МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Специальность и специализация

38.05.01 Экономическая безопасность. Экономико-правовое обеспечение экономической безопасности

Год набора на ОПОП
2019

Форма обучения
очная

Владивосток 2022

Рабочая программа дисциплины (модуля) «Информационная безопасность предприятия» составлена в соответствии с требованиями ФГОС ВО по направлению(ям) подготовки 38.05.01 Экономическая безопасность (утв. приказом Минобрнауки России от 16.01.2017г. №20) 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

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	000000000097EBC6
Владелец	Кийкова Е.В.

Заведующий кафедрой (выпускающей)
Варкулевич Т.В.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	1575458423
Номер транзакции	0000000000981511
Владелец	Варкулевич Т.В.

1. Цель и задачи освоения дисциплины (модуля)

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.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемыми результатами обучения по дисциплине являются знания, умения, навыки, соотнесенные с компетенциями, которые формирует дисциплина, и обеспечивающие достижение планируемых результатов по образовательной программе в целом. Перечень компетенций, формируемых в результате изучения дисциплины (модуля), приведен в таблице 1.

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

Название ОПОП ВО, сокращенное	Код компетенции	Формулировка компетенции	Планируемые результаты обучения	
38.05.01 «Экономическая безопасность» (ЭБ)	ПК-43	способность принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	Знания:	видов и источников угроз информационной безопасности, основных требований информационной безопасности
			Умения:	выявлять угрозы информационной безопасности, планировать и осуществлять мероприятия по защите информации
			Навыки:	владения современными средствами обеспечения информационной безопасности
	ОПК-3	способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	Знания:	современных средств и методов защиты информации
			Умения:	подобрать и использовать современные средства защиты информации при осуществлении коммуникаций

3. Место дисциплины (модуля) в структуре основной образовательной программы

Дисциплина «Информационная безопасность предприятия» входит в базовую часть Блока 1 Дисциплины (модули) учебного плана.

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Администрирование территорий с особым экономическим

режимом», «Банковское дело», «Безопасность жизнедеятельности», «Криминалистика», «Организация предприятий малого и среднего бизнеса», «Основы экономической безопасности предприятия (бизнеса)», «Практический аудит», «Проектная деятельность», «Специальная подготовка (Предпринимательское право)», «Специальная подготовка (Управление рисками организации)», «Судебные и правоохранительные органы», «Теория права», «Уголовное право», «Уголовный проце. На данную дисциплину опираются «Проектный менеджмент базовый курс», «Производственная преддипломная практика», «Судебная экономическая экспертиза», «Управление качеством базовый курс».

4. Объем дисциплины (модуля)

Объем дисциплины 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		
38.05.01 Экономическая безопасность	ОФО	С.1.Б	8	3	55	18	36	0	1	0	53	Э

5. Структура и содержание дисциплины (модуля)

5.1 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	Кол-во часов, отведенное на				Форма текущего контроля
		Лек	Практ	Лаб	СРС	
1	Введение. Правовое обеспечение информационной безопасности предприятия	3	1	0	5	подготовка к контрольным вопросам собеседования, подготовка отчета по практической работе, подготовка к промежуточной аттестации
2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	0	4	0	4	отчет по практической работе, собеседование
3	Экономическая безопасность предприятия	4	1	0	5	отчет по практической работе, собеседование
4	Методики менеджмента информационной безопасности предприятия	0	4	0	4	отчет по практической работе, собеседование

5	Физическая и инженерно-техническая безопасность предприятия	3	2	0	5	отчет по практической работе, собеседование
6	Методики проведения аудита информационной безопасности предприятия	0	4	0	4	отчет по практической работе, собеседование
7	Кадровая безопасность предприятия	4	2	0	5	отчет по практической работе, собеседование
8	Противодействие техническим методам экономической разведки и промышленного шпионажа	0	4	0	4	отчет по практической работе, собеседование
9	Программно-аппаратное обеспечение информационной безопасности предприятия	4	2	0	5	отчет по практической работе, собеседование
10	Угрозы безопасности компьютерных сетей	0	4	0	4	отчет по практической работе, собеседование
11	Организация безопасного электронного документооборота	0	4	0	4	отчет по практической работе, собеседование
12	Криптографические методы защиты информации	0	4	0	4	отчет по практической работе, собеседование
Итого по таблице		**18**	**36**	**0**	**53**	

5.2 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: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: отчет по практической работе, собеседование.

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 занятие.

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: лекция, 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 занятие.

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: лекция, 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 занятие.

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: лекция, 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 занятие.

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: лекция, 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 занятие.

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 занятие.

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

6. Методические указания по организации изучения дисциплины (модуля)

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 пункте 5 настоящей РПД.

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.

7. 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 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.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 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=379717

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

8.2 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)

8.3 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/

9. Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

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