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. 108 академических часа (лекции – 0 часов, лабораторные занятия – 54 часов, самостоятельная работа студентов – 54 часа, форма контроля – дифференцированный зачет) в 6 семестре.

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			6
1	**Аудиторные занятия**	**54**	6
	В том числе:		
1.1	Лекции	-	-
1.2	Семинарские/практические занятия	-	-
1.3	Лабораторные занятия	54	6
2	**Самостоятельная работа**	**54**	**6**
3	**Промежуточная аттестация**		**6**
	Диф. зачет		6
	Итого:	**108**	

3.2 Тематический план изучения дисциплины

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Цифровая экономика и управление знаниями	**18**			10		8
2	Тема 2. Аутсорсинг в сфере информационной безопасности	**18**			10		8
3	Тема 3. Основы противодействие конкурентной разведке и примышленному шпионажу	**18**			10		8
4	Тема 4. Защита от внутренних угроз информационной безопасности	**18**			8		10
5	Тема 5. Задачи экономики и управления бизнес-процессами в информационной безопасности	**18**			8		10
6	Тема 6. Оценка экономической и информационной безопасности предприятия	**18**			8		10
Итого		**108**			**54**		**54**

3.3 Содержание дисциплины

Тема 1. Цифровая экономика и управление знаниями

Информационные ресурсы общества. Революции в образовании и экономика знаний. Общая характеристика теории управления. История становления менеджмента**.** Внешняя и внутренняя среды организации. Модели для выявления и анализа возможностей, рисков и угроз. SWOT-анализ. Динамические контурные потоки в организации.

Функции управления: планирование, организация, мотивация и контроль. Коммуникации в системе управления ИБ.

Принятие управленческих решений. Власть и влияние. Лидерство: стиль, ситуация, эффективность.

Групповая динамика и руководство. Управление персоналом. Управление рисками в организации. Модели для выявления и анализа возможностей, рисков и угроз.

Знания как информационное оружие. Управление знаниями, как новая функция управления. Структура и процесс управления знаниями. Основные компоненты УЗ. Источники знаний в компании. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе. Подготовка и планирование внедрения знаний. Внедрение системы управления знаниями и ее развитие. Общение и обучение. Анализ хода реализации проекта.

Тема 2. Аутсорсинг в сфере информационной безопасности

Рынок аутсорсинга бизнес-процессов. Поставщики и потребители услуг ИТ-аутсорсинга. Сферы применения аутсорсинга. Законодательная и нормативная база аутсорсинга. Правовые аспекты соглашения об аутсорсинге. Оценка экономической эффективности внедрения ИТ-аутсорсинга. Аутсорсинг управления ИТ-проектами. Основные характеристики форм и видов аутсорсинга.

Проблемы и перспективы использования внешних ИТ-услуг. Аутстаффинг: сущность, исторические предпосылки, специфика, формы организации, преимущества и риски. Система менеджмента качества в сфере ИТ-аутсорсинга. Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005. Аутсорсинг безопасности в РФ. Аутсорсинг безопасности за рубежом. Аутсорсинг информационной безопасности — краткий обзор рынка

Тема 3. Основы противодействие конкурентной разведке и примышленному шпионажу

Способы получения и оценки информации. Методы поиска и вербовки информаторов. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека. Обеспечение безопасности разведывательной работы.

Элементы системы безопасности. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность. Организация встреч. Проблемы безопасности бизнесмена.

Тема 4. Защита от внутренних угроз информационной безопасности

Введение в инсайдерские угрозы. Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров. Классификация инсайдерских угроз. Нормативная совместимость. Нормативные акты корпоративного управления: Федеральный закон «О персональных данных». Корпоративное управление.

Проблема утечки конфиденциальной информации. Методы оценки эффективности в сфере защиты информации от утечек. Организационные меры защиты. Кадровая безопасность. Нетрадиционные методы оценки персонала. Управление изменениями в ИТ-инфраструктуре. Службы обмена мгновенными сообщениями и инсайдеры.

