МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Направление и направленность (профиль)
38.03.01 Экономика. Экономическая безопасность

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2022

Рабочая программа дисциплины (модуля) «Информационная безопасность предприятия» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.01 Экономика (утв. приказом Минобрнауки России от 12.08.2020г. №954) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 05.04.2017 г. N301).

Составитель(и):

Боршевников А.Е., старший преподаватель, Кафедра информационных технологий и систем, Aleksey.Borshevnikov@vvsu.ru

Павликов С.Н., кандидат технических наук, профессор, Кафедра информационных технологий и систем, Pavlikov.SN@vvsu.ru

Утверждена на заседании кафедры информационных технологий и систем от 31.05.2022 , протокол № 7

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Кийкова Е.В.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	1575633692
Номер транзакции	0000000000981A1B
Владелец	Кийкова Е.В.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью освоения дисциплины «Информационная безопасность предприятия» является формирование у студентов системы знаний в области методов обеспечения информационной безопасности предприятия.

Задачи освоения дисциплины: формирование умения обеспечить систематизированные знания, сформировать умения и навыки, которые позволят грамотно осуществлять менеджмент деятельностью предприятий с учетом функции защиты бизнеса от внутренних и внешних угроз его безопасности, а также аудит и контроль реализации данной функции.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
38.03.01 «Экономика» (Б-ЭУ)	ПКВ-2 : Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга	ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации	РД3	Знание	видов и источников угроз информационной безопасности, основных требований информационной безопасности
			РД4	Умение	выявлять угрозы информационной безопасности, планировать и осуществлять мероприятия по защите информации
		ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации	РД1	Знание	современных средств и методов защиты информации
			РД2	Умение	подобрать и использовать современные средства защиты информации при осуществлении коммуникаций

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Информационная безопасность предприятия» относится к элективным дисциплинам Блока 1 Дисциплины (модули) учебного плана. Для изучения данной дисциплины необходимы базовые знания в области информационных технологий, юриспруденции и экономики.

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества

академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
38.03.01 Экономика	ОФО	Б1.ДВ.Б	6	3	55	18	36	0	1	0	53	З

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение. Правовое обеспечение информационной безопасности предприятия	РД1, РД3	3	1	0	5	отчет по практической работе, собеседование
2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	РД1	0	4	0	4	отчет по практической работе, собеседование
3	Экономическая безопасность предприятия	РД3, РД4	4	1	0	5	отчет по практической работе, собеседование
4	Методики менеджмента информационной безопасности предприятия	РД2	0	4	0	4	отчет по практической работе, собеседование
5	Физическая и инженерно-техническая безопасность предприятия	РД2, РД4	3	2	0	5	отчет по практической работе, собеседование
6	Методики проведения аудита информационной безопасности предприятия	РД2	0	4	0	4	отчет по практической работе, собеседование
7	Кадровая безопасность предприятия	РД2, РД3	4	2	0	5	отчет по практической работе, собеседование
8	Противодействие техническим методам экономической разведки и промышленного шпионажа	РД4	0	4	0	4	отчет по практической работе, собеседование
9	Программно-аппаратное обеспечение информационной безопасности предприятия	РД4	4	2	0	5	отчет по практической работе, собеседование
10	Угрозы безопасности компьютерных сетей	РД2, РД3	0	4	0	4	отчет по практической работе, собеседование
11	Организация безопасного электронного документооборота	РД4	0	4	0	4	отчет по практической работе, собеседование
12	Криптографические методы защиты информации	РД4	0	4	0	4	отчет по практической работе, собеседование

Итого по таблице		**18**	**36**	**0**	**53**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение. Правовое обеспечение информационной безопасности предприятия.

Содержание темы: Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Организационное обеспечение информационной безопасности. Политика безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 2 Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Содержание темы: Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 3 Экономическая безопасность предприятия.

Содержание темы: Экономическая безопасность предприятия. Финансовые преступления и методы защиты от них.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 4 Методики менеджмента информационной безопасности предприятия.

Содержание темы: Обучение методам планирования и управления информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 5 Физическая и инженерно-техническая безопасность предприятия.

Содержание темы: Инженерная защита объектов. Защита информации от утечки по техническим каналам.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 6 Методики проведения аудита информационной безопасности предприятия.

Содержание темы: Обучение методам учета и анализа рисков.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 7 Кадровая безопасность предприятия.

Содержание темы: Особенности обеспечения кадровой безопасности предприятия. Мероприятия по обеспечению кадровой безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 8 Противодействие техническим методам экономической разведки и промышленного шпионажа.

Содержание темы: Рассмотрение примеров методов защиты от промышленного шпионажа и экономической разведки.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 9 Программно-аппаратное обеспечение информационной безопасности предприятия.

Содержание темы: Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекционное занятие, практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 10 Угрозы безопасности компьютерных сетей.

Содержание темы: Изучение настроек средств антивирусной защиты информации. Изучение настроек средств антивирусной защиты информации. Создание защищенного канала связи средствами виртуальной частной сети.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 11 Организация безопасного электронного документооборота.

Содержание темы: Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое занятие.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

Тема 12 Криптографические методы защиты информации.

Содержание темы: Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Использование средств стеганографии.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание.

Виды самостоятельной подготовки студентов по теме: Подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Успешное освоение дисциплины «Информационная безопасность предприятия» предполагает активную работу студентов на всех занятиях аудиторной формы: лекции, практические занятия, консультации, выполнение аттестационных мероприятий, эффективную самостоятельную работу.

В процессе изучения дисциплины «Информационная безопасность предприятия» необходимо ориентироваться на самостоятельную подготовку лекционного материала, подготовку к практическим занятия, ответы на вопросы для самоконтроля, самостоятельное выполнение некоторых разделов курса.

Контрольные вопросы для самостоятельной оценки качества освоения учебной дисциплины:

Тема 1. Введение. Правовое обеспечение информационной безопасности предприятия.

