Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Анатольевна
Должность: Ректор
Дата подписания: 10.10.2023 15:54:31
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.О.03.26 «Оценка экономической эффективности защиты информации»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2023

Рабочая программа дисциплины «Оценка экономической эффективности защиты информации» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации 17.11.2020 № 1427.

Составитель:
Старший преподаватель _Ю.С. Мунирова

РПД обсуждена на заседании ученого совета Высшей школы интеллектуальных систем и кибертехнологий
23.05.2025 г., протокол № 10

Директор Высшей школы интеллектуальных систем и кибертехнологий ___к.э.н. доцент_____ О.А. Филиппова

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Цель освоения дисциплины – формирование у обучающихся знаний, умений и навыков экономического обоснования решений по защите информации: оценки стоимости информационных активов и возможного ущерба, анализа рисков информационной безопасности, расчета затрат и показателей экономической эффективности систем защиты информации, подготовки исходных данных для технико-экономического обоснования проектных решений.

-формирование у обучающихся общепрофессиональных компетенций *в области использования информационно-коммуникационных технологий и т.п.*

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1. Демонстрирует знания основ правовых норм о противодействии проявлениям экстремизма, терроризма, коррупционному поведению	**Знать:** базовые экономические понятия (затраты, доходы, ущерб, риск, дисконтирование); принципы оценки эффективности инвестиций **Уметь:** сопоставлять альтернативные варианты решений по экономическим критериям; учитывать фактор времени и риска при оценке вариантов **Владеть:** навыками выбора экономически оптимального варианта системы защиты информации; навыками оформления технико-экономического обоснования и бюджета ИБ
	ИУК-10.2. Использует законодательные и другие нормативно-правовые акты, обеспечивающие борьбу с проявлениями экстремизма, терроризма, коррупции в различных областях жизнедеятельности, в том числе профессиональной.	
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИОПК-12.1. Знает порядок проектирования подсистем, средств обеспечения защиты информации	**Знать:** методы оценки стоимости информационных активов и ущерба; методы анализа рисков ИБ; структуру затрат на защиту информации; показатели экономической эффективности СЗИ **Уметь:** проводить инвентаризацию и оценку информационных активов; рассчитывать SLE, ALE, ROSI, NPV, IRR, срок окупаемости; оценивать совокупную стоимость владения СЗИ **Владеть:** навыками выбора экономически оптимального варианта системы защиты информации; навыками оформления технико-экономического обоснования и бюджета ИБ
	ИОПК-12.2. Формулирует требования и характеристики подсистем и средств обеспечения защиты информации для их последующего проектирования	
	ИОПК-12.3. Осуществляет подготовку исходных данных для технико-экономического обоснования проектных решений	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части, Блока 1. Дисциплины (модули) образовательной программы (Б.1.О.03 Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем дисциплины по видам учебной работы

Общая трудоёмкость дисциплины составляет **__5_ з.е. (_180_ час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**180**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**96/60**
занятия лекционного типа (лекции)	48/28
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	48/32
лабораторные работы	-
Самостоятельная работа всего, в т.ч.:	**57/111**
Самоподготовка по темам (разделам) дисциплины	57/111
Выполнение курсового проекта /курсовой работы	36/ 36
Контроль (часы на экзамен, зачет)	**27/ 9**
Промежуточная аттестация	**Экзамен/защита КР**