Тема 5. Задачи экономики и управления бизнес-процессами в информационной безопасности

Практика принятия управленческих решений. Законодательные акты, регулирующие экономические вопросы защиты информации. Система защиты информации и непрерывность бизнеса предприятия.

Методы сравнительного анализа сложных систем. Экспертные методы. Математическое и имитационное моделирование.

Подходы к определению затрат на защиту информации. Объем и доля бюджета фирм, выделяемых на ИБ.

Анализ структуры затрат, выделяемых на ИБ. Нормативное регулирование построения и функционирование системы защиты информации.

Тема 6. Оценка экономической и информационной безопасности предприятия

Уровень экономической безопасности предприятия. Задачи экономической безопасности предприятия. Функциональные критерии экономической безопасности предприятия.

Внутренние и внешние угрозы производственной деятельности предприятия. Нематериальные и материальные активы предприятия. Информация как важный ресурс предприятия. Ресурсы предприятия и служб защиты информации.

Оценка затрат на создание программных средств защиты информации. Методы оценки целесообразности затрат на систему информационной безопасности. Эффективность капиталовложений в создание средств ЗИ

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Лабораторные работы

Тема 1. Цифровая экономика и управление знаниями

Лабораторная работа 1. Информационные ресурсы общества. Революции в образовании и экономика знаний. Общая характеристика теории управления. История становления менеджмента**.** Внешняя и внутренняя среды организации. Модели для выявления и анализа возможностей, рисков и угроз. SWOT-анализ.

Лабораторная работа 2. Модели для выявления и анализа возможностей, рисков и угроз. PESTLE-анализ.

Лабораторная работа 3. Динамические контурные потоки в организации.

Лабораторная работа 4. Групповая динамика и руководство. Управление персоналом. Управление рисками в организации. Модели для выявления и анализа возможностей, рисков и угроз.

Лабораторная работа 5. Знания как информационное оружие. Управление знаниями, как новая функция управления. Структура и процесс управления знаниями. Основные компоненты УЗ. Источники знаний в компании. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе. Подготовка и планирование внедрения знаний. Внедрение системы управления знаниями и ее развитие. Общение и обучение. Анализ хода реализации проекта.

Тема 2. Аутсорсинг в сфере информационной безопасности

Лабораторная работа 1. Рынок аутсорсинга бизнес-процессов. Поставщики и потребители услуг ИТ-аутсорсинга. Сферы применения аутсорсинга.

Лабораторная работа 2. Законодательная и нормативная база аутсорсинга. Правовые аспекты соглашения об аутсорсинге.

Лабораторная работа 3. Оценка экономической эффективности внедрения ИТ-аутсорсинга. Аутсорсинг управления ИТ-проектами. Основные характеристики форм и видов аутсорсингаПроблемы и перспективы использования внешних ИТ-услуг. Аутстаффинг: сущность, исторические предпосылки, специфика, формы организации, преимущества и риски. Система менеджмента качества в сфере ИТ-аутсорсинга.

Лабораторная работа 4. Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005. Аутсорсинг безопасности в РФ. Аутсорсинг безопасности за рубежом. Аутсорсинг информационной безопасности — краткий обзор рынка

Тема 3. Основы противодействие конкурентной разведке и примышленному шпионажу

Лабораторная работа 1. Способы получения и оценки информации. Обеспечение безопасности разведывательной работы.

Лабораторная работа 2. Методы поиска и вербовки информаторов. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека.

Лабораторная работа 3. Элементы системы безопасности. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность.

Лабораторная работа 4. Организация встреч. Проблемы безопасности бизнесмена.

Тема 4. Защита от внутренних угроз информационной безопасности

Лабораторная работа 1. Введение в инсайдерские угрозы. Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров. Классификация инсайдерских угроз.

Лабораторная работа 2. Нормативная совместимость. Нормативные акты корпоративного управления: Федеральный закон «О персональных данных». Корпоративное управление.

Лабораторная работа 3. Проблема утечки конфиденциальной информации. Методы оценки эффективности в сфере защиты информации от утечек.

