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)
11.03.02 Инфокоммуникационные технологии и системы связи. Интернет-вещей и оптические системы и сети

Год набора на ОПОП
2019

Форма обучения
очная

Владивосток 2022

Рабочая программа дисциплины (модуля) «Информационная безопасность и защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (утв. приказом Минобрнауки России от 19.09.2017г. №930) 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

Тарасов В.С., ассистент, Кафедра информационных технологий и систем, Valentin.Tarasov@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	00000000009802AB
Владелец	Кийкова Е.В.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

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

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	
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ОПК-3 : Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.5к : Пользуется методами и навыками обеспечения информационной безопасности в системах связи	РД1	Знание	требований к защите информации определенного типа
			РД2	Умение	обеспечивать защиту информации
			РД3	Навык	владения современными методами обеспечения защиты информации

2 Место дисциплины (модуля) в структуре ОПОП

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

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		
11.03.02 Инфокоммуникационные технологии и системы связи	ОФО	Б1.Б	5	4	73	36	36	0	1	0	71	Э

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 в информационную безопасность	РД1	2	0	0	5	Собеседование
2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	РД1	0	2	0	6	отчет по практической работе
3	Правовое обеспечение информационной безопасности	РД1	6	0	0	6	Собеседование
4	Использование криптографических средств защиты информации	РД2	0	6	0	6	отчет по практической работе
5	Организационное обеспечение информационной безопасности	РД1	6	0	0	6	Собеседование
6	Реализация работы инфраструктуры открытых ключей	РД1	0	6	0	6	отчет по практической работе
7	Технические средства и методы защиты информации	РД2, РД3	6	0	0	6	Собеседование
8	Средства стеганографии для защиты информации	РД3	0	6	0	6	отчет по практической работе
9	Программно-аппаратные средства и методы обеспечения информационной безопасности	РД2, РД3	8	0	0	6	Собеседование
10	Настройка безопасного сетевого соединения	РД2, РД3	0	8	0	6	отчет по практической работе
11	Криптографические методы защиты информации	РД3	8	0	0	6	Собеседование
12	Антивирусные средства защиты информации	РД2, РД3	0	8	0	6	отчет по практической работе
Итого по таблице			**36**	**36**	**0**	**71**	

4.2 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.

5 Методические указания для обучающихся по изучению и реализации дисциплины

(модуля)

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

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.

Лекционные 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.

Вопросы к экзамену для оценки качества освоения учебной дисциплины

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Распределение объемов различного вида контролей можно проиллюстрировать следующими цифрами на примере семестра: текущий контроль – 40 условных баллов;

промежуточный контроль - 30 условных баллов; итоговый контроль - 30 условных баллов. Вся дисциплина оценивается в 100 условных баллов, если вся дисциплина оценивается цифрой, отличной от 100 баллов, то под условным баллом следует понимать процент от максимального числа баллов.

При этом действует следующая система перевода рейтинговых (условных) баллов в обычную шкалу качественных оценок: «Отлично» (5) - 91−100 условных баллов; «Хорошо» (4) - 75−90 условных баллов; «Удовлетворительно» (3) - 61−74 условных баллов; «Неудовлетворительно» (2) -

Приведенные цифры говорят о том, что на любой стадии обучение студента можно считать удовлетворительным, если он набирает не менее 61 условных баллов. Так, например, набрав в ходе ТК и ПК 61 баллов, студент гарантирует себе оценку «Удовлетворительно».