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-10 ИОПК-10.1 ОПК-12 ИОПК-12.1	Тема 1. Экономика информационной безопасности: предмет, задачи, основные понятия. Содержание темы дисциплины: Информация как экономический ресурс и товар. Предмет и задачи экономики информационной безопасности. Основные понятия: стоимость информационного актива, ущерб, риск, затраты на защиту, эффективность. Виды эффективности системы защиты информации: целевая, техническая, экономическая. Подходы к оценке эффективности: затратный, рисковый, доходный. Экономические аспекты в нормативных документах (ГОСТ Р ИСО/МЭК 27001, 27005).	5 / 4				Устный опрос, тест
	Практическое занятие № 1. Анализ подходов к оценке эффективности защиты информации; разбор кейсов экономических последствий инцидентов ИБ			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-12 ИОПК-12.1 ИОПК-12.2	Тема 2. Оценка стоимости информационных активов и возможного ущерба Содержание темы дисциплины Инвентаризация и классификация информационных активов. Методы оценки стоимости информации: затратный (стоимость создания/восстановления), рыночный, доходный. Оценка ценности по критериям конфиденциальности, целостности, доступности. Виды ущерба: прямой и косвенный, материальный и репутационный, упущенная выгода, штрафные санкции регуляторов. Методики расчета ущерба от утечки персональных данных и простоя информационных систем	5 / 4				Устный опрос, практическое задание
	Практическое занятие № 2. Инвентаризация и оценка стоимости информационных активов организации; расчет ущерба от нарушения конфиденциальности,			5 / 4		

	целостности, доступности					
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-12 ИОПК-12.1 ИОПК-12.2	Тема 3. Анализ и оценка рисков информационной безопасности Содержание темы дисциплины Процесс менеджмента риска ИБ по ГОСТ Р ИСО/МЭК 27005. Идентификация угроз и уязвимостей; Методика оценки угроз безопасности информации ФСТЭК России (2021). Качественные методы оценки риска: матрицы риска, экспертные оценки. Количественные методы: стоимость однократной потери (SLE = AV × EF), ежегодная частота реализации (ARO), ожидаемые годовые потери (ALE = SLE × ARO). Остаточный риск. Варианты обработки риска: снижение, передача, избежание, принятие. Программные средства анализа рисков	5 / 4-				Практическое задание, устный опрос
	Практическое занятие № 3. Количественная оценка рисков ИБ: расчет SLE, ARO, ALE; построение матрицы рисков			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-12 ИОПК-12.1 ИОПК-12.2	Тема 4. Затраты на обеспечение информационной безопасности Содержание темы дисциплины Классификация затрат на защиту информации: капитальные и текущие, прямые и косвенные, на предупреждение, контроль и устранение последствий. Затраты на приобретение и внедрение средств защиты, лицензии, аттестацию, персонал, обучение, аутсорсинг (услуги MSSP). Совокупная стоимость владения (TCO) средствами защиты информации: структура и методика расчета. Амортизация средств защиты. Соотношение затрат на защиту и величины риска	5 / 4				Практическое задание, тест
	Практическое занятие № 4. Расчет затрат и совокупной стоимости владения (TCO) системой защиты информации			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	

ОПК-10 ИОПК-10.2 ОПК-12 ИОПК-12.2	Тема 5. Показатели экономической эффективности инвестиций в защиту информации Содержание темы дисциплины Инвестиционный подход к защите информации. Показатель возврата инвестиций в безопасность ROSI. Учет фактора времени: дисконтирование денежных потоков, ставка дисконтирования. Чистый дисконтированный доход (NPV), внутренняя норма доходности (IRR), индекс доходности (PI), дисконтированный срок окупаемости (DPP). Предотвращенный ущерб как «доход» проекта по защите информации. Анализ чувствительности и учет неопределенности.	5 / 4-				Практическое задание, устный опрос
	Практическое занятие № 5. Расчет показателей ROSI, NPV, IRR, PI, DPP для проекта по защите информации (MS Excel / МойОфис Таблица)			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-10 ИОПК-10.2 ОПК-12 ИОПК-12.2 ИОПК-12.3	Тема 6. Методы оптимизации затрат и выбора варианта системы защиты информации Содержание темы дисциплины Постановка задачи оптимизации: минимизация суммы затрат на защиту и ожидаемого ущерба. Модель Гордона – Лёба (Gordon–Loeb). Критерий «стоимость – эффективность». Многокритериальный выбор средств защиты: метод анализа иерархий, взвешенные оценки. Учет требований регуляторов как ограничений оптимизации. Формирование оптимального набора мер защиты при ограниченном бюджете.	5 / 4				Устный опрос, решение ситуационных задач
	Практическое занятие № 6. Выбор оптимального варианта СЗИ методом анализа иерархий; оптимизация набора мер при ограниченном бюджете			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-12 ИОПК-12.2 ИОПК-12.3	Тема 7. Технико-экономическое обоснование проектных решений и бюджетирование ИБ	5 / 4				Практическое задание, доклад