Лабораторная работа 4. Организационные меры защиты. Кадровая безопасность. Нетрадиционные методы оценки персонала. Управление изменениями в ИТ-инфраструктуре. Службы обмена мгновенными сообщениями и инсайдеры.

Тема 5. Задачи экономики и управления бизнес-процессами в информационной безопасности

Лабораторная работа 1. Практика принятия управленческих решений. Законодательные акты, регулирующие экономические вопросы защиты информации.

Лабораторная работа 2. Система защиты информации и непрерывность бизнеса предприятия. Методы сравнительного анализа сложных систем.

Лабораторная работа 3. Экспертные методы. Математическое и имитационное моделирование.

Лабораторная работа 4. Подходы к определению затрат на защиту информации. Объем и доля бюджета фирм, выделяемых на ИБ. Анализ структуры затрат, выделяемых на ИБ. Нормативное регулирование построения и функционирование системы защиты информации.

Тема 6. Оценка экономической и информационной безопасности предприятия

Лабораторная работа 1. Уровень экономической безопасности предприятия. Задачи экономической безопасности предприятия. Функциональные критерии экономической безопасности предприятия.

Лабораторная работа 2. Внутренние и внешние угрозы производственной деятельности предприятия. Нематериальные и материальные активы предприятия.

Лабораторная работа 3. Информация как важный ресурс предприятия. Ресурсы предприятия и служб защиты информации.

Лабораторная работа 4. Оценка затрат на создание программных средств защиты информации. Методы оценки целесообразности затрат на систему информационной безопасности. Эффективность капиталовложений в создание средств ЗИ.

3.5. Тематика курсовых проектов (курсовых работ)

Не предусмотрено учебной программой.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. ГОСТ Р 55.0.06-2021 Управление активами. Руководство по обеспечению согласованности финансовой и нефинансовой деятельности при управлении активами
2. ГОСТ Р ИСО/ТО 10014-2005 Руководство по управлению экономикой качества

4.2 Основная литература

1. Балукова, В. А. Управление знаниями : учебное пособие / В. А. Балукова, К. А. Карпов, М. В. Мирославская. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2022. — 129 с. — ISBN 978-5-907324-77-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/382250 (дата обращения: 21.09.2025). — Режим доступа: для авториз. пользователей.
2. Гребенников, П. И. Макроэкономика : учебник / П. И. Гребенников. — Москва : Проспект, 2021. — 208 с. — ISBN 978-5-392-34197-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/280319 (дата обращения: 22.09.2025). — Режим доступа: для авториз. пользователей.
3. Дронов, В. Ю. Бизнес-процесс «Обеспечение информационной безопасности организации» : учебное пособие / В. Ю. Дронов, Г. А. Дронова. — Новосибирск : НГТУ, 2021. — 76 с. — ISBN 978-5-7782-4537-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/306350 (дата обращения: 22.09.2025). — Режим доступа: для авториз. пользователей.
4. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-45723-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/311825 (дата обращения: 22.09.2025). — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

1. Гребенников, П. И. Экономика : учебник для вузов / П. И. Гребенников, Л. С. Тарасевич. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 310 с. — (Высшее образование). — ISBN 978-5-534-08979-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488548 (дата обращения: 27.09.2025).
2. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889 (дата обращения: 22.09.2025). — Режим доступа: для авториз. пользователей.
2. Ларина И.Е. Экономика защиты информации. Учебное пособие.; МГИУ, 2010 г
3. Плашенков В.В. Обеспечение безопасности бизнеса промышленных предприятий : теория и практика: учебное пособие. Издательство ЧГУ , 2014 г. -Режим доступа - http://biblioclub.ru
4. Семененко В.А. Информационная безопасность : учеб. пособие для вузов. - М.: МГИУ, 2010 г.

4.4 Электронные образовательные ресурсы

1. ЭОР разрабатывается
2. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
3. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань https://mospolytech.ru/obuchauschimsya/biblioteka/

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. http://www.risk-manage.ru/
2. http://www.genrih-lemke.narod.ru
3. Операционная система Windows 10(или ниже) – MicrosoftOpenLicense Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215
4. Офисные приложения, MicrosoftOffice 2013(или ниже) – MicrosoftOpenLicense Лицензия № 61984042.

