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

«Построение и совершенствование систем управления информационной безопасностью»

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр по защите информации

Формы обучения
Очная

Москва, 2023 г.

Разработчики:

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

 / И.В. Калуцкий /

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

 / К.В. Пителинский /

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н.  /С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Построение и совершенствование систем управления 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.
- приобретение студентами базовых теоретических знаний и практических навыков по экономическому обоснованию затрат на создание и эксплуатацию технических, организационных и программно-аппаратных средств системы защиты объектов информатизации.
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой магистратуры по направлению, в том числе формирование у них умений по выявлению недостатков и оценки эффективности внедрения прогрессивных технологий и средств информационной безопасности.

К **основным задачам** освоения дисциплины «Построение и совершенствование систем управления 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
- Освоение методологии анализа и стоимостной оценки ущерба, наносимого владельцу информации, в результате противоправного ее использования, методики оценки затрат на эксплуатацию системы информационной безопасности, технико-экономического обоснования целесообразности инвестиций в комплексные системы защиты информации предприятия..

В результате освоения дисциплины «Построение и совершенствование систем управления информационной безопасностью» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	**знать:** • требования к системе обеспечения информационной безопасности; **уметь:**

	• разрабатывать проект технического задания на создание системы обеспечения информационной безопасности; **владеть:** • инструментарием формирования требований к системе обеспечения информационной безопасности
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты"	**знать:** • направления развития информационных (телекоммуникационных) технологий; **уметь:** • прогнозировать эффективность функционирования объектов защиты; **владеть:** • методами оценки затрат и рисков, формирования политик безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	**знать:** • принципы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности; **уметь:** • использовать программы и методики испытаний средств и систем обеспечения информационной безопасности; **владеть:** • принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности
ПК-13. Способен организовать управление информационной безопасностью	**знать:** • способы организации управления информационной безопасностью; **уметь:** • организовать управление информационной безопасностью; **владеть:** • принципами организации управления информационной безопасностью

2 Место дисциплины в структуре образовательной программы

Дисциплина «Построение и совершенствование систем управления информационной безопасностью» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы магистра (Б1.2.1).

Дисциплина «Построение и совершенствование систем управления информационной безопасностью» взаимосвязана логически и 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 и правовое обеспечение информационной безопасности».

Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Управление информационной безопасностью» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часа (лекции – 0 часов, лабораторные занятия – 72 часов, самостоятельная работа студентов – 72 часа, курсовой проект, форма контроля – экзамен) в 1 семестре.

Структура и содержание дисциплины «Построение и совершенствование систем управления информационной безопасностью» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**72**	1	1-18
	В том числе:			
1.1	Лекции	-	-	-
1.2	Семинарские/практические занятия			-
1.3	Лабораторные занятия		1	1-18
2	**Самостоятельная работа**	**72**	1	1-18
3	**Промежуточная аттестация**		1	6-17
	Зачет/диф. зачет/экзамен	экзамен	1	По расписанию
	Курсовой проект	диф. зачет	1	По расписанию
	Итого	**144**		

3.2 Тематический план изучения дисциплины

(по формам обучения)

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	
1.1	Тема 1. Цифровая экономика и управление знаниями	24	-	-	12	-	12
1.2	Тема 2. Аутсорсинг в сфере информационной безопасности	24	-	-	12	-	12
1.3	Тема 3. Защита от внешних и внутренних угроз информационной безопасности	24	-	-	12	-	12
1.4	Тема 4. Задачи экономики и управления бизнес-процессами в информационной безопасности	24	-	-	12	-	12
1.5	Тема 5. Оценка экономической и информационной безопасности предприятия	24	-	-	12	-	12
1.6	Тема 6. Оценка затрат на создание системы защиты информации	24	-	-	12	-	12
Итого		**144**			**72**		**72**

3.3 Содержание дисциплины

В данном курсе лекции не предусмотрены учебным планом

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Лабораторные занятия

Тема 1. Цифровая экономика и управление знаниями

Лабораторная работа 1. Информационные ресурсы общества. Представление информации и информационные технологии. Революции в образовании и экономика знаний. Общая характеристика теории управления. История становления менеджмента**.**

Лабораторная работа 2. 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.