	Содержание темы дисциплины Назначение и структура технико-экономического обоснования (ТЭО) проекта системы защиты информации. Исходные данные для ТЭО: перечень активов, модель угроз, требования, варианты решений, сметы. Расчет капитальных и эксплуатационных затрат по вариантам. Бюджет информационной безопасности: подходы к формированию (от рисков, от бенчмарков, от требований), согласование с руководством. Представление ТЭО лицам, принимающим решения.					
	Практическое занятие № 7. Подготовка технико-экономического обоснования и бюджета ИБ для условного предприятия			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-10 ИОПК-10.1 ОПК-12 ИОПК-12.3	Тема 8. Страхование информационных рисков. Оценка эффективности функционирования СОИБ Содержание темы дисциплины Передача риска: страхование киберрисков, условия и ограничения договоров страхования, расчет страховой премии. Метрики и ключевые показатели эффективности (KPI) информационной безопасности; подходы ГОСТ Р ИСО/МЭК 27004. Оценка зрелости процессов ИБ. Мониторинг экономических показателей СОИБ и корректировка инвестиционной политики.	5 / 4				Устный опрос, решение ситуационных задач, тест
	Практическое занятие № 8. Сравнение вариантов обработки риска (страхование / дополнительные меры); разработка системы KPI ИБ			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
	Выполнение курсовой работы				36/36	Самостоятельное выполнение с консультацией преподавателя
	ИТОГО	**48/28**	**- / -**	**48/32**	**57/111**	

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

-балльно-рейтинговая технология оценивания;

- электронное обучение;

- проблемное обучение;

- разбор конкретных ситуаций;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: *решение всех задач на практических занятиях.*

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.

2. Решение практических ситуаций и задач

Подготовка рефератов

3. Работу с ресурсами Интернет

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/

4.6. Методические указания для выполнения курсового проекта / работы

Выполнение курсового проекта/ работы способствует лучшему освоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся готовности к самостоятельной профессиональной деятельности, является этапом к выполнению выпускной квалификационной работы.

Курсовая работа является самостоятельной учебной работой, направленной на закрепление теоретических знаний и формирование навыков экономического обоснования проектных решений по защите информации на примере конкретного (условного) объекта. Курсовая работа выполняется в 7 семестре; объем – 25–35 страниц.

Примерная тематика курсовых работ:

1. Экономическое обоснование системы защиты персональных данных в организации (на примере …).
2. Оценка экономической эффективности внедрения системы предотвращения утечек информации (DLP).
3. Технико-экономическое обоснование выбора средств антивирусной защиты для корпоративной сети.
4. Оценка рисков информационной безопасности и обоснование мер по их снижению для предприятия торговли.
5. Экономическая оценка внедрения системы мониторинга событий ИБ (SIEM).
6. Обоснование затрат на обеспечение безопасности значимого объекта КИИ.
7. Сравнительная экономическая оценка собственного центра мониторинга ИБ и аутсорсинга (MSSP).
8. Оценка эффективности инвестиций в резервное копирование и обеспечение непрерывности бизнеса.
9. Технико-экономическое обоснование системы контроля и управления доступом на объекте.
10. Экономическое обоснование межсетевого экранирования и сегментации корпоративной сети.
11. Оценка экономической эффективности программы повышения осведомленности персонала в области ИБ.
12. Формирование бюджета информационной безопасности организации на основе анализа рисков.
13. Оценка целесообразности страхования киберрисков для организации финансового сектора.
14. Экономическое обоснование внедрения средств криптографической защиты каналов связи.
15. Оценка экономической эффективности системы защиты информации образовательной организации.

Структура курсовой работы: введение; 1 – анализ объекта защиты и информационных активов; 2 – оценка рисков информационной безопасности; 3 – выбор вариантов мер и средств защиты, расчет затрат; 4 – расчет показателей экономической эффективности и выбор оптимального варианта; заключение; список использованных источников; приложения.

