МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление и направленность (профиль)

38.03.05 Бизнес-информатика. Бизнес-аналитика

Год набора на ОПОП
2020

Форма обучения
очная

Владивосток 2022

Рабочая программа дисциплины (модуля) «Информационная безопасность и защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению(ям) подготовки 38.03.05 Бизнес-информатика (утв. приказом Минобрнауки России от 11.08.2016г. №1002) 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	000000000097DD03
Владелец	Кийкова Е.В.

Заведующий кафедрой (выпускающей)
Мазелис Л.С.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	1575656200
Номер транзакции	00000000009823B8
Владелец	Мазелис Л.С.

1. Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины "Информационная безопасность и защита информации" является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи освоения дисциплины: формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли; формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов; формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств

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	
38.03.05 «Бизнес-информатика» (Б-БИ)	ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности	Знания:	действующее законодательство в области информационной безопасности
			Умения:	использовать действующее законодательство в области информационной безопасности для организации бизнес-процессов
			Навыки:	методами анализа нормативно-распорядительной документации, регулирующих отношения в области информационной безопасности
	ПК-9	Организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	Знания:	современные технологии, методики и средства защиты информации
			Умения:	управлять информационной безопасностью организации
			Навыки:	методами оценки рисков информационной безопасности и современными технологиями защиты информации

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

Дисциплина «Информационная безопасность и защита информации» входит в

базовую часть Блока 1 Дисциплины (модули)

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Математический анализ модуль 1», «Математический анализ модуль 2», «Объектно-ориентированное программирование», «Операционные системы», «Проектирование информационных систем», «Сети ЭВМ и телекоммуникации». На данную дисциплину опираются «Производственная практика по получению профессиональных умений и опыта профессиональной деятельности», «Производственная преддипломная практика».

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		
38.03.05 Бизнес-информатика	ОФО	Бл1.Б	7	4	52	34	17	0	1	0	92	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 в информационную безопасность	2	0	0	7	собеседование
2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	0	2	0	7	отчет по практической работе
3	Правовое обеспечение информационной безопасности	6	0	0	7	собеседование
4	Использование криптографических средств защиты информации	0	3	0	7	отчет по практической работе
5	Организационное обеспечение информационной безопасности	6	0	0	8	собеседование
6	Реализация работы инфраструктуры открытых ключей	0	3	0	8	отчет по практической работе

7	Технические средства и методы защиты информации	6	0	0	8	собеседование
8	Средства стеганографии для защиты информации	0	3	0	8	отчет по практической работе
9	Программно-аппаратные средства и методы обеспечения информационной безопасности	8	0	0	8	собеседование
10	Настройка безопасного сетевого соединения	0	3	0	8	отчет по практической работе
11	Криптографические методы защиты информации	6	0	0	8	собеседование
12	Антивирусные средства защиты информации	0	3	0	8	отчет по практической работе
Итого по таблице		**34**	**17**	**0**	**92**	

5.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение в информационную безопасность.

Содержание темы: Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.

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

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

Тема 3 Правовое обеспечение информационной безопасности.

Содержание темы: Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

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

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

Тема 4 Использование криптографических средств защиты информации.

Содержание темы: Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

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

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

Тема 5 Организационное обеспечение информационной безопасности.

Содержание темы: Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Формы и методы проведения занятий по теме, применяемые образовательные

технологии: Лекционное занятие.

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

Тема 6 Реализация работы инфраструктуры открытых ключей.

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 задание.

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

Тема 7 Технические средства и методы защиты информации.

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

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

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

Тема 8 Средства стеганографии для защиты информации.

Содержание темы: Использование средств стеганографии для защиты файлов.

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

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

Тема 9 Программно-аппаратные средства и методы обеспечения информационной безопасности.

Содержание темы: Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

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

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

Тема 10 Настройка безопасного сетевого соединения.

Содержание темы: 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 отчета по практической работе, подготовка к промежуточной аттестации.

Тема 11 Криптографические методы защиты информации.

Содержание темы: Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

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

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

Тема 12 Антивирусные средства защиты информации.

Содержание темы: Изучение настроек средств антивирусной защиты информации.

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

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

6. Методические указания по организации изучения дисциплины (модуля)

Текущая самостоятельная работа по курсу «Информационная безопасность и защита информации» направлена на углубление и закрепление знаний, на развитие практических умений и включает такие виды работ, как:

- работа с лекционным материалом;
- работа с рекомендованной литературой при подготовке к практическим занятиям;
- подготовка к экзамену.

При изучении дисциплины "Информационная безопасность и защита информации" рекомендуется рейтинговая технология обучения, которая позволяет реализовать непрерывную и комплексную систему оценивания учебных достижений студентов. Непрерывность означает, что текущие оценки не усредняются (как в традиционной технологии), а непрерывно складываются на протяжении семестра при изучении первого или второго модуля. Комплексность означает учет всех форм учебной и творческой работы студента в течение семестра.