1. Что такое информационная безопасность?
2. Какие существуют модели информационной безопасности?
3. Право. Источники права.
4. Перечислите виды защищаемой информации.
5. Какие основные законы в области защиты информации в РФ?
6. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
7. Что такое концепция информационной безопасности?
8. Что такое доктрина информационной безопасности?
9. Что такое конфиденциальная информация?
10. Что такое персональные данные?
11. В каких случаях возможно использовать персональные данные без согласия обладателя?
12. Постановление правительства №1119.
13. Приказ ФСБ №378. Приказ ФСТЭК №21.
14. Приказ ФСТЭК №17.
15. Охарактеризуйте биометрические данные как персональные данные.
16. Что такое профессиональная тайна?

17. Что такое коммерческая тайна?
18. Что такое режим коммерческой тайны?
19. Что такое государственная тайна?
20. Опишите правовой режим государственной тайны.
21. ФЗ-374 и ФЗ-375.
22. ФЗ-63.
23. Какие главные государственные органы в области обеспечения информационной безопасности?
24. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
25. Какие основные международные стандарты в области информационной безопасности?
26. Расскажите в чем суть "оранжевой книги" (ISO 15408).
27. Как связаны международные стандарты и стандарты РФ?
28. Какие основные стандарты РФ в области информационной безопасности существуют?
29. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2012.
30. Что такое политика безопасности?
31. Служба безопасности предприятия. Функции.
32. Руководящие документы Гостехкомиссии. Основные положения.
33. Какие существуют принципы построения системы безопасности?
34. Как анализировать внутреннюю и внешнюю среды предприятия?
35. Зачем нужен анализ успехов и поражений на однородных рынках?
36. Как использовать чужой опыт?
37. Нужно ли применять теорию организации при построении системы безопасности?
38. Существуют ли отраслевая и региональная специфики?
39. Как подобрать менеджера безопасности?
40. Как управлять сложными системами безопасности?
41. Аутсорсинг или собственные силы?
42. Как определить достаточность финансирования безопасности?
43. Как организовать аудит системы безопасности?
44. Возможен ли контроль менеджера безопасности?
45. Что такое промышленный шпионаж?
46. Каковы основные способы промышленного шпионажа?
47. Какие методы сбора разведданных используются в промышленном шпионаже?
48. Что понимается под оперативными видами разведки?
49. Какую роль играют технические средства промышленного шпионажа?
50. Что такое электронная разведка?
51. Чем можно объяснить дуализм отношений бизнеса и государства в сфере промышленного шпионажа?
52. Кто и в каких случаях может получать информацию, составляющую банковскую тайну?

Тема 3. Экономическая безопасность предприятия

1. Что такое задолженность?
2. Какие виды задолженности, помимо банковской, существуют на рынке?
3. Что такое недобросовестное сотрудничество?
4. Какие классификации должников существуют?
5. Что такое мошенничество?
6. Как не допустить возникновения задолженности?
7. Каковы плюсы и минусы возврата долгов через аутсорсинг?
8. Каковы полномочия судебных приставов в процедуре возврата?
9. Что такое ситуационная осведомленность?
10. Каковы 6 элементов системы бизнес-аналитики?
11. Каковы задачи подразделения бизнес-разведки?

12. Как преодолеть проблему асимметричности информации?
13. Каковы ключевые позиции подтверждения факта существования контрагента?
14. Какие источники легитимной информации для бизнеса существуют в России?
15. Каковы основные правила определения надежности контрагента?
16. Назовите крупнейшие зарубежные консалтинговые компании.
17. Что понимается под стоп-факторами при изучении контрагента?
18. Как избежать операционных рисков при подготовке контрактов?
19. Каковы признаки компаний-однодневок?
20. Что такое сфера поглощений и слияний?
21. Чем от легитимного поглощения отличается рейдерский захват?
22. Какие типы агрессии известны в конкуренции?
23. Каковы способы превентивной защиты от рейдерского захвата?
24. Существует ли коррупция в сфере поглощений и слияний?
25. Можно ли привлечь к уголовной ответственности за действия по враждебному поглощению?
26. Что такое платежные системы?
27. Какие мировые платежные системы известны в настоящее время?
28. Какие платежные системы действуют на территории Российской Федерации?
29. Кто вырабатывает рекомендации по осуществлению банковского надзора?
30. Какие международные принципы банковского надзора существуют в настоящее время?
31. Какова роль центральных банков и подразделений внутреннего контроля?
32. Какие государственные органы осуществляют валютное регулирование и контроль в нашей стране?
33. Какие формы противоправных действий известны в сфере международных расчетов?
34. Как используются офшорные зоны для финансовых махинаций?
35. Почему международное сообщество пришло к необходимости противодействия отмывания денежных средств?
36. Каковы меры ФАТФ по борьбе с отмыванием денежных средств?
37. Что кроется за операциями по «обналичиванию» денежных средств?
38. Что понимается под термином «контроль политически значимых лиц»?
39. Какие виды предприятий являются субъектами ФЗ-115?
40. Какой федеральный орган является регулятором мер по ПОД/ФТ в сфере страховой деятельности?
41. Каковы меры воздействия Банка России по организации ПОД/ФТ в банковской сфере?

Тема 5. Физическая и инженерно-техническая безопасность предприятия

1. Что такое инженерная защита объектов?
2. Каким способом описывается инженерная защита. Описать модель.
3. Какие средства применяются для защиты 1-го периметра?
4. Какие средства применяются для защиты 2-го периметра?
5. Какие средства применяются для защиты 3-го периметра?
6. Биометрия. Биометрические характеристики.
7. Что такое технические каналы утечки информации?
8. Перечислите основные виды технических каналов утечки информации?
9. Перечислите методы защиты информации от утечки по визуальному каналу.
10. Перечислите методы защиты информации от утечки по электромагнитному каналу.
11. Перечислите методы защиты информации от утечки по электрическому каналу.
12. Перечислите методы защиты информации от утечки по индукционному каналу
13. Перечислите методы защиты информации от утечки по параметрическому каналу.
14. Перечислите методы защиты информации от утечки по воздушному каналу.
15. Перечислите методы защиты информации от утечки по вибрационному каналу.
16. Перечислите методы защиты информации от утечки по акустоэлектрическому каналу.
17. Перечислите методы защиты информации от утечки по оптико-электронному каналу.