Лабораторная работа 3. 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.

Лабораторная работа 4. Знания как информационное оружие. Управление знаниями, как новая функция управления. Структура и процесс управления знаниями. Основные компоненты УЗ. Источники знаний в компании.

Лабораторная работа 5. 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. Законодательная и нормативная база аутсорсинга.

Лабораторная работа 2. Правовые аспекты соглашения об аутсорсинге. Оценка экономической эффективности внедрения ИТ-аутсорсинга. Аутсорсинг управления ИТ-проектами.

Лабораторная работа 3. Основные характеристики форм и видов аутсорсинга. Проблемы и перспективы использования внешних ИТ-услуг. Аутстаффинг: сущность, исторические предпосылки, специфика, формы организации, преимущества и риски.

Лабораторная работа 4. Система менеджмента качества в сфере ИТ-аутсорсинга. Нормативное регулирование построения и функционирование системы защиты информации.

Лабораторная работа 5. ISO/IES 27001-27005. Аутсорсинг безопасности в РФ. Аутсорсинг безопасности за рубежом. Аутсорсинг информационной безопасности — краткий обзор рынка.

Тема 3. Защита внешних и внутренних угроз информационной безопасности

Лабораторная работа 1. Способы получения и оценки информации. Методы поиска и вербовки информаторов. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека.

Лабораторная работа 2. Обеспечение безопасности разведывательной работы. Элементы системы безопасности. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность. Организация встреч. Проблемы безопасности бизнесмена.

Лабораторная работа 3. 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».

Лабораторная работа 4. Корпоративное управление. Проблема утечки конфиденциальной информации. Методы оценки эффективности в сфере защиты информации от утечек. Организационные меры защиты. Кадровая безопасность. Управление изменениями в ИТ-инфраструктуре. Службы обмена мгновенными сообщениями и инсайдеры.

Тема 4. 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. Подходы к определению затрат на защиту информации. Объем и доля бюджета фирм, выделяемых на ИБ.

Лабораторная работа 4. Анализ структуры затрат, выделяемых на ИБ. Нормативное регулирование построения и функционирование системы защиты информации.

Тема 5. 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. Принципы разумной достаточности при создании системы защиты информации. Связь затрат на информационную безопасность и уровня достигаемой защищенности предприятия.

Тема 6. Оценка затрат на создание системы защиты информации

Лабораторная работа 1. Регламентирующие документы на разработку и применение программного и аппаратного обеспечения защиты информации на предприятии.

Лабораторная работа 2. Понятие и оценка совокупной стоимости владения информационной системы и системы безопасности (ТСО). Перечень затрат на планирование, разработку, внедрение и управление КСЗИ.

Лабораторная работа 3. Оценка затрат на создание программных средств защиты информации. Эффективность капиталовложений в создание средств защиты информации.

Лабораторная работа 4. Методы оценки целесообразности затрат на систему информационной безопасности (AIE), (CI), (EVA), (PM), (BSC).

3.5 Тематика курсовых проектов (курсовых работ)

По дисциплине «Построение и совершенствование систем управления информационной безопасностью» предусмотрен курсовой проект.

Тематика курсового проекта: Оценка системы управления экономической и информационной безопасностью предприятия/организации.

Состав проекта:

Оценка стоимости материальных и нематериальных активов предприятия/организации, подлежащих защите. Выбор метода оценки целесообразности затрат на систему информационной безопасности (AIE), (CI), (EVA), (PM), (BSC) предприятия/организации. Оценка затрат на планирование, разработку, внедрение и управление КСЗИ

4 Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1. ГОСТ Р 59503-2021/ISO/IEC TR 27016:2014. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации. – М., 2021
5 Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК РФ 11 февраля 2014 г.)

https://it-security.admin-smolensk.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii/metodicheskij-dokument-mery-zaschity-informacii-v-gosudarstvennyh-informacionnyh-sistemah-/
6 ГОСТ Р 59712–2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты».
7 ГОСТ 7.1–84. Библиографическое описание документа. Общие требования и правила составления. – М., 1985