Курсовая работа оформляется в соответствии с ГОСТ 7.32-2017 и локальными нормативными актами ФГБОУ ВО «ПВГУС», проверяется в системе «Антиплагиат» и защищается перед комиссией (руководителем).

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Нормативные правовые акты и нормативно-методические документы

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 N 149-ФЗ (последняя ред.) : [принят Гос. Думой 8 декабря 2006 г. : одобрен Советом Федерации 14 июля 2006 г.]. – Текст : электронный // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 09.11.2023).

2. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности : нац. стандарт РФ : дата введения: 2011-12-01. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: https://docs.cntd.ru/document/1200084141?ysclid=mvqjdlblri655785298 (дата обращения: 09.11.2023).

3. ГОСТ Р 58771-2019. Менеджмент риска. Технологии оценки риска : нац. стандарт РФ : дата введения: 2020-03-01. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: https://docs.cntd.ru/document/1200170253?ysclid=mvqjpagdam415968025 (дата обращения: 09.11.2023).

4. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования : нац. стандарт РФ : дата введения: 2022-01-01. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: https://docs.cntd.ru/document/1200181890?ysclid=mvqjs6asge226155770 (дата обращения: 09.11.2023).

5. ГОСТ 7.32-2017. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления : межгос. стандарт РФ : дата введения: 2018-07-01. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: https://docs.cntd.ru/document/1200157208?ysclid=mvqjvtifek27923506 (дата обращения: 09.11.2023).

Основная литература

6. Кормишкина, Л. А. Экономическая безопасность организации (предприятия) : учеб. пособие / Л. А. Кормишкина, Е. Д. Кормишкин, И. Е. Илякова. – Документ read. – Москва : РИОР [и др.], 2023. – 296 с. – (Высшее образование). – Прил. – URL: https://znanium.com/read?id=422327 (дата обращения: 09.11.2023). - Режим доступа: для

авториз. пользователей. – ISBN 978-5-369-01671-8. - 978-5-16-103849-9. – Текст : электронный.

7. Петрова, Е. А. Информационный менеджмент : учебник / Е. А. Петрова, Е. А. Фокина. – Документ Reader. – Санкт-Петербург [и др.] : Лань, 2022. – 142 с. – Прил. - Слов. терминов. - Англ.-рус. слов. сокр. - Законы и норматив. док. – URL: https://reader.lanbook.com/book/207098 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-8114-3923-2 : 0-00. – Текст : электронный.

8. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. – Документ read. – Москва : ФОРУМ [и др.], 2022. – 592 с. : ил. – (Высшее образование - Бакалавриат) (Высшее образование - Бакалавриат). – Предм. указ. – URL: https://znanium.ru/read?id=389857 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-8199-0730-6. - 978-5-16-106148-0. – Текст : электронный.

Дополнительная литература

9. Дубинин, Е. А. Оценка относительного ущерба безопасности информационной системы : монография / Е. А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. – Документ read. – Москва : РИОР [и др.], 2022. – 192 с. – (Научная мысль). – Прил. – URL: https://znanium.com/read?id=400262 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-369-01371-7. - 978-5-16-101863-7. – Текст : электронный.

10. Леонов, О. А. Практикум по экономике качества : учеб. пособие / О. А. Леонов, Н. Ж. Шкаруба, Г. Н. Темасова. – Документ Reader. – Санкт-Петербург [и др.] : Лань, 2023. – 156 с. – URL: https://e.lanbook.com/book/276560 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-507. – Текст : электронный.

11. Основы управления информационной безопасностью : учеб. пособие для вузов по направлениям подгот. (специальностям) укрупн. группы специальностей "Информ. безопасность" / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 2-е изд., испр. – Москва : Горячая линия -Телеком, 2016. – 244 с. : ил. – (Вопросы управления информационной безопасностью. Книга 1). – Прил. – ISBN 978-5-9912-0361-6 : 400-18. – Текст : непосредственный.

12. Поддержка принятия решений при проектировании систем защиты информации : монография / В. В. Бухтояров, М. Н. Жукова, В. В. Золотарев [и др.]. – Документ read. – Москва : ИНФРА-М, 2020. – 131 с. – (Научная мысль). – URL: https://znanium.com/read?id=343296 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-16-100714-3. – Текст : электронный.