18. Перечислите средства и методы защиты информации от утечки информации в телефонных линиях.
19. Можно ли использовать возможности полиции для охраны объектов бизнеса?
20. Что такое особые уставные задачи в сфере обращения оружия?
21. Вооружена ли ведомственная охрана объектов?
22. Как работает служба инкассации?
23. Кто не может быть частным охранником?
24. От каких угроз защищает объектовая охрана?
25. Зачем нужна личная охрана?
26. Какой пропускной режим можно считать эффективным и цивилизованным?
27. Какие возможности для работодателя (помимо штатных функций) предоставляет система контроля доступа?
28. Как обосновать законность применения средств аудио и видеозаписи в переговорных комнатах?
29. Можно ли сэкономить при планировании средств на прибытие групп быстрого реагирования по сигналу тревоги?
30. Как широко можно применять инженерно-технические средства безопасности для решения задач бизнеса?

Тема 7. Кадровая безопасность предприятия

1. Для чего нужна кадровая безопасность?
2. Чем кадровая безопасность отличается от безопасности персонала?
3. Что такое «искушение бизнесом»?
4. Почему злоупотребления менеджеров наиболее опасны для бизнеса?
5. Каковы кадровые риски организации?
6. В чем состоит контроль персонала?
7. Кого не стоит нанимать на работу?
8. Для чего изучают кандидатов при приеме на работу?
9. Какие известны типологии личности?
10. Можно ли обойтись без психологического тестирования при рекрутинге?
11. Каковы общие принципы профилактики нарушений со стороны персонала?
12. Каковы типовые формы внутреннего мошенничества?
13. Как правильно провести внутреннее служебное расследование?
14. Зачем нужен полиграф (детектор лжи)?
15. Почему меры по обеспечению кадровой безопасности должны соответствовать действующему законодательству?

Тема 9. Программно-аппаратное обеспечение информационной безопасности предприятия

1. Что такое программно-аппаратные средства защиты информации?
2. Что такое программные средства защиты информации?
3. Какие механизмы реализуют программно-аппаратные средства защиты информации?
4. Как реализуются механизмы программно-аппаратных средств защиты информации?
5. Какие компьютерные угрозы безопасности существуют?
6. Что такое сниффинг? Какие методы защиты против него существуют?
7. Что такое IP-спуффинг? Какие методы защиты против него существуют?
8. Что такое сетевая разведка? Какие методы защиты против нее существуют?
9. Что такое переполнение буфера? Какие методы защиты против него существуют?
10. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
11. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
12. Что такое фишинг? Какие методы защиты против него существуют?
13. Дополнительные способы защиты (резервное копирование, honeypot, DLP-системы,

сканеры безопасности, IDS, IPS).

14. Что такое компьютерный вирус? Какие виды вирусов существуют?
15. Опишите механизм работы вируса. Как вирус может проникнуть на компьютер?
16. Какие существуют механизмы работы антивируса? Опишите их.
17. Что такое файервол?
18. Что такое шифр? Какие виды шифров существуют?
19. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
20. Что такое цифровая подпись? Примеры.
21. Чем цифровая подпись отличается от электронной подписи?
22. Каковы основные правила обращения с носителями ЭП?
23. Что такое инфраструктура открытых ключей?
24. Что такое аутентификация? Что такое идентификация? Что такое верификация?
25. Что такое стеганография? Понятие стеганоконтейнера. Методы создания стеганоконтейнеров на основе аудиоинформации.
26. Реализация методов стеганографии и криптографии.
27. Каким требованиям должна отвечать модель обеспечения кибернетической безопасности предприятия?
28. В чем заключается роль персонала в вопросах обеспечения кибернетической безопасности предприятия?
29. Каков механизм мошеннических действий по проникновению в систему банк-клиент?
30. Каковы основные методы расследования кибер-преступлений?
31. В чем заключаются основы обеспечения сетевой безопасности?

Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационного материала, обеспечивающего тематические иллюстрации, соответствующие темам лекций, представленным в настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум : Учебное пособие [Электронный ресурс] : РИОР , 2020 - 320 - Режим доступа: https://znanium.com/catalog/document?id=357569

2. Гришина Н.В. Основы информационной безопасности предприятия : Учебное пособие [Электронный ресурс] : Инфра-М , 2021 - 216 - Режим доступа: https://znanium.com/catalog/document?id=366211

3. Жук А.П., Жук Е.П., Лепешкин О.М. и др. Защита информации : Учебное пособие [Электронный ресурс] : РИОР - Режим доступа: https://znanium.com/catalog/document?id=339378

7.2 Дополнительная литература

1. Бирюков А.А. Информационная безопасность [Электронный ресурс] : Издательство "ДМК Пресс" , 2017 - 434 - Режим доступа: https://e.lanbook.com/book/93278#book

2. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] : Издательство "Горячая линия-Телеком" , 2018 - 586 - Режим доступа: https://e.lanbook.com/book/111027#book

3. Введение в криптографию : Учебное пособие [Электронный ресурс] : Издательство ФОРУМ , 2020 - 240 - Режим доступа: https://znanium.com/catalog/document?id=345516

4. Галимов, Р.Р. Программно-аппаратные средства защиты информации : метод. указания / А.А. Рычкова; Оренбургский гос. ун- т; Р.Р. Галимов .— Оренбург : ОГУ, 2015 .— 89 с. : ил. — URL: https://lib.rucont.ru/efd/304038 (дата обращения: 20.02.2023)

5. Ерохин В.В., Погонышева Д.А., Степченко И.Г. Безопасность информационных систем : Учебные пособия [Электронный ресурс] : ФЛИНТА , 2015 - 182 - Режим доступа: https://e.lanbook.com/book/62972#book

6. Программно-аппаратная защита информации : Учебное пособие [Электронный ресурс] : Издательство ФОРУМ , 2019 - 352 - Режим доступа: https://znanium.com/catalog/document?id=340852

7. Сагдеев, К. М. Физические основы защиты информации : учебное пособие. Направление подготовки 10.03.01 – Информационная безопасность. Бакалавриат / В. И. Петренко, А. Ф. Чипига; К. М. Сагдеев .— Ставрополь : изд-во СКФУ, 2015 .— 394 с. — URL: https://lib.rucont.ru/efd/578849 (дата обращения: 20.02.2023)