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. 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

7.2 Дополнительная литература

1. Акмаров, П.Б. Кодирование и защита информации : учебное пособие / П.Б. Акмаров .— Ижевск : ФГБОУ ВО Ижевская ГСХА, 2016 .— 136 с. — URL: https://lib.rucont.ru/efd/363163 (дата обращения: 20.02.2023)

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

3. 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

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

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

7.3 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. Электронно-библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/
6. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
7. 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 И ЗАЩИТА ИНФОРМАЦИИ

Направление и направленность (профиль)

11.03.02 Инфокоммуникационные технологии и системы связи. Интернет-вещей и оптические системы и сети

Год набора на ОПОП
2019

Форма обучения
очная

Владивосток 2022

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ОПК-3 : Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.5к : Пользуется методами и навыками обеспечения информационной безопасности в системах связи

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 ОПК-3 «Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности»

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	
ОПК-3.5к : Пользуется методами и навыками обеспечения информационной безопасности в системах связи	РД 1	Знание	требований к защите информации определенного типа	Сформировавшееся систематическое знание требований к защите информации определенного типа
	РД 2	Умение	обеспечивать защиту информации	Сформировавшееся систематическое умение обеспечивать защиту информации
	РД 3	Навык	владения современными методами обеспечения защиты информации	Сформировавшееся систематическое владение современными методами обеспечения защиты информации

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 : требований к защите информации определенного типа	1.1. Введение в информационную безопасность	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.3. Правовое обеспечение информационной безопасности	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
РД2	Умение : обеспечивать защиту информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.7. Технические средства и методы защиты информации	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.12. Антивирусные средства защиты информации	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
РД3	Навык : владения современными методами обеспечения защиты информации	1.7. Технические средства и методы защиты ин	Практическая работа	Экзамен в письменной форме

		формации	Собеседование	Экзамен в письменной форме
		1.8. Средства стеганографии для защиты информации	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.11. Криптографические методы защиты информации	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен в письменной форме
		1.12. Антивирусные средства защиты информации	Практическая работа	Экзамен в письменной форме
			Собеседование	Экзамен 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	Экзамен	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, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.

от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примерный перечень вопросов по темам

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. Чтотакое DNS Cache Poisoning? Какие методы защиты против него существуют?
26. Чтотакое 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.

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

Тема 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.

Тема 2. Использование криптографических средств защиты информации.

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.

Тема 3. Реализация работы инфраструктуры открытых ключей.

Студентам необходимо выполнить следующее рабочее задание использованием криптографической библиотеки OpenSSL под управлением ОС Linux Mint/Windows 7:

1. Установить OpenSSL
2. Настроить СКЗИ (исправить файл openssl.cnf)
3. Подготовить окружение
4. Сформировать закрытый ключ УЦ
5. Сформировать запрос на сертификат УЦ.
6. Выпустить самоподписанный сертификат УЦ
7. Сформировать ключи, запросы на сертификат и сертификаты не менее чем двум пользователям. В качестве имен пользователей рекомендуется использовать вымышленные, но осмысленные имена.
8. Отозвать один из сертификатов пользователей.
9. Сформировать список отозванных сертификатов.
10. Создать документ формата .txt и наполнить его данными. Получить открытый ключ для секретного ключа пользователя, созданного в ходе выполнения предыдущей работы.
11. Сформировать подпись созданного на шаге 10 документа.
12. Проверить подпись документа.
13. Подготовить отчет о проделанной работе.

Тема 4. Средства стеганографии для защиты информации.

Студентам необходимо выполнить следующее рабочее задание использованием стеганографических программных средств под управлением ОС Linux Mint:

1. Создать документ формата .txt и наполнить его данными.
2. Установить TrueCrypt.
3. Создать контейнер. Имя – Фамилия студента. Алгоритм шифрования – AES. Хеш-функция – SHA-512. Размер - необходимый. Пароль – по усмотрению.
4. Зашифровать созданный документ с помощью TrueCrypt.

5. Установить VeraCrypt.
6. Создать контейнер. Имя – Фамилия студента. Алгоритм шифрования – AES. Хеш-функция – Streebog. Размер - необходимый. Пароль – ключевой файл.
7. Зашифровать созданный документ с помощью VeraCrypt.
8. Зашифровать созданный документ с помощью BitLocker.
9. Установить ViPNet SafeDisk.
10. Создать контейнер. Имя – Фамилия студента. Алгоритм шифрования – ГОСТ. Размер – Необходимый. Пароль – по усмотрению.
11. Установить Image Spyer.
12. Сконфигурировать Image Spyer.
13. Замаскировать некоторое сообщение с помощью Image Spyer.
14. Извлечь сообщения из стеганоконтейнера.
15. Сокрыть информацию с помощью OpenPuff в аудиофайле.
16. Добавить в этот же аудиофайл цифровой водяной знак.
17. Проверить правильность выполнения задания.
18. Подготовить отчет о проделанной работе. К отчету приложить все зашифрованные стеганофайлы, а также все пароли от зашифрованных и замаскированных сообщений.