13. Скрипкин, К. Г. Экономическая эффективность информационных систем в России : монография / К. Г. Скрипкин ; Моск. гос. ун-т им. М. В. Ломоносова, Экон. фак. – Документ read. – Москва : МАКС Пресс, 2014. – 155 с. – URL: http://znanium.com/bookread2.php?book=533938 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-317-04863-1. – Текст : электронный.

14. Фомичев, А. Н. Риск-менеджмент : учеб. по направлениям подгот. "Менеджмент", "Гос. и муницип. упр." (уровень бакалавриата) / А. Н. Фомичев. – 107-е изд. – Документ read. – Москва : Дашков и К, 2023. – 366 с. : табл. – (Учебные издания для бакалавров). – Слов. понятий и терминов. – URL: https://znanium.ru/read?id=431837 (дата

обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-394-05406-8. – Текст : электронный.

15. Шлегель, О. А. Экономическая эффективность предприятий сферы информационных услуг : монография / О. А. Шлегель. – Тольятти : ПВГУС, 2011. – 263 с. – ISBN 978-5-9581-0246-4 : 47-30;33-00;40-50;24-20;38-50;27-50;45-10;75-90;113-30;39-00;343-00;125-00. – Текст : непосредственный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. 3DNEWS.RU : Электронное периодическое издание : сайт. – Москва, 1997 - . - URL: https://3dnews.ru/ (дата обращения: 09.11.2023). – Текст: электронный.
2. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 09.11.2023). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
3. Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. – URL: http://docs.cntd.ru (дата обращения: 09.11.2023). – Текст электронный.
4. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения: 09.11.2023). - Текст : электронный.
5. Электронная библиотека. Техническая литература : сайт. - URL : http://techliter.ru/ (дата обращения: 09.11.2023). - Текст : электронный.
6. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.
7. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

компьютерные классы университета;

библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Экзамен/защита КР	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует*

необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Доклад/сообщение	5	4	20
Тестирование по темам лекционных занятий	4	10	40
Устный опрос, практическое задание	5	4	20
Творческий рейтинг (участие в конференциях, олимпиадах и т.п.) *Дополнительные баллы за активное изучение дисциплины и др.*	2	10	20
Итого по дисциплине			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

3.1. Вопросы для устного опроса

Тема 1. Экономика информационной безопасности: предмет, задачи, основные понятия

1. Почему информация рассматривается как экономический ресурс?

2. Раскройте понятия «ущерб», «риск», «затраты на защиту информации».

3. Чем экономическая эффективность СЗИ отличается от целевой (технической)?

4. Назовите основные подходы к оценке эффективности защиты информации.

Тема 2. Оценка стоимости информационных активов и возможного ущерба

1. Какие методы оценки стоимости информации вы знаете?

2. Как учитываются свойства конфиденциальности, целостности и доступности при оценке ценности актива?

3. Какие составляющие включает косвенный ущерб?

4. Как рассчитать ущерб от простоя информационной системы?

5. Какие штрафные санкции учитываются при оценке ущерба от утечки персональных данных?

Тема 3. Анализ и оценка рисков информационной безопасности

1. Каковы этапы процесса менеджмента риска ИБ по ГОСТ Р ИСО/МЭК 27005?

2. Как рассчитываются показатели SLE и ALE?

3. В чем преимущества и недостатки качественных методов оценки рисков?

4. Перечислите способы обработки риска.

5. Что такое остаточный риск и как определяется его приемлемый уровень?

Тема 4. Затраты на обеспечение информационной безопасности

1. Какие группы затрат на защиту информации выделяют?

2. Что включает совокупная стоимость владения СЗИ?

3. Как учитывается амортизация при расчете затрат?

4. Каковы особенности затрат при использовании аутсорсинга ИБ?

Тема 5. Показатели экономической эффективности инвестиций в защиту информации

1. Как рассчитывается показатель ROSI?

2. Почему при оценке проектов ИБ необходимо дисконтирование?

3. Раскройте экономический смысл NPV и IRR.