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/
2. Электронная библиотечная система ZNANIUM.COM - Режим доступа: https://znanium.com/
3. Электронно-библиотечная система "РУКОНТ" - Режим доступа: https://rucont.ru/
4. Электронно-библиотечная система издательства "Лань" - Режим доступа: https://e.lanbook.com/
5. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
6. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Вуаль-Генератор акустических и виброакустических помеховых сигналов
- Мульт. медийный комплект № 2: Проектор Panasonic PT-LX26HE, потолочное крепление Tuarex Corsa, клеммный модуль Kramer WX -1N, коннектор VGA, экран Lumien Ecopicture
- Персональный компьютер №1 "B-tronix professional 3872\2015"
- Смарт-АВ (на базе СКМ-21.2)- Программно-аппаратный комплекс оценки эффективности защиты речевой информации от утечки по акустическому и виброакустическому каналам
- Соната-Р3.1 Средство активной защиты информации от утечки за счет побочных электромагнитных колебаний и наводок
- Спектроанализатор IFR2397

Программное обеспечение:

- Microsoft Windows 7 Ultimate Russian
- VMware Workstation 9 for Linux andWindows

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Направление и направленность (профиль)

38.03.01 Экономика. Экономическая безопасность

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2022

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
38.03.01 «Экономика» (Б-ЭУ)	ПКВ-2 : Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга	ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации
		ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-2 «Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации	РД 3	Знание	видов и источников угроз информационной безопасности, основных требований информационной безопасности	знание наиболее распространенных видов и источников угроз информационной безопасности, основных требований информационной безопасности в области профессиональной деятельности
	РД 4	Умение	выявлять угрозы информационной безопасности, планировать и осуществлять мероприятия по защите информации	выявление угроз информационной безопасности, планирование и осуществление мероприятия по защите информации в области профессиональной деятельности
ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации	РД 1	Знание	современных средств и методов защиты информации	знание основных современных средств и методов защиты информации, используемых в профессиональной деятельности
	РД 2	Умение	подобрать и использовать современные средства защиты информации при осуществлении коммуникаций	подбор и использование современных средств защиты информации при осуществлении коммуникаций в области профессиональной деятельности

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : современных средств и методов защиты информации	1.1. Введение. Правовое обеспечение информационной безопасности предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
РД2	Умение : подобрать и использовать современные средства защиты информации при осуществлении коммуникаций	1.4. Методики менеджмента информационной безопасности предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.5. Физическая и инженерно-техническая безопасность предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.6. Методики проведения аудита информационной безопасности предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.7. Кадровая безопасность предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.10. Угрозы безопасности компьютерных сетей	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
РД3	Знание : видов и источников угроз информационной безопасности, основных требований информационной безопасности	1.1. Введение. Правовое обеспечение информационной безопасности предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.3. Экономическая безопасность предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме

		1.7. Кадровая безопасность предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.10. Угрозы безопасности компьютерных сетей	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
РД4	Умение : выявлять угрозы информационной безопасности, планировать и осуществлять мероприятия по защите информации	1.3. Экономическая безопасность предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.5. Физическая и инженерно-техническая безопасность предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.8. Противодействие техническим методам экономической разведки и промышленного шпионажа	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.9. Программно-аппаратное обеспечение информационной безопасности предприятия	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.11. Организация безопасного электронного документооборота	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме
		1.12. Криптографические методы защиты информации	Практическая работа	Зачет в письменной форме
			Собеседование	Зачет в письменной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Собеседование	Практические работы	Зачет	Итого
Лекции	10			10
Практические занятия		60		60
Промежуточная аттестация			20	20
Самостоятельная работа	10			10
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, об наруживает всестороннее, систематическое и глубокое знание учебного матер иала, усвоил основную литературу и знаком с дополнительной литературой, ре комендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниям и, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: ос новные знания, умения освоены, но допускаются незначительные ошибки, нет очности, затруднения при аналитических операциях, переносе знаний и умени й на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительн о»	Студент демонстрирует сформированность дисциплинарных компетенций: в х оде контрольных мероприятий допускаются значительные ошибки, проявляетс я отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарн ым компетенциям, студент испытывает значительные затруднения при оперир овании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворитель но»	У студента не сформированы дисциплинарные компетенции, проявляется недо статочность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворитель но»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примерный перечень вопросов по темам

Пример вопросов для собеседования

Тема 1. Введение. Правовое обеспечение информационной безопасности предприятия.

1. Что такое информационная безопасность?
2. Какие существуют модели информационной безопасности?
3. Право. Источники права.
4. Перечислите виды защищаемой информации.
5. Какие основные законы в области защиты информации в РФ?
6. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
7. Что такое концепция информационной безопасности?
8. Что такое доктрина информационной безопасности?
9. Что такое конфиденциальная информация?
10. Что такое персональные данные?
11. В каких случаях возможно использовать персональные данные без согласия обладателя?
12. Постановление правительства №1119.
13. Приказ ФСБ №378. Приказ ФСТЭК №21.
14. Приказ ФСТЭК №17.
15. Охарактеризуйте биометрические данные как персональные данные.
16. Что такое профессиональная тайна?
17. Что такое коммерческая тайна?
18. Что такое режим коммерческой тайны?
19. Что такое государственная тайна?

20. Опишите правовой режим государственной тайны.

21. ФЗ-374 и ФЗ-375.

22. ФЗ-63.

23. Какие главные государственные органы в области обеспечения информационной безопасности?

24. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

25. Какие основные международные стандарты в области информационной безопасности?

26. Расскажите в чем суть "оранжевой книги" (ISO 15408).

27. Как связаны международные стандарты и стандарты РФ?

28. Какие основные стандарты РФ в области информационной безопасности существуют?

29. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2012.

30. Что такое политика безопасности?

31. Служба безопасности предприятия. Функции.

32. Руководящие документы Гостехкомиссии. Основные положения.

33. Какие существуют принципы построения системы безопасности?

34. Как анализировать внутреннюю и внешнюю среды предприятия?

35. Зачем нужен анализ успехов и поражений на однородных рынках?

36. Как использовать чужой опыт?

37. Нужно ли применять теорию организации при построении системы безопасности?

38. Существуют ли отраслевая и региональная специфики?

39. Как подобрать менеджера безопасности?

40. Как управлять сложными системами безопасности?

41. Аутсорсинг или собственные силы?

