МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление и направленность (профиль)
09.03.02 Информационные системы и технологии. Информационные системы и технологии

Год набора на ОПОП
2020

Форма обучения
заочная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Информационная безопасность и защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии (утв. приказом Минобрнауки России от 19.09.2017г. №926) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

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

Шумик Е.Г., кандидат экономических наук, доцент, Кафедра математики и моделирования, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 18.05.2023 , протокол № 7

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Мазелис Л.С.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	1575656200
Номер транзакции	0000000000BB6EE8
Владелец	Мазелис Л.С.

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 дисциплин		
			Код результата	Формулировка результата	
09.03.02 «Информационные системы и технологии» (Б-ИС)	ОПК-1 : Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.2к : Решает профессиональные задачи с применением естественнонаучных и общеинженерных знаний	РД1	Знание	современных законов, стандартов, методов и технологий в области защиты информации
	ОПК-2 : Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.2к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД2	Знание	требований к защите информации определенного типа
			РД3	Умение	использовать современные программно-аппаратные средства защиты информации
	ОПК-3 : Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	ОПК-3.1к : Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с	РД4	Умение	обеспечивать защиту информации
			РД5	Навык	владения современными методами обеспечения защиты информации

	информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	РД6	Знание	современных методов и средс защиты информации
			РД7	Умение	анализировать информационну безопасность организации
			РД8	Навык	владения современными технологиями и методами обеспечения информационно безопасности организации
	ПКВ-4 : Способен осуществлять управление (выполнять работы по обслуживанию) доступом к программно-аппаратным средствам информационных служб, мониторинг состояния оборудования и учет отказов оборудования инфокоммуникационной системы	ПКВ-4.1к : Управляет доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	РД10	Умение	управлять информационно безопасностью организации
			РД11	Навык	владения методами оценк рисков информационно безопасности
			РД9	Знание	современных технологий, методик и средств 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 обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
09.03.02 Информационные системы и технологии	ЗФО	Б1.Б	4	5	17	8	8	0	1	0	163	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ЗФО

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 ЗФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение в информационную безопасность	РД1, РД6	1	0	0	7	собеседование
2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	РД1	0	1	0	7	отчет по практической работе
3	Правовое обеспечение информационной безопасности	РД1, РД2	1	0	0	7	собеседование
4	Использование криптографических средств защиты информации	РД3, РД4, РД6, РД8, РД9	0	1	0	7	отчет по практической работе
5	Организационное обеспечение информационной безопасности	РД2, РД4, РД7, РД8, РД10	1	0	0	7	собеседование
6	Реализация работы инфраструктуры открытых ключей	РД2, РД4, РД6, РД7, РД9, РД10, РД11	0	1	0	8	отчет по практической работе
7	Технические средства и методы защиты информации	РД3, РД4, РД5, РД6, РД7, РД9	1	0	0	8	собеседование
8	Средства стеганографии для защиты информации	РД5, РД9	0	1	0	8	отчет по практической работе
9	Программно-аппаратные средства и методы обеспечения информационной безопасности	РД3, РД4, РД5, РД7, РД8, РД9, РД11	2	0	0	8	собеседование
10	Настройка безопасного сетевого соединения	РД3, РД4, РД5, РД8, РД9, РД11	0	2	0	8	отчет по практической работе
11	Криптографические методы защиты информации	РД5, РД8, РД9, РД11	2	0	0	8	собеседование
12	Антивирусные средства защиты информации	РД3, РД4, РД5, РД9, РД11	0	2	0	8	отчет по практической работе
Итого по таблице			**8**	**8**	**0**	**91**	

4.2 Содержание разделов и тем дисциплины (модуля) для ЗФО

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: лекция.

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 занятие.

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: лекция.

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 занятие.

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: лекция.

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 занятие.

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: лекция.

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 занятие.

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: лекция.

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 занятие.

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: лекция.

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 занятие.

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 буфера? 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 списку 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. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912992 (дата обращения: 26.02.2024).
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: 16.02.2024)
2. Введение в криптографию : Учебное пособие [Электронный ресурс] : Издательство ФОРУМ , 2020 - 240 - Режим доступа: https://znanium.com/catalog/document?id=345516
3. 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 "ZNANIUM.COM"
4. Электронно-библиотечная система "РУКОНТ"
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

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление и направленность (профиль)

09.03.02 Информационные системы и технологии. Информационные системы и технологии

Год набора на ОПОП
2020

Форма обучения
заочная

Владивосток 2023

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
09.03.02 «Информационные системы и технологии» (Б-ИС)	ОПК-1 : Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.2к : Решает профессиональные задачи с применением естественнонаучных и общеинженерных знаний
	ОПК-2 : Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.2к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
	ОПК-3 : Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1к : Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ПКВ-4 : Способен осуществлять управление (выполнять работы по обслуживанию) доступом к программно-аппаратным средствам информационных служб, мониторинг состояния оборудования и учет отказов оборудования инфокоммуникационной системы	ПКВ-4.1к : Управляет доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы

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

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-4 «Способен осуществлять управление (выполнять работы по обслуживанию) доступом к программно-аппаратным средствам информационных служб, мониторинг состояния оборудования и учет отказов оборудования инфокоммуникационной системы»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

	Результаты обучения по дисциплине	
Код и формулировка индикат		Критерии оценивания результ

ора достижения компетенции	Код рез-та	Тип рез-та	Результат	атов обучения
ПКВ-4.1к : Управляет доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	РД 9	Знание	современных технологий, методик и средств защиты информации	Сформировавшееся систематическое знание современных технологий, методик и средства защиты информации
	РД 10	Умение	управлять информационной безопасностью организации	Сформировавшееся систематическое умение управлять информационной безопасностью организации
	РД 11	Навык	владения методами оценки рисков информационной безопасности	Сформировавшееся систематическое владение методами оценки рисков информационной безопасности

Компетенция ОПК-1 «Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности»

Таблица 2.2 – 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-1.2к : Решает профессиональные задачи с применением естественнонаучных и общеинженерных знаний	РД 1	Знание	современных законов, стандартов, методов и технологий в области защиты информации	Сформировавшееся систематическое знание современных законов, стандартов, методов и технологий в области защиты информации

Компетенция ОПК-2 «Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности»

Таблица 2.3 – 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-2.2к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения	РД 2	Знание	требований к защите информации определенного типа	Сформировавшееся систематическое знание требований к защите информации определенного типа

задач профессиональной деятельности	РД3	Умение	использовать современные программно-аппаратные средства защиты информации	Сформировавшееся систематическое умение использовать современные программно-аппаратные средства защиты информации

Компетенция ОПК-3 «Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»

Таблица 2.4 – 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-3.1к : Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	РД4	Умение	обеспечивать защиту информации	Сформировавшееся систематическое умение обеспечивать защиту информации
	РД5	Навык	владения современными методами обеспечения защиты информации	Сформировавшееся систематическое владение современными методами обеспечения защиты информации
	РД6	Знание	современных методов и средств защиты информации	Сформировавшееся систематическое знание современных методов и средств защиты информации
	РД7	Умение	анализировать информационную безопасность организации	Сформировавшееся систематическое умение анализировать информационную безопасность организации
	РД8	Навык	владения современными технологиями и методами обеспечения информационной безопасности организации	Сформировавшееся систематическое владение современными технологиями и методами обеспечения информационной безопасности организации

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

Заочная форма обучения				
РД1	Знание : современных законов, стандартов, методов и технологий в области защиты информации	1.1. Введение в информационную безопасность	Практическая работа	Собеседование
		1.2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Практическая работа	Собеседование
		1.3. Правовое обеспечение информационной безопасности	Практическая работа	Собеседование
РД2	Знание : требований к защите информации определенного типа	1.3. Правовое обеспечение информационной безопасности	Практическая работа	Собеседование
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
РД3	Умение : использовать современные программно-аппаратные средства защиты информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
РД4	Умение : обеспечивать защиту информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование

РД5	Навык : владения современными методами обеспечения защиты информации	1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
		1.8. Средства стеганографии для защиты информации	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
РД6	Знание : современных методов и средств защиты информации	1.1. Введение в информационную безопасность	Практическая работа	Собеседование
		1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
РД7	Умение : анализировать информационную безопасность организации	1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
РД8	Навык : владения современными технологиями и методами обеспечения информационной безопасности организации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование

РД9	Знание : современных технологий, методик и средств защиты информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
		1.8. Средства стеганографии для защиты информации	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
РД10	Умение : управлять информационной безопасностью организации	1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
РД11	Навык : владения методами оценки рисков информационной безопасности	1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование

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	Итого
Лекции	10		10

Практические занятия		60	60
Промежуточная аттестация	20		20
Самостоятельная работа	10		10
Итого	40	60	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, нет очности, 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 буфера? 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.

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	32–40	Студент полностью ответил на заданные вопросы
3	24–31	Студент смог почти полностью ответить на заданные вопросы
2	15–23	Студент дал неполный ответ на вопросы, но смог передать основную суть вопроса
1	0–14	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.

Тема 2. Использование криптографических средств защиты информации.

Тема 3. Реализация работы инфраструктуры открытых ключей.

Тема 4. Средства стеганографии для защиты информации.

Тема 5. Настройка безопасного сетевого соединения.

Тема 6. Антивирусные средства защиты информации.

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.