4. Как определяется дисконтированный срок окупаемости?

5. Для чего проводится анализ чувствительности?

Тема 6. Методы оптимизации затрат и выбора варианта системы защиты информации

1. Сформулируйте задачу оптимизации затрат на защиту информации.

2. Каков основной вывод модели Гордона – Лёба?

3. Как применяется метод анализа иерархий при выборе СЗИ?

4. Как учитываются обязательные требования регуляторов при оптимизации?

Тема 7. Технико-экономическое обоснование проектных решений и бюджетирование ИБ

1. Какова структура технико-экономического обоснования проекта СЗИ?

2. Какие исходные данные необходимы для подготовки ТЭО?

3. Какие подходы к формированию бюджета ИБ применяются?

4. Как обосновать бюджет ИБ перед руководством организации?

Тема 8. Страхование информационных рисков. Оценка эффективности функционирования СОИБ

1. Какие риски покрывает страхование киберрисков?

2. Как сравнить целесообразность страхования и внедрения дополнительных мер защиты?

3. Приведите примеры метрик и KPI информационной безопасности.

4. Для чего оценивается зрелость процессов ИБ?

3.2. Тестовые задания закрытого типа

*Примечание: правильные варианты ответов выделены **полужирным шрифтом с подчеркиванием**. В варианте ФОС, предъявляемом обучающимся, выделение снимается.*

1. Ожидаемые годовые потери (ALE) рассчитываются по формуле: (ИОПК-12.1)

а) ALE = AV × EF

б) ALE = SLE × ARO

в) ALE = SLE / ARO

г) ALE = AV + EF

2. Показатель SLE (Single Loss Expectancy) – это: (ИОПК-12.1)

а) ежегодная частота реализации угрозы

б) стоимость однократной потери от реализации угрозы

в) стоимость средства защиты

г) чистый дисконтированный доход

3. Коэффициент EF (Exposure Factor) характеризует: (ИОПК-12.1)

а) долю стоимости актива, теряемую при однократной реализации угрозы

б) число атак в год

в) ставку дисконтирования

г) срок окупаемости

4. Стоимость актива 2 000 000 руб., EF = 0,25, ARO = 2. Величина ALE составляет: (ИОПК-12.2)

а) 500 000 руб.

б) 1 000 000 руб.

в) 4 000 000 руб.

г) 250 000 руб.

5. Проект по защите информации экономически целесообразен, если: (ИУК-10.2)

а) NPV < 0

б) NPV > 0

в) IRR меньше ставки дисконтирования

г) PI < 1

6. Внутренняя норма доходности (IRR) – это ставка дисконтирования, при которой: (ИУК-10.1)

а) NPV максимален

б) NPV = 0

в) PI = 0

г) срок окупаемости равен году

7. Показатель ROSI рассчитывается как: (ИОПК-12.1)

а) (снижение ALE – затраты на защиту) / затраты на защиту

б) затраты на защиту / ALE

в) ALE × ARO

г) NPV / IRR

8. К способам обработки риска по ГОСТ Р ИСО/МЭК 27005 относятся (выберите все верные): (ИОПК-12.1)

а) снижение риска

б) передача риска

в) сокрытие риска

г) принятие риска

9. Страхование киберрисков является примером: (ИУК-10.1)

а) снижения риска

б) передачи риска

в) избежания риска

г) принятия риска

10. Совокупная стоимость владения (TCO) включает: (ИОПК-12.1)

а) только стоимость покупки лицензий

б) капитальные и эксплуатационные затраты за весь срок использования

в) только затраты на персонал

г) величину ожидаемого ущерба

11. Согласно модели Гордона – Лёба, оптимальные инвестиции в защиту информационного актива не превышают: (ИУК-10.2)

а) 50 % ожидаемых потерь

б) примерно 37 % (1/e) ожидаемых потерь

в) 100 % стоимости актива

г) 10 % бюджета ИТ

12. Упущенная выгода в результате простоя ИС относится к: (ИОПК-12.1)

а) прямому ущербу

б) косвенному ущербу

в) затратам на защиту

г) остаточному риску

13. Риск, остающийся после применения мер обработки, называется: (ИОПК-12.1)