42. Как определить достаточность финансирования безопасности?

43. Как организовать аудит системы безопасности?

44. Возможен ли контроль менеджера безопасности?

45. Что такое промышленный шпионаж?

46. Каковы основные способы промышленного шпионажа?

47. Какие методы сбора разведданных используются в промышленном шпионаже?

48. Что понимается под оперативными видами разведки?

49. Какую роль играют технические средства промышленного шпионажа?

50. Что такое электронная разведка?

51. Чем можно объяснить дуализм отношений бизнеса и государства в сфере промышленного шпионажа?

52. Кто и в каких случаях может получать информацию, составляющую банковскую тайну?

Тема 3. Экономическая безопасность предприятия

1. Что такое задолженность?

2. Какие виды задолженности, помимо банковской, существуют на рынке?

3. Что такое недобросовестное сотрудничество?

4. Какие классификации должников существуют?

5. Что такое мошенничество?

6. Как не допустить возникновения задолженности?

7. Каковы плюсы и минусы возврата долгов через аутсорсинг?

8. Каковы полномочия судебных приставов в процедуре возврата?

9. Что такое ситуационная осведомленность?

10. Каковы 6 элементов системы бизнес-аналитики?

11. Каковы задачи подразделения бизнес-разведки?

12. Как преодолеть проблему асимметричности информации?

13. Каковы ключевые позиции подтверждения факта существования контрагента?

14. Какие источники легитимной информации для бизнеса существуют в России?
15. Каковы основные правила определения надежности контрагента?
16. Назовите крупнейшие зарубежные консалтинговые компании.
17. Что понимается под стоп-факторами при изучении контрагента?
18. Как избежать операционных рисков при подготовке контрактов?
19. Каковы признаки компаний-однодневок?
20. Что такое сфера поглощений и слияний?
21. Чем от легитимного поглощения отличается рейдерский захват?
22. Какие типы агрессии известны в конкуренции?
23. Каковы способы превентивной защиты от рейдерского захвата?
24. Существует ли коррупция в сфере поглощений и слияний?
25. Можно ли привлечь к уголовной ответственности за действия по враждебному поглощению?
26. Что такое платежные системы?
27. Какие мировые платежные системы известны в настоящее время?
28. Какие платежные системы действуют на территории Российской Федерации?
29. Кто вырабатывает рекомендации по осуществлению банковского надзора?
30. Какие международные принципы банковского надзора существуют в настоящее время?
31. Какова роль центральных банков и подразделений внутреннего контроля?
32. Какие государственные органы осуществляют валютное регулирование и контроль в нашей стране?
33. Какие формы противоправных действий известны в сфере международных расчетов?
34. Как используются офшорные зоны для финансовых махинаций?
35. Почему международное сообщество пришло к необходимости противодействия отмывания денежных средств?
36. Каковы меры ФАТФ по борьбе с отмыванием денежных средств?
37. Что кроется за операциями по «обналичиванию» денежных средств?
38. Что понимается под термином «контроль политически значимых лиц»?
39. Какие виды предприятий являются субъектами ФЗ-115?
40. Какой федеральный орган является регулятором мер по ПОД/ФТ в сфере страховой деятельности?
41. Каковы меры воздействия Банка России по организации ПОД/ФТ в банковской сфере?

Тема 5. Физическая и инженерно-техническая безопасность предприятия

1. Что такое инженерная защита объектов?
2. Каким способом описывается инженерная защита. Описать модель.
3. Какие средства применяются для защиты 1-го периметра?
4. Какие средства применяются для защиты 2-го периметра?
5. Какие средства применяются для защиты 3-го периметра?
6. Биометрия. Биометрические характеристики.
7. Что такое технические каналы утечки информации?
8. Перечислите основные виды технических каналов утечки информации?
9. Перечислите методы защиты информации от утечки по визуальному каналу.
10. Перечислите методы защиты информации от утечки по электромагнитному каналу.
11. Перечислите методы защиты информации от утечки по электрическому каналу.
12. Перечислите методы защиты информации от утечки по индукционному каналу
13. Перечислите методы защиты информации от утечки по параметрическому каналу.
14. Перечислите методы защиты информации от утечки по воздушному каналу.
15. Перечислите методы защиты информации от утечки по вибрационному каналу.
16. Перечислите методы защиты информации от утечки по акустоэлектрическому

каналу.

17. Перечислите методы защиты информации от утечки по оптико-электронному каналу.

18. Перечислите средства и методы защиты информации от утечки информации в телефонных линиях.

19. Можно ли использовать возможности полиции для охраны объектов бизнеса?

20. Что такое особые уставные задачи в сфере обращения оружия?

21. Вооружена ли ведомственная охрана объектов?

22. Как работает служба инкассации?

23. Кто не может быть частным охранником?

24. От каких угроз защищает объектовая охрана?

25. Зачем нужна личная охрана?

26. Какой пропускной режим можно считать эффективным и цивилизованным?

27. Какие возможности для работодателя (помимо штатных функций) предоставляет система контроля доступа?

28. Как обосновать законность применения средств аудио и видеозаписи в переговорных комнатах?

29. Можно ли сэкономить при планировании средств на прибытие групп быстрого реагирования по сигналу тревоги?

30. Как широко можно применять инженерно-технические средства безопасности для решения задач бизнеса?

Тема 7. Кадровая безопасность предприятия

1. Для чего нужна кадровая безопасность?

2. Чем кадровая безопасность отличается от безопасности персонала?

3. Что такое «искушение бизнесом»?

4. Почему злоупотребления менеджеров наиболее опасны для бизнеса?

5. Каковы кадровые риски организации?

6. В чем состоит контроль персонала?

7. Кого не стоит нанимать на работу?

8. Для чего изучают кандидатов при приеме на работу?

9. Какие известны типологии личности?

10. Можно ли обойтись без психологического тестирования при рекрутинге?

11. Каковы общие принципы профилактики нарушений со стороны персонала?

12. Каковы типовые формы внутреннего мошенничества?

13. Как правильно провести внутреннее служебное расследование?

14. Зачем нужен полиграф (детектор лжи)?

15. Почему меры по обеспечению кадровой безопасности должны соответствовать действующему законодательству?