Тема 5. Настройка безопасного сетевого соединения.

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.

Тема 6. Антивирусные средства защиты информации.

Студентам необходимо выполнить следующее рабочее задание с использованием программного средства Kaspersky Endpoint Security и Kaspersky Security Center под управлением ОС Windows 7:

1. Осуществите локальную установку Kaspersky Endpoint Security.
2. Внедрите модуль управления Kaspersky Security Center.
3. Создайте структуру управляемых компьютеров.
4. Настройте модуль «Защиты от файловых угроз».
5. Настройте задачи поиска вирусов.

6. Настройте исключения для выбранной папки.
7. Настройте модуль «Защиты от почтовых угроз».
8. Настройте защиту от программ вымогателей.
9. Настройте защиту от сетевых угроз.
10. Настройте сетевой экрана для мобильной политики.
11. Настройте исключения из самозащиты.
12. Настройте защиту паролем для KES.
13. Настройте Контроль программ.
14. Заблокируйте запуск неизвестных файлов в сети.
15. Запретите доступ к съемным носителям информации.
16. Настройте права к съемным носителям информации.
17. Настройте контроль доступа к веб-ресурсам.
18. Настройте дэшборд.
19. Соберите журналы трассировки.
20. Организуйте резервное копирование и восстановление Kaspersky Security Center.
21. Подготовить отчет о проделанной работе.

Краткие методические указания

На выполнение одной практической работы 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 практические задания по теме практической работы.

Шкала оценки

№	Баллы	Описание
5	49–60	Студент демонстрирует умения на итоговом уровне: умеет свободно выполнять практические 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 допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, перенесе умений на новые, нестандартные ситуации.
3	24–36	Студент демонстрирует умения и навыки на базовом уровне: в ходе контрольных мероприятий 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 недостаточность умений и навыков.
1	0–10	Студентом проявляется полное или практически полное отсутствие умений и навыков.

5.3 Вопросы к экзамену

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.
4. Перечислите основные законы в области защиты информации РФ. Опишите основные положения стратегии национальной безопасности и Доктрины информационной безопасности.
5. Охарактеризуйте биометрические данные как персональные данные. В каких случаях возможно использовать персональные данные без согласия обладателя?
6. Перечислите и опишите основные международные стандарты в области информационной безопасности? Как связаны международные стандарты и стандарты РФ?
7. Что такое персональные данные? Опишите основные положения Федеральных законов в области персональных данных.
8. Что такое служебная и коммерческая тайна? Охарактеризуйте принципиальные

различия. Опишите основные положения Федеральных законов в области служебной и коммерческой тайна.

9. 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).
20. Что такое аудит информационной безопасности? Опишите методику проведения аудита информационной безопасности.
21. Опишите методику оценки рисков нарушения информационной безопасности.
22. Что такое инженерная защита объектов? Каким способом описывается инженерная защита? Описать модель.
23. Что такое модель охраны периметра? Описать модель. Какие средства применяются для защиты 1-го, 2-го и 3-го периметров?
24. Какие средства применяются для защиты 2-го периметра?
25. Какие средства применяются для защиты 3-го периметра?
26. Перечислите и опишите технические средства обнаружения несанкционированного доступа к охраняемому объекту.
27. Что такое биометрия. Опишите биометрические характеристики (приведите примеры).
28. Что такое технические каналы утечки информации? Перечислите и опишите основные виды технических каналов утечки информации.
29. Опишите методику спецпроверки, специсследования и спецобследования? В чем состоит принципиальное различие между указанными методиками?
30. Перечислите и опишите методы защиты информации от утечки по зрительному и воздушному каналам.
31. Перечислите методы защиты информации от утечки по электромагнитному и электрическому каналам.
32. Перечислите методы защиты информации от утечки по индукционному каналу и параметрическому каналам.
33. Перечислите методы защиты информации от утечки по вибрационному и акустоэлектрическому каналам.
34. Перечислите методы защиты информации от утечки.
35. Перечислите средства и методы защиты информации по оптикоэлектронному каналу и от утечки информации в телефонных линиях.
36. Что такое программно-аппаратные средства защиты информации? Какие механизмы реализуют программно-аппаратные средства защиты информации? Какие