4.6 Современные профессиональные базы данных и информационные справочныематериалы

1. ГАРАНТ – Законодательство (кодексы, законы, указы, постановления) РФ, аналитика, комментарии, практика https://www.garant.ru/
2. Консультант Плюс https://consultantplus.helpline.ru/
3. Управление качеством в организации | Государственный портал ProКачество https://kachestvo.pro/

5 Материально-техническое обеспечение

Для проведения лабораторных работ и самостоятельной работы студентов подходят аудитории, оснащенные компьютерами с программным обеспечением в соответствии со списком в пункте 4.5 и подключенные к интернету.

Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лабораторные работы*.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Лабораторные работы* проводятся по теоретическим и проблемным вопросам ИБ. Лабораторные работы предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении лабораторных работ преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на лабораторной работе учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением лабораторных работ и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на лабораторных работах, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на лабораторных работах, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Методика преподавания дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение интерактивных лекционных и практических занятий в форме видеоуроков;
- подготовка к выполнению практических работ с использованием видеоуроков;
- обсуждение и защита рефератов по дисциплине;
- подготовка, представление и обсуждение презентаций на практических занятиях;
- подготовка к экзамену.

Удельный вес занятий, проводимых в интерактивных формах, определен образовательной программой, особенностью контингента обучающихся и содержанием дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» и в целом по дисциплине составляет 100% (54 часа) занятий практического типа составляют 100% (54 часа).

7.2. Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: основы экономики функционирования предприятия	Обучающийся демонстрирует полное отсутствие знаний об экономической деятельности и экономической безопасности предприятия	Обучающийся демонстрирует неполное знание экономической деятельности и экономической безопасности предприятия	Обучающийся демонстрирует частичное знание экономической деятельности и экономической безопасности предприятия	Обучающийся демонстрирует полное знание экономической деятельности и экономической безопасности предприятия

уметь: принимать обоснованные экономические решения в различных областях жизнедеятельности	Обучающийся не умеет принимать обоснованные экономические решения в различных областях жизнедеятельности	Обучающийся демонстрирует неполное умение принимать обоснованные экономические решения в различных областях жизнедеятельности	Обучающийся демонстрирует частичное умение принимать обоснованные экономические решения в различных областях жизнедеятельности	Обучающийся демонстрирует полное умение принимать обоснованные экономические решения в различных областях жизнедеятельности
владеть: инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся не владеет методами анализа затрат и результатов деятельности предприятия	Обучающийся не полностью владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся частично владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся в полном объеме владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности
ПК-5 Способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности				
знать: основные подходы к определению экономического ущерба, нанесенного информационным ресурсам предприятия;	Обучающийся демонстрирует полное отсутствие знаний основных подходов к определению экономического ущерба, нанесенного информационным ресурсам предприятия	Обучающийся демонстрирует неполное знание основных подходов к определению экономического ущерба, нанесенного информационным ресурсам предприятия	Обучающийся демонстрирует частичное знание основных подходов к определению экономического ущерба, нанесенного информационным ресурсам предприятий	Обучающийся демонстрирует полное знание основных подходов к определению экономического ущерба, нанесенного информационным ресурсам предприятий
уметь: проводить анализ, предлагать и обосновывать выбор решений по обеспечению экономической и информационной безопасности в сфере профессиональной деятельности	Обучающийся не умеет проводить анализ, предлагать и обосновывать выбор решений по обеспечению экономической и информационной безопасности в сфере профессиональной деятельности	Обучающийся демонстрирует неполное умение проводить анализ, предлагать и обосновывать выбор решений по обеспечению экономической и информационной безопасности в сфере профессиональной деятельности	Обучающийся демонстрирует частичное умение проводить анализ, предлагать и обосновывать выбор решений по обеспечению экономической и информационной безопасности в сфере профессиональной деятельности	Обучающийся демонстрирует полное умение проводить анализ, предлагать и обосновывать выбор решений по обеспечению экономической и информационной безопасности в сфере профессиональной деятельности
владеть: инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся не владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся в неполном объеме владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся частично владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности	Обучающийся в полном объеме владеет инструментарием принятия обоснованных управленческих решений в различных областях жизнедеятельности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме дифференцированного зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по дисциплине «Экономика и управление бизнес-процессами в информационной безопасности», при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине.