Тема 9. Программно-аппаратное обеспечение информационной безопасности предприятия

1. Что такое программно-аппаратные средства защиты информации?

2. Что такое программные средства защиты информации?

3. Какие механизмы реализуют программно-аппаратные средства защиты информации?

4. Как реализуются механизмы программно-аппаратных средств защиты информации?

5. Какие компьютерные угрозы безопасности существуют?

6. Что такое сниффинг? Какие методы защиты против него существуют?

7. Что такое IP-спуффинг? Какие методы защиты против него существуют?

8. Что такое сетевая разведка? Какие методы защиты против нее существуют?

9. Что такое переполнение буфера? Какие методы защиты против него существуют?

10. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?

11. Что такое отказ в обслуживании? Какие методы защиты против него существуют?

12. Что такое фишинг? Какие методы защиты против него существуют?

13. Дополнительные способы защиты (резервное копирование, honey pot, DLP-системы, сканеры безопасности, IDS, IPS).

14. Что такое компьютерный вирус? Какие виды вирусов существуют?

15. Опишите механизм работы вируса. Как вирус может проникнуть на компьютер?

16. Какие существуют механизмы работы антивируса? Опишите их.

17. Что такое файервол?

18. Что такое шифр? Какие виды шифров существуют?

19. Что такое хеш-функция? Какие виды хеш-функций вы знаете?

20. Что такое цифровая подпись? Примеры.

21. Чем цифровая подпись отличается от электронной подписи?

22. Каковы основные правила обращения с носителями ЭП?

23. Что такое инфраструктура открытых ключей?

24. Что такое аутентификация? Что такое идентификация? Что такое верификация?

25. Что такое стеганография? Понятие стеганоконтейнера. Методы создания стеганоконтейнеров на основе аудиоинформации.

26. Реализация методов стеганографии и криптографии.

27. Каким требованиям должна отвечать модель обеспечения кибернетической безопасности предприятия?

28. В чем заключается роль персонала в вопросах обеспечения кибернетической безопасности предприятия?

29. Каков механизм мошеннических действий по проникновению в систему банк-клиент?

30. Каковы основные методы расследования кибер-преступлений?

31. В чем заключаются основы обеспечения сетевой безопасности?

Краткие методические указания

Собеседование проводится в устной форме во время последнего занятия по теме. Обучающемуся задается 2 случайных вопроса из списка вопросов. Обучающийся должен ответить на вопросы в течение 5 минут. Во время проведения собеседования использование литературы и других информационных ресурсов не допускается.

Шкала оценки

№	Баллы	Описание
4	16-20	Студент полностью ответил на заданные вопросы
3	11-15	Студент смог почти полностью ответить на заданные вопросы
2	6-10	Студент дал неполный ответ на вопросы, но смог передать основную суть вопроса
1	0-5	Студент не смог или фрагментарно ответил на заданные вопросы

5.2 Примеры заданий для выполнения практических работ

№ 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

На основе предложенного описания предприятия и изученной нормативно-распорядительной документации в области обеспечения информационной безопасности, группе студентов по 2-3 человека необходимо разработать обобщенную политику организации системы защиты персональных данных предприятия.

№ 2. Методики менеджмента информационной безопасности предприятия

На основе предложенного описания предприятия и изученной нормативно-распорядительной документации в области обеспечения информационной безопасности, группе студентов по 2-3 человека необходимо:

1. Загрузить ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности». Часть 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомиться с Приложениями C, D и E ГОСТа.

3. Выбрать три различных информационных актива организации (см. вариант).
4. Из Приложения D ГОСТа подобрать три конкретных уязвимости системы защиты указанных информационных активов. Пользуясь Приложением С ГОСТа написать три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
5. Пользуясь одним из методов (см. вариант) предложенных в Приложении Е ГОСТа произвести оценку рисков информационной безопасности.
6. Оценку ценности информационного актива произвести на основании возможных потерь для организации в случае реализации угрозы.

1. Подготовить отчет о проделанной работе.

№3. Методики проведения аудита информационной безопасности предприятия

На основе предложенного описания предприятия и изученной нормативно-распорядительной документации в области обеспечения информационной безопасности, группе студентов по 2-3 человека необходимо:

1. Составить план аудита.
2. Провести аудит информационной безопасности в соответствие со стандартом ISO 17799.
3. Провести оценку результатов воздействий от несанкционированного доступа к информационным и программным ресурсам.
4. Подготовить отчет о проделанной работе.

№4. Противодействие техническим методам экономической разведки и промышленного шпионажа

На основе предложенного описания предприятия и изученной нормативно-распорядительной документации в области обеспечения информационной безопасности, группе студентов по 2-3 человека необходимо:

1. Проанализировать угрозы, начиная с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы.
2. Принять решение по инженерно-технической защите охраняемого объекта, результаты оформить в соответствии с регламентами регулятора (ФСТЭК РФ).

№5. Угрозы безопасности компьютерных сетей

Имеются две локальные сети. В каждой из них есть сервер с установленным Kerio Winroute Firewall, с предустановленным VPN сервером. Студентам необходимо выполнить следующее рабочее задание под управлением ОС Linux Mint:

1. Объедините две локальные сети друг с другом, чтобы пользователи имели доступ к компьютерам и серверам из разрозненных сетей. Для этих задач нужно создать между двумя серверами, подключенными к Интернет, VPN Туннель.
2. На одну из виртуальных машин установите web-сервер .
3. На другую установите – Nmap .
4. Определите IP адрес виртуальной машины, где установлен web-сервер apache.
5. Произведите сканирование web-сервера всеми описанными методами (Изучение средств сканирования Nmap).
6. Установите Honeyd.
7. Ознакомьтесь с информацией по настройке Honeyd и стандартным содержимым файла /etc/honeypot/honeyd.conf.
8. Настройте Honeypot изменив содержание файла /etc/honeypot/honeyd.conf .
9. Запустите .
10. Запустите honeyd.
11. Произведите сканирование сети с honeypot.

12. Измените настройки Honeypot. Усложните конфигурационный файл. Добавьте несколько ловушек, измените информацию об ОС, информацию о роутере, об открытых портах и.т.д.
13. Запустите honeyd.
14. Произведите сканирование.
15. Подготовить отчет о проделанной работе.