4.2. Основная литература

1. Основы финансовой грамотности / Е. И. Костюкова, И. И. Глотова, Е. П. Томилина [и др.]. — Санкт-Петербург : Лань, 2023. — 316 с. — ISBN 978-5-507-45627-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/311807.
2. 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.
3. Егоров, В. П. Документоведение и документационное обеспечение управления в условиях цифровой экономики / В. П. Егоров, А. В. Слиньков. — 4-е изд., стер. — Санкт-Петербург : Лань, 2023. — 372 с. — ISBN 978-5-507-45695-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/279827
4. Земляк, С. В. Актуальные вопросы экономики и управления : материалы конференции / С. В. Земляк, О. Ю. Крамлих. — Москва : Дашков и К, 2022. — 501 с. — ISBN 978-5-394-05409-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/330410.

4.3. Дополнительная литература

1. Колбин, В. В. Оценка и управление риском / В. В. Колбин, В. А. Ледовская. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 248 с. — ISBN 978-5-507-46864-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/322655
2. Виссия, Х. Э. Принятие решений в информационном обществе : учебное пособие / Х. Э. Виссия, В. В. Краснопрошин, А. Н. Вальвачев. — Санкт-Петербург : Лань, 2022. — 228 с. — ISBN 978-5-8114-3747-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206723.
3. Управленческая экономика : учебник для вузов / С. В. Каледин, Г. М. Грейз, И. П. Довбий, М. С. Моторина. — Санкт-Петербург : Лань, 2021. — 516 с. — ISBN 978-5-8114-6742-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165833.

4.4. Электронные образовательные ресурсы

1. ЭОР на стадии разработки
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань https://mospolytech.ru/obuchauschimsya/biblioteka/

4.5. Лицензионное и свободно распространяемое программное обеспечение

Программное обеспечение не предусмотрено

Полезные учебно-методические и информационные материалы представлены на сайтах:

1. ИТ-портал компании «Инфосистемы джет» -Режим доступа - http://www.jetinfo.ru
2. «Информационная безопасность», журнал – Режим доступа - http://itsec.ru/imag/

4.6. Современные профессиональные базы данных и информационные справочные системы

1. Банк данных угроз безопасности информации ФСТЭК России https://bdu.fstec.ru/

5. Материально-техническое обеспечение

Проведение лекционных и практических осуществляется в мультимедийной аудитории

6. Методические рекомендации

6.1. Методические рекомендации для преподавателя по организации обучения

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки магистр **10.04.01 Информационная безопасность.**

6.2. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины «Построение и совершенствование систем управления информационной безопасностью» осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции. При рассмотрении учебного материалы рекомендуется делать акцент на структуру и взаимосвязь аспектов безопасности - методологии, информационного обеспечения, организации, экономических методах, кадрового обеспечения и нормативно-правовой базы. Полезно также сосредоточить внимание студентов на анализе угроз и оценке рисков информационной безопасности, оценке прямого и косвенного ущерба от риска потери информации, определении упущенной выгоды предприятия, методах оценки целесообразности и эффективности затрат на систему информационной безопасности

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачету, а также самостоятельно изучают отдельные темы учебной программы. В тематическом плане указанные темы выделены курсивом и снабжены пометкой «самостоятельно». Преподаватель направляет самостоятельную работу студентов, отвечает на возникающие вопросы, дает рекомендации по методике изучения тем.

Практические занятия 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. Практические занятия проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие 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 практического занятия 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 практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине «Построение и совершенствование систем управления информационной безопасностью» предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий 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 практических занятиях, промежуточный контроль осуществляется в 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 практических занятиях, промежуточный контроль осуществляется на экзамене в устной форме.

Критериями оценки результатов самостоятельной работы студента являются:

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

7. Фонд оценочных средств

7.1. Методы контроля и оценивания результатов обучения

Методика преподавания дисциплины «Построение и совершенствование систем управления информационной безопасностью» 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:

- обсуждение и защита рефератов по дисциплине;
- подготовка, представление и обсуждение презентаций по темам рефератов на семинарских занятиях;
- использование интерактивных форм текущего контроля в форме тестирования;

Удельный вес занятий, проводимых в интерактивных формах, определен главной целью образовательной программы, особенностью контингента обучающихся, содержанием дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» и в целом по дисциплине составляет 25% аудиторных занятий. Занятия лекционного типа составляют 50% от объема аудиторных занятий.