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. Присутствовал более чем на ¾ занятий
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. Присутствовал более чем на ¾ занятий
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. Присутствовал более чем на ½ занятий
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. Присутствовал менее чем на ½ занятий

7.3. Оценочные средства

7.3.1 Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ и промежуточных тестирований.

Тестовые вопросы по курсу

1. Что понимается под прибылью предприятия при создании и эксплуатации систем информационной безопасности?

а. Разница, полученная предприятием, между выручкой и себестоимостью произведенной продукции, работ и услуг
б. Количественная оценка уменьшения потерь информации от предотвращения действия угрозы
в. Количественная оценка уменьшения потерь информации от предотвращения действия угрозы плюс реализационная прибыль от продажи произведенной продукции, работ и услуг.

2. Экономическое обоснование затрат на создание и эксплуатацию технических и программных средств защиты необходимо
а . для оценки эффективности принятых мер по защите информации на предприятии
б. для сокращения доли бюджета предприятий, выделяемую на собственную безопасность
в. для обоснования оптимальной структуры и состава системы зашиты информации на предприятии

3. Экономический эффект от использования системы защиты информации определяется
а . исходя из анализа и классификации рисков, возникающих при защите информации
б. на основе экспертных оценок уровня, понесенного или предотвращенного ущерба в результате внедрения КСЗИ
в. на основе оценки затрат на создание и эксплуатацию комплексной системы защиты информации и стоимости уровня, понесенного и/или предотвращенного ущерба

4. На каком этапе построения системы информационной безопасности оценивается эффективность КСЗИ
а . на этапе обоснования структуры и технологии функционирования КСЗИ
б. на этапе технико-экономической оценки разрабатываемого проекта КСЗИ
в. на этапе обоснования задач защиты информации и определения необходимых мер обеспечения информационной безопасности на предприятии

5. Необходимым условием обоснования эффективности создания и функционирования системы информационной безопасности является
а . анализ угроз информационной безопасности предприятия
б. проведение аудита состояния информационной безопасности предприятия
в. анализ угроз и оценка состояния информационной безопасности предприятия

6. Уровень экономической безопасности предприятия по информационной составляющей определяется
а. как отношение общего понесенного ущерба экономической безопасности предприятия к предотвращенному ущербу за период
б. как отношение общего предотвращенного ущерба экономической безопасности предприятия к понесенному ущербу и затратам на обеспечение информационной безопасности на предприятии за анализируемый период
в. как отношение общего понесенного ущерба экономической безопасности предприятия и затратам на обеспечение информационной безопасности на предприятии к предотвращенному ущербу за анализируемый период

7. Ущерб от различных рисков потери информации включает
а. прямые и косвенные убытки
б упущенную выгоду предприятия от простоя атакованного узла
в. прямые убытки от понесенного ущерба

8. При оценке рисков информационной безопасности не по двум, а по трем факторам какой дополнительный фактор учитывается
   а. цена потери
   б. вероятность происшествия
   в. вероятность угрозы

9. К какому способу воздействия на риск относится способ страхование рисков
   а. исключение риска
   б. снижения вероятности возникновения риска
   в. сохранение существующего уровня риска

10 . В каких случаях применяется страхование как дополнительная мера защиты информации
   а. когда других мер по обеспечению безопасности недостаточно
   б. когда другие меры непригодны или слишком дороги
   в. когда вероятность реализации угрозы не очень велика, но последствия для информационной системы незначительны.