№6. Организация безопасного электронного документооборота

Студентам необходимо выполнить следующее рабочее задание использованием криптографического программного GnuPG под управлением ОС Linux Mint/Windows 7:

1. Сгенерируйте пару ключей (публичный, приватный) по типу «DSA and ElGamal» под именем user1.
2. Проверьте корректность характеристик ключей.
3. Зашифруйте обычный текстовый файл на открытом ключе пользователя user1. Затем расшифруйте его.
4. Подпишите ранее созданный текстовый файл и просмотрите файл с цифровой подписью.
5. Измените содержимое текстового файла и проверьте подлинность цифровой подписи.
6. Создайте архив (tar –cvf) и создайте для него цифровую подпись.
7. Проверьте подлинность цифровой подписи архива.
8. Создайте в каталоге /mnt подкаталог со своей фамилией.
9. Экспортируйте в созданный каталог свой открытый ключ.
10. Сгенерируйте также свои ключи, но под именем user2.
11. Из каталога /mnt/ФИО_студента импортируйте открытый ключ user1
12. Убедитесь, что ключ добавился к вашему набору открытых ключей.
13. Зашифруйте file1 для пользователя user1 и сохраните его в директории /mnt/ФИО_студента.
14. Зашифруйте и подпишите file2 для пользователя user1.
15. Попробуйте расшифровать file1.asc и file2.asc при помощи ключа user2.
16. Перейдите в сеанс user1 и расшифруйте file1 и file2.
17. Подготовить отчет о проделанной работе.

№7. Криптографические методы защиты информации

Задание 1:

Студентам необходимо произвести шифрование сообщения (индивидуальные варианты выдаются преподавателем):

1. шифром атбаш;

1. шифром Цезаря;
2. шифром многоалфавитной замены (2 варианта);
3. с помощью квадрата Полибия;
4. с помощью таблицы Виженера;
5. методом перестановок;
6. с помощью системы Плейфейра.

Задание 2. Студентам необходимо произвести дешифрование сообщения (индивидуальные варианты выдаются преподавателем):

Краткие методические указания

На выполнение одного практического занятия отводится не более 3 двухчасовых занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме практического занятия.

Шкала оценки

№	Баллы	Описание

5	49–60	Студент демонстрирует умения на итоговом уровне: умеет свободно выполнять практическ ие задания, предусмотренные программой, свободно оперирует приобретенными умениями , применяет их в ситуациях повышенной сложности.
4	37–48	Студент демонстрирует умения на среднем уровне: освоил основные умения, но допускают ся незначительные ошибки, неточности, затруднения при аналитических операциях, перено се умений на новые, нестандартные ситуации.
3	24–36	Студент демонстрирует умения и навыки на базовом уровне: в ходе контрольных меропри тий допускаются значительные ошибки, проявляется отсутствие отдельных умений, навыко в по дисциплинарной компетенции, испытываются значительные затруднения при опериро вании умениями и при их переносе на новые ситуации.
2	11–23	Студент демонстрирует умения и навыки на уровне ниже базового: проявляется недостаточ ность умений и навыков.
1	0–10	Студентом проявляется полное или практически полное отсутствие умений и навыков.

5.3 Вопросы к зачету (письменная форма)

1. Что такое информационная безопасность? Охарактеризуйте методы и основные составляющие информационной безопасности.
2. Перечислите виды защищаемой информации. Классифицируйте и опишите основные угрозы информационной безопасности.
3. Перечислите и опишите модели информационной безопасности.
    1. Перечислите основные законы в области защиты информации РФ. Опишите основные положения стратегии национальной безопасности и Доктрины информационной безопасности.
    2. Охарактеризуйте биометрические данные как персональные данные. В каких случаях возможно использовать персональные данные без согласия обладателя?
    3. Перечислите и опишите основные международные стандарты в области информационной безопасности? Как связаны международные стандарты и стандарты РФ?

1. Что такое персональные данные? Опишите основные положения Федеральных законов в области персональных данных.

1. Что такое служебная и коммерческая тайна? Охарактеризуйте принципиальные различия. Опишите основные положения Федеральных законов в области служебной и коммерческой тайна.
2. Опишите правовой режим государственной тайны. Какие главные государственные органы РФ в области обеспечения информационной безопасности? Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

10. Опишите основные положения ГОСТ Р ИСО/МЭК 27002-2012 и ГОСТ Р ИСО/МЭК 27005-2010.

11. Опишите организационные и технические меры по защите персональных данных в системах обработки персональных данных.

12. Перечислите и опишите типы криптографических средств защиты информации в информационных системах обработки персональных данных.

13. Опишите требования к защите информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах.

14. Опишите требования к защите объектов критической информационной инфраструктуры.

15. Опишите требование к средствам антивирусной защиты. Классифицируйте средства антивирусной защиты.

16. Опишите требования к межсетевым экранам и средствам доверенной загрузки.

17. Перечислите и опишите основные положения основных руководящих документов Гостехкомиссии.

18. Опишите меры защиты информации в государственных информационных системах.

19. Что такое политика безопасности? Служба безопасности предприятия (структура и функции).

1. Как анализировать внутреннюю и внешнюю среды предприятия? Зачем нужен анализ успехов и поражений на однородных рынках? Как использовать чужой опыт?
2. Нужно ли применять теорию организации при построении системы безопасности? Существуют ли отраслевая и региональная специфики?
3. Как подобрать менеджера безопасности? Как управлять сложными системами безопасности? Аутсорсинг или собственные силы?

23. Что такое аудит информационной безопасности? Опишите методику проведения аудита информационной безопасности.

24. Опишите методику оценки рисков нарушения информационной безопасности.

1. Что такое промышленный шпионаж? Каковы основные способы промышленного шпионажа?
2. Какие методы сбора разведданных используются в промышленном шпионаже? Что понимается под оперативными видами разведки?
3. Какую роль играют технические средства промышленного шпионажа? Что такое электронная разведка?
4. Чем можно объяснить дуализм отношений бизнеса и государства в сфере промышленного шпионажа? Кто и в каких случаях может получать информацию, составляющую банковскую тайну?

29. Что такое инженерная защита объектов? Каким способом описывается инженерная защита? Описать модель.

30. Что такое модель охраны периметра? Описать модель. Какие средства применяются для защиты 1-го, 2-го и 3-го периметров?