а) исходным

б) остаточным

в) приемлемым

г) системным

14. Дисконтирование денежных потоков позволяет учесть: (ИУК-10.1)

а) инфляцию и альтернативную стоимость денег во времени

б) только налоги

в) стоимость лицензий

г) частоту атак

15. Метод оценки стоимости информации по затратам на ее создание или восстановление называется: (ИОПК-12.1)

а) доходным

б) рыночным

в) затратным

г) экспертным

16. Индекс доходности PI проекта больше 1 означает, что: (ИУК-10.2)

а) проект убыточен

б) дисконтированные выгоды превышают инвестиции

в) NPV < 0

г) IRR = 0

17. Методический документ ФСТЭК России, применяемый для определения актуальных угроз (2021 г.): (ИОПК-12.1)

а) Методика оценки угроз безопасности информации

б) Базовая модель угроз ПДн 2008 г.

в) ГОСТ 7.32-2017

г) Приказ ФСТЭК № 31

18. К капитальным затратам на защиту информации относятся: (ИОПК-12.2)

а) заработная плата администратора безопасности

б) приобретение и внедрение межсетевых экранов

в) ежемесячная абонентская плата за мониторинг

г) расходные материалы

19. Метод анализа иерархий используется для: (ИОПК-12.3)

а) расчета ставки дисконтирования

б) многокритериального выбора альтернатив

в) расчета ALE

г) определения EF

20. Стандарт, содержащий рекомендации по мониторингу, измерению и оценке результативности СМИБ: (ИОПК-12.1)

а) ГОСТ Р ИСО/МЭК 27004

б) ГОСТ Р ИСО/МЭК 27002

в) ГОСТ Р 50922

г) ГОСТ 34.201

Типовые задания к практическим занятиям

1. Проведите инвентаризацию информационных активов условной организации и оцените их стоимость затратным методом.
2. Для пяти угроз рассчитайте SLE, ARO и ALE; ранжируйте угрозы по величине ожидаемых годовых потерь.
3. Рассчитайте TCO межсетевого экрана нового поколения за 5 лет (приобретение, внедрение, поддержка, персонал, обучение).
4. Для проекта внедрения DLP-системы рассчитайте NPV, IRR, PI и DPP при ставке дисконтирования, равной ключевой ставке ЦБ РФ + 3 %.

5. Методом анализа иерархий выберите систему антивирусной защиты из трех альтернатив по четырем критериям.

6. Сформируйте оптимальный набор мер защиты при бюджете 2 млн руб. (задача о рюкзаке) и оцените остаточный риск.

7. Подготовьте ТЭО и проект бюджета ИБ для условного предприятия на год.

8. Сравните экономическую целесообразность страхования киберрисков и внедрения дополнительных мер защиты.

3.5. Темы докладов (рефератов)

1. Экономика инцидентов ИБ: статистика ущерба от утечек данных в России.
2. Модель Гордона – Лёба и ее практическое применение.
3. Рынок страхования киберрисков в России.
4. Аутсорсинг информационной безопасности: экономические аспекты.
5. Метрики и KPI информационной безопасности.
6. Оценка стоимости информации: зарубежный и отечественный опыт.
7. Оборотные штрафы за утечки персональных данных и их влияние на экономику ИБ.
8. Бюджетирование ИБ в крупных компаниях.
9. Импортозамещение средств защиты информации: экономическая оценка.
10. Экономические последствия атак программ-вымогателей.
11. Оценка эффективности обучения персонала по ИБ.
12. Программные средства анализа рисков ИБ.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *экзамен/ защита курсового проекта (курсовой работы) (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Защита курсового проекта/ работы. *Результаты защиты курсового проекта/ работы выставляются по пятибалльной системе оценивания ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно") с обязательным проставлением количества баллов, набранных в соответствии с балльно-рейтинговой системой (по стобалльной шкале).*

Перечень вопросов к защите курсового проекта /работы

1. Экономическое обоснование системы защиты персональных данных в организации (на примере …).
2. Оценка экономической эффективности внедрения системы предотвращения утечек информации (DLP).
3. Технико-экономическое обоснование выбора средств антивирусной защиты для корпоративной сети.
4. Оценка рисков информационной безопасности и обоснование мер по их снижению для предприятия торговли.
5. Экономическая оценка внедрения системы мониторинга событий ИБ (SIEM).
6. Обоснование затрат на обеспечение безопасности значимого объекта КИИ.
7. Сравнительная экономическая оценка собственного центра мониторинга ИБ и аутсорсинга (MSSP).