11. Какие виды страхования в рамках системы защиты информации возможны
   а. страхование имущества и личное страхование
   б. страхование имущества, ответственности и личное страхование
   в. страхование имущества и ответственности

12 Какие производственные затраты оцениваются при оценке эффективности построения системы информационной безопасности
   а . затраты на основные средства, нематериальные активы, материалы и трудовые ресурсы
   б. затраты на основные средства, программное обеспечение, трудовые ресурсы
   в. затраты на программное и аппаратное обеспечение системы информационной безопасности предприятия

13 Как оцениваются затраты на технические средства в процессе эксплуатации системы безопасности предприятия
   а. путем расчета амортизационных отчислений на восстановление стоимости технических средств
   б. путем определения срока полезного использования и расчета амортизационных отчислений на восстановление стоимости технических средств
   в. затраты на технические средства в процессе эксплуатации технических средств не рассчитываются.

14 Как оцениваются затраты на программные средства используемые в процессе эксплуатации системы безопасности предприятия
   а. путем расчета амортизационных отчислений на восстановление стоимости программного обеспечения
   б. путем определения срока полезного использования и расчета амортизационных отчислений на восстановление стоимости программного обеспечения
   в. затраты на программные средства оцениваются только в период их приобретения

15. Какие показатели используются для оценки эффективности КСЗИ
   а. условно-годовая экономия от внедрения КСЗИ, затраты на создание КСЗИ
   б. фактический срок окупаемости и коэффициент эффективности КСЗИ
   в. годовой экономический эффект и фактический срок окупаемости

16. Можно ли рассматривать годовую экономию от внедрения КСЗИ как предполагаемый ущерб, которое предприятие могло бы понести в случае утечки информации?
    а. да
    б. нет

17. Когда инвестиционный проект в систему защиты информации является эффективным
    а. когда чистый дисконтированный доход > 1
    б. когда чистый дисконтированный доход < 1
    в. когда индекс доходности <1

18. Для чего используется Функционально-стоимостной анализ при построении КСЗИ на предприятии
    а. используется как метод снижения затрат при создании системы информационной безопасности предприятия
    б используется как метод снижения затрат и оптимизации структуры системы информационной безопасности предприятия
    в. используется как метод снижения затрат, оптимизации структуры и выполняемых функций системы информационной безопасности предприятия

Примерная тематика рефератов по курсу «Управление информационной безопасностью»

1. Революции в образовании и экономика знаний.
2. Модели для выявления и анализа возможностей, рисков и угроз.
3. Управление рисками в организации.
4. Модели для выявления и анализа возможностей, рисков и угроз.
5. Структура и процесс управления знаниями.
6. Основные компоненты УЗ и источники знаний в компании.
7. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе.
8. Подготовка, планирование и внедрение системы управления знаниями
9. Рынок аутсорсинга бизнес-процессов.
10. Поставщики и потребители услуг ИТ-аутсорсинга.
11. Правовые аспекты соглашения об аутсорсинге.
12. Оценка экономической эффективности внедрения ИТ-аутсорсинга.
13. Основные характеристики форм и видов аутсорсинга.
14. Аутстаффинг: сущность, исторические предпосылки, специфика, формы организации, преимущества и риски.
15. Система менеджмента качества в сфере ИТ-аутсорсинга.
16. Аутсорсинг безопасности в РФ и за рубежом.
17. Проблемы безопасности бизнесмена. Организация встреч.
18. Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров.
19. Методы оценки эффективности в сфере защиты информации от утечек.
20. Организационные меры защиты.
21. Законодательные акты, регулирующие экономические вопросы защиты информации.
22. Система защиты информации и непрерывность бизнеса предприятия.
23. Подходы к определению затрат на защиту информации.
24. Анализ структуры затрат, выделяемых на ИБ.