31. Какие средства применяются для защиты 2-го периметра?

32. Какие средства применяются для защиты 3-го периметра?

33. Перечислите и опишите технические средства обнаружения несанкционированного доступа к охраняемому объекту.

34. Что такое биометрия. Опишите биометрические характеристики (приведите примеры).

35. Что такое технические каналы утечки информации? Перечислите и опишите основные виды технических каналов утечки информации.

36. Опишите методику спецпроверки, специсследования и спецобследования? В чем состоит принципиальное различие между указанными методиками?

37. Перечислите и опишите методы защиты информации от утечки по зрительному и воздушному каналам.

38. Перечислите методы защиты информации от утечки по электромагнитному и электрическому каналам.

39. Перечислите методы защиты информации от утечки по индукционному каналу и параметрическому каналам.

40. Перечислите методы защиты информации от утечки по вибрационному и акустоэлектрическому каналам.

41. Перечислите методы защиты информации от утечки.

42. Перечислите средства и методы защиты информации по оптикоэлектронному каналу и от утечки информации в телефонных линиях.

43. Можно ли использовать возможности полиции для охраны объектов бизнеса? Что такое особые уставные задачи в сфере обращения оружия?

44. Как работает служба инкассации? Кто не может быть частным охранником? От каких угроз защищает объектовая охрана? Какой пропускной режим можно считать

эффективным и цивилизованным?

45. Какие возможности для работодателя (помимо штатных функций) предоставляет система контроля доступа? Как обосновать законность применения средств аудио и видеозаписи в переговорных комнатах?

46. Можно ли сэкономить при планировании средств на прибытие групп быстрого реагирования по сигналу тревоги? Как широко можно применять инженерно-технические средства безопасности для решения задач бизнеса?

1. Для чего нужна кадровая безопасность? Чем кадровая безопасность отличается от безопасности персонала? Что такое «искушение бизнесом»?
2. Почему злоупотребления менеджеров наиболее опасны для бизнеса? Каковы кадровые риски организации? В чем состоит контроль персонала? Кого не стоит нанимать на работу?
3. Для чего изучают кандидатов при приеме на работу? Какие известны типологии личности? Каковы общие принципы профилактики нарушений со стороны персонала?
4. Каковы типовые формы внутреннего мошенничества? Как правильно провести внутреннее служебное расследование? Почему меры по обеспечению кадровой безопасности должны соответствовать действующему законодательству?

51. Что такое программно-аппаратные средства защиты информации? Какие механизмы реализуют программно-аппаратные средства защиты информации? Какие компьютерные угрозы безопасности существуют?

52. Что такое сетевая разведка? Какие методы защиты против нее существуют? Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?

53. В чем суть атаки «отказ в обслуживании»? Ее отличия от распределенной кибератаки «отказ в обслуживании»? Какие методы защиты против него существуют?

54. Перечислите и опишите основные виды программных уязвимостей. Какие методы защиты против них существуют?

55. Что такое переполнение буфера? Перечислите о пишите методы защиты.

56. Что такое дефекты форматных строк? Перечислите о пишите методы защиты.

57. Что такое целочисленные переполнения? Перечислите о пишите методы защиты.

58. Что такое «состояние гонки». Перечислите опишите методы защиты.

59. Что такое атака «Человек по середине»? Что такое IP-спуффинг? Какие методы защиты против указанных атак существуют?

60. В чем суть технологии VPN? Можно ли рассматривать использование SSH как реализацию VPN? Может ли шифрование полностью защитить данные, передаваемые через VPN? С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

61. Что такое социальная инженерия? Что такое фрод. Перечислите о опишите методы борьбы с фродом.

62. Что такое фишинг? Какие методы защиты против него существуют? Что такое кардинг? Опишите методы защиты от кардинга.

63. Назначение, цели, описание Honeypot. Как выявлять Honeypot?

64. Что такое и для чего используются средства контекстной фильтрации? Охарактеризуйте DLP-системы и SIEM-системы.

65. Что такое сканеры безопасности? Для чего используется RPC-сканирование? Перечислите и опишите основные методы сканирования.

66. Что такое и для чего используются системы обнаружения вторжений и системы предотвращения вторжений?

67. Что такое вредоносные программы? Классифицируйте компьютерные вирусы. Опишите типовой механизм работы вируса. Что такое эксплоит?

68. Что такое шифр? Какие виды шифров существуют? Опишите принципы построения и принципиальные отличия.

69. Что такое поточный и блочный шифры? Опишите принципы построения и

принципиальные отличия.

70. Что такое хеш-функция (описать принцип работы)? Какие виды хеш-функций вы знаете?

Что такое Дерево Меркла?

71. Что такое цифровая подпись? Опишите цифровую подпись RSA и Эль-Гамаля.

72. Что такое инфраструктура открытых ключей? Описать методику распределения ключей на примере подписания сертификата. Описать зависимость публичного и приватного ключей

73. Что такое аутентификация, идентификация, верификация, авторизация. Опишите принципиальные отличия между ними. Приведите примеры.

74. Простейшие протоколы идентификации.

75. Что такое стеганография и стеганоконтейнер? Какие виды стеганоконтейнеров существуют? Опишите методы создания стеганоконтейнеров на основе текстовой информации, видеоинформации и аудиоинформации.

76. Каким требованиям должна отвечать модель обеспечения кибернетической безопасности предприятия? В чем заключается роль персонала в вопросах обеспечения кибернетической безопасности предприятия?

77. Каков механизм мошеннических действий по проникновению в систему банк-клиент?

78. Каковы основные методы расследования кибер-преступлений?

Краткие методические указания

Зачет проводится в письменной форме. Обучающемуся задается 2 случайных вопроса из списка вопросов. Обучающийся должен письменно ответить на вопросы в течение 60 минут. Во время проведения зачета использование литературы и других информационных ресурсов не допускается.

Шкала оценки

№	Баллы	Описание
4	16-20	Студент полностью ответил на заданные вопросы
3	11-15	Студент смог почти полностью ответить на заданные вопросы
2	6-10	Студент дал неполный ответ на вопросы, но смог передать основную суть вопроса
1	0-5	Студент не смог или фрагментарно ответил на заданные вопросы