8. Оценка эффективности инвестиций в резервное копирование и обеспечение непрерывности бизнеса.

9. Технико-экономическое обоснование системы контроля и управления доступом на объекте.

10. Экономическое обоснование межсетевого экранирования и сегментации корпоративной сети.

Перечень вопросов к экзамену

УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

1. Информация как экономический ресурс. Предмет и задачи экономики информационной безопасности.
2. Основные понятия: стоимость актива, ущерб, риск, затраты, эффективность.
3. Виды эффективности системы защиты информации.
4. Подходы к оценке эффективности защиты информации.
5. Инвентаризация и классификация информационных активов.
6. Методы оценки стоимости информации.
7. Виды ущерба от реализации угроз ИБ.
8. Оценка ущерба от нарушения доступности информационных систем.
9. Оценка ущерба от утечки персональных данных.
10. Процесс менеджмента риска ИБ по ГОСТ Р ИСО/МЭК 27005.
11. Методика оценки угроз безопасности информации ФСТЭК России.
12. Качественные методы оценки рисков ИБ.
13. Количественные методы оценки рисков: SLE, ARO, ALE.
14. Способы обработки рисков. Остаточный риск.
15. Классификация затрат на защиту информации.
16. Совокупная стоимость владения средствами защиты информации.
17. Инвестиционный подход к защите информации.
18. Показатель ROSI: расчет и интерпретация.
19. Дисконтирование денежных потоков. Выбор ставки дисконтирования.
20. Чистый дисконтированный доход (NPV).
21. Внутренняя норма доходности (IRR) и индекс доходности (PI).
22. Дисконтированный срок окупаемости.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

23. Анализ чувствительности проектов по защите информации.
24. Задача оптимизации затрат на защиту информации.
25. Модель Гордона – Лёба.
26. Многокритериальный выбор средств защиты. Метод анализа иерархий.
27. Структура технико-экономического обоснования проекта СЗИ.
28. Исходные данные для ТЭО проектных решений по защите информации.
29. Бюджет информационной безопасности: подходы к формированию.
30. Страхование информационных (кибер-) рисков.
31. Метрики и KPI информационной безопасности.
32. Оценка зрелости процессов информационной безопасности.

4.2. Типовые практические задания к экзамену

1. Стоимость сервера с базой клиентов – 3 млн руб., EF = 0,3, ARO = 1,5. Рассчитайте SLE

и ALE.
2. ALE до внедрения СЗИ – 1,2 млн руб., после – 0,3 млн руб., годовая стоимость СЗИ – 0,45 млн руб. Рассчитайте ROSI и сделайте вывод.
3. Инвестиции – 2 млн руб.; ежегодный эффект – 0,8 млн руб. в течение 4 лет; ставка – 12 %. Рассчитайте NPV и PI.
4. Рассчитайте TCO СЗИ за 3 года: покупка 900 тыс. руб., внедрение 200 тыс. руб., поддержка 15 % от стоимости покупки в год, администрирование 300 тыс. руб. в год.
5. Выберите один из двух вариантов СЗИ по критерию минимума суммы затрат и ожидаемых потерь (исходные данные в билете).
6. Сравните страхование (премия 250 тыс. руб., франшиза 100 тыс. руб.) и внедрение мер защиты (400 тыс. руб., снижение ALE на 70 %) при ALE = 600 тыс. руб.
7. Определите простой и дисконтированный (ставка 10 %) сроки окупаемости проекта: инвестиции 1 млн руб., эффект 350 тыс. руб. в год.
8. Ранжируйте риски по матрице «вероятность – ущерб» (5 × 5) и предложите способ обработки для каждого.