7.2. Шкала и критерии оценивания результатов обучения

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

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
ПК-1	Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты

ПК-4	Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
ПК-13	Способен организовать управление информационной безопасностью

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

7.2.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине. При этом индикаторы освоения компетенций согласно ОПОП реализуются вариативно преподавателем, ведущим данную дисциплину

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: требования к системе обеспечения информационной безопасности;	Обучающийся демонстрирует полное отсутствие знаний об требованиях к системе обеспечения информационной безопасности	Обучающийся демонстрирует неполное знание об требованиях к системе обеспечения информационной безопасности	Обучающийся демонстрирует частичное знание об требованиях к системе обеспечения информационной безопасности	Обучающийся демонстрирует полное знание об требованиях к системе обеспечения информационной безопасности
уметь: разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Обучающийся не умеет разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Обучающийся демонстрирует неполное умение разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Обучающийся демонстрирует частичное умение разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Обучающийся демонстрирует полное умение разрабатывать проект технического задания на создание системы обеспечения информационной безопасности

владеть: инструментарием формирования требований к системе обеспечения информационной безопасности	Обучающийся не владеет инструментарием формирования требований к системе обеспечения информационной безопасности	Обучающийся не полностью владеет инструментарием формирования требований к системе обеспечения информационной безопасности	Обучающийся частично владеет инструментарием формирования требований к системе обеспечения информационной безопасности	Обучающийся в полном объеме владеет инструментарием формирования требований к системе обеспечения информационной безопасности
ПК-1 Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты				
знать: направления развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует полное отсутствие знаний направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует неполное знание направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует частичное знание направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует полное знание направлений развития информационных (телекоммуникационных) технологий
уметь: прогнозировать эффективность функционирования объектов защиты	Обучающийся не умеет прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует неполное умение прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует частичное умение прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует полное умение прогнозировать эффективность функционирования объектов защиты
владеть: методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся не владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся в неполном объеме владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся частично владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся в полном объеме владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты
ПК-4 Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности				

знать: принципы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное отсутствие знаний принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует неполное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует частичное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности
уметь: использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся не умеет использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует неполное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует частичное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности
владеть: принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся не владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся в неполном объеме владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся частично владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся в полном объеме владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности
ПК-13 Способен организовать управление информационной безопасностью				
знать: способы организации управления информационной безопасностью	Обучающийся демонстрирует полное отсутствие знаний способов организации управления информационной безопасностью	Обучающийся демонстрирует неполное знание способов организации управления информационной безопасностью	Обучающийся демонстрирует частичное знание способов организации управления информационной безопасностью	Обучающийся демонстрирует полное знание способов организации управления информационной безопасностью

уметь: организовать управление информационной безопасностью	Обучающийся не умеет организовать управление информационной безопасностью	Обучающийся демонстрирует неполное умение организовать управление информационной безопасностью	Обучающийся демонстрирует частичное умение организовать управление информационной безопасностью	Обучающийся демонстрирует полное умение организовать управление информационной безопасностью
владеть: принципами организации управления информационной безопасностью	Обучающийся не владеет принципами организации управления информационной безопасностью	Обучающийся в неполном объеме владеет принципами организации управления информационной безопасностью	Обучающийся частично владеет принципами организации управления информационной безопасностью	Обучающийся в полном объеме владеет принципами организации управления информационной безопасностью

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), 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».

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 в процессе защиты презентаций рефератов, подготовленных в рамках самостоятельной работы по выбранной и согласованной теме.

Примерные темы презентаций (рефератов)

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

Тестовые вопросы по курсу

«Построение и совершенствование систем управления информационной безопасностью»

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

7.3.2. Промежуточная аттестация

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), 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».

Вопросы к экзамену 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

Пример билета по курсу
«Построение и совершенствование систем управления информационной безопасностью»

Билет №1

1. Аутстаффинг: сущность, исторические предпосылки, специфика, формы организации, преимущества и риски.
2. Способы получения и оценки информации.
3. Сферы применения аутсорсинга