Рейтинг направлен на повышение ритмичности и эффективности самостоятельной работы студентов. Он основывается на широком использовании тестов и заинтересованности каждого студента в получении более высокой оценки знаний по дисциплине.

Принципы рейтинга: непрерывный контроль (в идеале на каждом из аудиторных занятий) и получение более высокой оценки за работу, выполненную в срок. При проведении практических занятий необходимо предусматривать широкое использование активных и интерактивных форм (компьютерных симуляций, деловых и ролевых игр).

Рейтинг включает в себя два вида контроля: текущий, промежуточный и итоговый по дисциплине.

Текущий контроль (ТК) - основная часть рейтинговой системы, основанная на беглом опросе раз в неделю или в две недели. Формы: оценка за сдачу теоретических минизачетов, выполнение индивидуальных заданий и практических работ. Важнейшей формой ТК, позволяющей опросить всех студентов на одном занятии являются теоретические модули, на которых студенты самостоятельно отвечают на вопросы для самостоятельной оценки.

Контрольные вопросы для самостоятельной оценки качества освоения учебной дисциплины

Тема 1. Введение в информационную безопасность

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?

11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности

1. Право. Источники права.
2. Какие основные законы в области защиты информации в РФ?
3. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
4. Стратегия национальной безопасности. Доктрина информационной безопасности.
5. Что такое конфиденциальная информация?
6. Что такое персональные данные?
7. В каких случаях возможно использовать персональные данные без согласия обладателя?
8. Охарактеризуйте биометрические данные как персональные данные.
9. Что такое профессиональная тайна?
10. Что такое служебная тайна?
11. Что такое коммерческая тайна?
12. Что такое режим коммерческой тайны?
13. Что такое государственная тайна?
14. Опишите правовой режим государственной тайны.
15. ФЗ-149.
16. ФЗ-152.
17. ФЗ-98.
18. ФЗ-390.
19. ФЗ-395-1.
20. ФЗ-126.
21. ФЗ-374 и ФЗ-375.
22. Постановление правительства №1119.

Тема 3. Организационное обеспечение информационной безопасности

1. Какие основные международные стандарты в области информационной безопасности?
2. "Оранжевая книга"
3. ISO/IEC 15408.
4. Как связаны международные стандарты и стандарты РФ?
5. ГОСТ Р ИСО/МЭК 27002-2012.
6. ГОСТ Р ИСО/МЭК 27005-2010.
7. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
8. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
9. Приказ ФСБ №378.
10. Приказ ФСТЭК №21.
11. Приказ ФСТЭК №17.
12. Приказ ФСТЭК №31.
13. Приказ ФСТЭК №28.
14. Приказ ФСТЭК №638.
15. Приказ ФСТЭК №9.
16. Приказ ФСТЭК №119.
17. Приказ Гостехкомиссии №114.
18. Руководящие документы Гостехкомиссии.
19. Меры защиты информации в государственных информационных системах. (Методический документ ФСТЭК).
20. Что такое политика безопасности?

21. Служба безопасности предприятия. Структура. Функции.
22. Типовая инструкция сотрудника по обеспечению информационной безопасности.
23. Экономическая разведка. Промышленный шпионаж.

Тема 4. Технические средства и методы защиты информации

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. Пожарные сигнализации.
7. Охранные сигнализации
8. Биометрия. Биометрические характеристики.
9. Что такое технические каналы утечки информации?
10. Перечислите основные виды технических каналов утечки информации?
11. Что такое спецпроверка?
12. Что такое специсследование?
13. Что такое спецобследование?
14. Перечислите методы защиты информации от утечки по зрительному каналу.
15. Перечислите методы защиты информации от утечки по электромагнитному каналу.
16. Перечислите методы защиты информации от утечки по электрическому каналу.
17. Перечислите методы защиты информации от утечки по индукционному каналу
18. Перечислите методы защиты информации от утечки по параметрическому каналу.
19. Перечислите методы защиты информации от утечки по воздушному каналу.
20. Перечислите методы защиты информации от утечки по вибрационному каналу.
21. Перечислите методы защиты информации от утечки по акустоэлектрическому каналу.
22. Перечислите методы защиты информации от утечки по оптикоэлектронному каналу.
23. Перечислите средства и методы защиты информации от утечки информации в телефонных линиях.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности

1. Что такое программно-аппаратные средства защиты информации?
2. Какие механизмы реализуют программно-аппаратные средства защиты информации?
3. Какие компьютерные угрозы безопасности существуют?
4. Что такое сетевая разведка? Какие методы защиты против нее существуют?
5. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
6. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
7. Основные виды программных уязвимостей.
8. Бэкдоры.
9. Что такое переполнение буффера? Методы защиты.
10. Что такое дефекты форматных строк? Методы защиты.
11. Что такое целочисленные переполнения? Методы защиты.
12. Ошибки обработки исключений. Методы защиты.
13. Внедрение команд. Методы защиты.
14. Некорректные обработки ошибок. Методы защиты.
15. Гонки. Методы защиты.
16. Выполнение кода с завышенными привилегиями.
17. Атака "Человек по середине".
18. Что такое IP-спуффинг? Какие методы защиты против него существуют?
19. ARP.
20. DHCP.