25. Задачи экономической безопасности предприятия.
26. Внутренние и внешние угрозы производственной деятельности предприятия.
27. Нематериальные и материальные активы предприятия.
28. Оценка затрат на создание программных средств защиты информации.
29. Методы оценки целесообразности затрат на систему информационной безопасности.
30. Эффективность капиталовложений в создание средств защиты информации

Список вопросов к зачету по дисциплине

1. Информационные ресурсы общества.
2. Революции в образовании и экономика знаний.
3. Общая характеристика теории управления.
4. История становления менеджмента**.**
5. Внешняя и внутренняя среды организации.
6. Модели для выявления и анализа возможностей, рисков и угроз.
7. SWOT-анализ.
8. Динамические контурные потоки в организации.
9. Функции управления: планирование, организация, мотивация и контроль.
10. Коммуникации в системе управления ИБ.
11. Принятие управленческих решений.
12. Власть и влияние.
13. Лидерство: стиль, ситуация, эффективность.
14. Групповая динамика и руководство.
15. Управление персоналом.
16. Управление рисками в организации.
17. Модели для выявления и анализа возможностей, рисков и угроз.
18. Знания как информационное оружие.
19. Управление знаниями, как новая функция управления.
20. Структура и процесс управления знаниями.
21. Основные компоненты УЗ.
22. Источники знаний в компании.
23. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе.
24. Подготовка и планирование внедрения знаний.
25. Внедрение системы управления знаниями и ее развитие.
26. Общение и обучение. Анализ хода реализации проекта.
27. Рынок аутсорсинга бизнес-процессов.
28. Поставщики и потребители услуг ИТ-аутсорсинга.
29. Сферы применения аутсорсинга.
30. Законодательная и нормативная база аутсорсинга.
31. Правовые аспекты соглашения об аутсорсинге.
32. Оценка экономической эффективности внедрения ИТ-аутсорсинга.
33. Аутсорсинг управления ИТ-проектами.
34. Основные характеристики форм и видов аутсорсинга.
35. Проблемы и перспективы использования внешних ИТ-услуг.
36. Аутстаффинг: сущность, исторические предпосылки, специфика, формы организации,

преимущества и риски.
37. Система менеджмента качества в сфере ИТ-аутсорсинга.
38. Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005.
39. Аутсорсинг безопасности в РФ.
40. Аутсорсинг безопасности за рубежом.
41. Аутсорсинг информационной безопасности — краткий обзор рынка
42. Способы получения и оценки информации.
43. Методы поиска и вербовки информаторов.
44. Методы обеспечения результативного общения.
45. Методы целенаправленного воздействия на человека.
46. Обеспечение безопасности разведывательной работы.
47. Элементы системы безопасности.
48. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность.
49. Проблемы безопасности бизнесмена. Организация встреч.
50. Инсайдерские угрозы.
51. Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров.
52. Классификация инсайдерских угроз.
53. Нормативная совместимость. Нормативные акты корпоративного управления:
54. Федеральный закон «О персональных данных». Корпоративное управление.
55. Проблема утечки конфиденциальной информации.
56. Методы оценки эффективности в сфере защиты информации от утечек.
57. Организационные меры защиты.
58. Кадровая безопасность.
59. Управление изменениями в ИТ-инфраструктуре.
60. Службы обмена мгновенными сообщениями и инсайдеры.
61. Практика принятия управленческих решений.
62. Законодательные акты, регулирующие экономические вопросы защиты информации.
63. Система защиты информации и непрерывность бизнеса предприятия.
64. Методы сравнительного анализа сложных систем.
65. Экспертные методы.
66. Математическое и имитационное моделирование.
67. Подходы к определению затрат на защиту информации.
68. Объем и доля бюджета фирм, выделяемых на ИБ.
69. Анализ структуры затрат, выделяемых на ИБ.
70. Нормативное регулирование построения и функционирование системы защиты информации.
71. Уровень экономической безопасности предприятия.
72. Задачи экономической безопасности предприятия.
73. Функциональные критерии экономической безопасности предприятия.
74. Внутренние и внешние угрозы производственной деятельности предприятия.
75. Нематериальные и материальные активы предприятия.
76. Информация как важный ресурс предприятия.
77. Ресурсы предприятия и служб защиты информации.
78. Оценка затрат на создание программных средств защиты информации.

79. Методы оценки целесообразности затрат на систему информационной безопасности.
80. Эффективность капиталовложений в создание средств защиты информации
81. Метод Саати и сферы его применения