компьютерные угрозы безопасности существуют?

37. Что такое сетевая разведка? Какие методы защиты против нее существуют? Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
38. В чем суть атаки «отказ в обслуживании»? Ее отличия от распределенной кибератаки «отказ в обслуживании»? Какие методы защиты против него существуют?
39. Перечислите и опишите основные виды программных уязвимостей. Какие методы защиты против них существуют?
40. Что такое переполнение буффера? Перечислите о пишите методы защиты.
41. Что такое дефекты форматных строк? Перечислите о пишите методы защиты.
42. Что такое целочисленные переполнения? Перечислите о пишите методы защиты.
43. Что такое «состояние гонки». Перечислите опишите методы защиты.
44. Что такое атака «Человек по середине»? Что такое IP-спуффинг? Какие методы защиты против указанных атак существуют?
45. В чем суть сетевого протокола ARP (описать в соответствии с эталонной моделью OSI и стеком протоколов TCP/IP)? Что такое ARP-спуффинг? Какие методы защиты против него существуют?
46. В чем суть сетевых протоколов DNS и DHCP (описать в соответствии с эталонной моделью OSI и стеком протоколов TCP/IP)? DNS Cache Poisoning? Какие методы защиты против них существуют?
47. В чем суть сетевых протоколов NAT и PAT (описать в соответствии с эталонной моделью OSI и стеком протоколов TCP/IP)? NetBIOS/NBNS spoofing? Какие методы защиты против них существуют?
48. 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?
49. Что такое социальная инженерия? Что такое фрод. Перечислите о опишите методы борьбы с фродом.
50. Что такое фишинг? Какие методы защиты против него существуют? Что такое кардинг? Опишите методы защиты от кардинга.
51. Назначение, цели, описание Honeypot. Как выявлять Honeypot?
52. Что такое и для чего используются средства контекстной фильтрации? Охарактеризуйте DLP-системы и SIEM-системы.
53. Что такое сканеры сканеры безопасности? Для чего используется RPC-сканирование? Перечислите и опишите основные методы сканирования.
54. Что такое и для чего используются системы обнаружения вторжений и системы предотвращения вторжений?
55. Что такое вредоносные программы? Классифицируйте компьютерные вирусы. Опишите типовой механизм работы вируса. Что такое эксплоит?
56. Что такое шифр? Какие виды шифров существуют? Опишите принципы построения и принципиальные отличия.
57. Что такое поточный и блочный шифры? Опишите принципы построения и принципиальные отличия.
58. Что такое хеш-функция (описать принцип работы)? Какие виды хеш-функций вы знаете?
59. Что такое Дерево Меркла?
60. Что такое цифровая подпись? Опишите цифровую подпись RSA и Эль-Гамаля.Что такое инфраструктура открытых ключей? Описать методику распределения ключей
61. на примере подписания сертификата. Описать зависимость публичного и приватного ключей
62. Что такое аутентификация, идентификация, верификация, авторизация. Опишите принципиальные отличия между ними. Приведите примеры.

63. Простейшие протоколы идентификации.
64. Опишите методику работу протокола защищенного обмена (в рамках VPN).
65. Что такое технология Blockchain? Опишите методы построения.
66. Что такое стеганография и стеганоконтейнер? Какие виды стеганоконтейнеров существуют? Опишите методы создания стеганоконтейнеров на основе текстовой информации, видеоинформации и аудиоинформации.

Краткие методические указания

Экзамен 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 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