21. NAT.
22. PAT.
23. IPv4. IPv6.
24. Что такое ARP-спуффинг? Какие методы защиты против него существуют?
25. Что такое DNS Cache Poisoning? Какие методы защиты против него существуют?
26. Что такое NetBIOS/NBNS spoofing? Какие методы защиты против него существуют?
27. VPN.
28. Социальная инженерия.
29. Фрод. Методы борьбы с фродом.
30. Что такое фишинг? Какие методы защиты против него существуют?
31. Кардинг. Методы защиты от кардинга.
32. Darkweb.
33. DMZ.
34. Анонимайзеры.
35. Прокси-серверы.
36. Резервное копирование.
37. Honey pot.
38. DLP-системы. SIEM-системы.
39. Сканеры безопасности.
40. Системы обнаружения вторжений.
41. Системы предотвращения вторжений.
42. Вредоносные программы. Компьютерные вирусы. Виды вирусов.
43. Эксплоиты.
44. Механизм работы вируса.
45. Антивирусы. Виды антивирусов.
46. Механизмы работы антивируса.
47. Межсетевой экран.

Тема 6. Криптографические методы защиты информации

1. Что такое шифр? Какие виды шифров существуют?
2. Что такое симметричный шифр? Какие симметричные шифры используются сейчас?
3. Что такое ассиметричный шифр? Какие ассиметричные шифры используются сейчас?
4. Принцип построения симметричных шифров.
5. Принцип построения ассиметричных шифров.
6. Стандартные шифры.
7. Поточные шифры.
8. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
9. Дерево Меркла.
10. Что такое цифровая подпись?
11. Цифровая подпись RSA.
12. Цифровая подпись Эль-Гамаля.
13. Что такое инфраструктура открытых ключей?
14. Жизненный цикл ключа.
15. Аутентификация, идентификация, верификация, авторизация.
16. Простейшие протоколы идентификации.
17. Основной протокол Kerberos.
18. IPSec.
19. Blockchain.
20. Что такое стеганография? Понятие стеганоконтейнера.
21. Какие виды стеганоконтейнеров существуют?
22. Методы создания стеганоконтейнеров на основе текстовой информации.
23. Методы создания стеганоконтейнеров на основе видеоинформации и стоп/кадров.
24. Методы создания стеганоконтейнеров на основе аудиоинформации.

25. Цифровые водяные знаки.

Основная цель ТК: своевременная оценка успеваемости студентов, побуждающая их работать равномерно, исключая малые загрузки или перегрузки в течение семестра.

Практические занятия желательно проводить в режиме презентаций с демонстрацией применения основного материала, излагаемого в теме. Это существенно улучшает динамику лекций.

Целесообразно обеспечивать студентов на 1-2 лекции вперед раздаточным материалом в электронном виде (сложные схемы, графики, аналитические исследования и опорный конспект). Основное время лекции лучше тратить на подробные аналитические комментарии и особенности применения рассматриваемого материала в профессиональной деятельности студента.

Практические работы следует проводить в компьютерном классе либо в аудитории с мультимедийным оборудованием, используя оригинальную методику и профессиональные программы. Можно рекомендовать установку оригинальных программ на ПК студентов и выполнять ряд задач дома. В этом случае в классе основное внимание концентрируется на методике использования названных программ и анализе полученных результатов.

Промежуточный контроль (ПК) - это проверка знаний студентов по разделу программы. Формы: Опрос по теории согласно списка вопросов для самостоятельной оценки усвоения материала.

Цель ПК: побудить студентов отчитаться за усвоение раздела дисциплины накопительным образом, т.е. сначала за первый, затем за второй, затем за третий разделы и т.д. В конечном итоге многие студенты могут получить итоговые оценки по дисциплине “автоматом”.

Итоговый контроль по дисциплине (ИКД) - это проверка уровня учебных достижений студентов по всей дисциплине за семестр. Формы контроля: экзамен. Цель итогового контроля: проверка базовых знаний дисциплины, полученных при изучении модуля, достаточных для последующего обучения.

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. 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

3. Казарин О. В., Забабурин А. С. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебник и практикум для вузов [Электронный ресурс] , 2020 - 312 - Режим доступа: https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-452368

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. 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

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

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 издательства "Лань" - Режим доступа: https://e.lanbook.com/
4. Электронно-библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/
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"
- 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