

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление и направленность (профиль)
01.03.04 Прикладная математика. Интеллектуальный анализ данных

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Информационная безопасность и защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.04 Прикладная математика (утв. приказом Минобрнауки России от 10.01.2018г. №11) 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):

Иванова А.В., старший преподаватель, Кафедра информационной безопасности,
Ivanova.A@vvsu.ru

Мартышенко Н.С., старший преподаватель, Кафедра информационной
безопасности, Nikolay.Martyshenko@vvsu.ru

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра
информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 ,
протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000E84672
Владелец	Шумик Е.Г.

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	
01.03.04 «Прикладная математика» (Б-ПМ)	УК-8 : Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.2в : Владеет навыками культуры безопасности и риск ориентированным мышлением по вопросам безопасности и сохранения окружающей среды	РД1	Знание	современных законов, стандартов, методов и технологий в области защиты информации
			РД10	Умение	управлять информационной безопасностью организации
			РД11	Навык	владения методами оценки рисков информационной безопасности
			РД2	Знание	требований к защите информации определенного типа
			РД3	Умение	использовать современные программно-аппаратные средства защиты информации
			РД4	Умение	обеспечивать защиту информации
			РД5	Навык	владения современными методами обеспечения защиты информации
			РД6	Знание	современных методов и средств защиты информации
			РД7	Умение	анализировать информационную безопасность организации
			РД8	Навык	владения современными технологиями и методами обеспечения

					информационной безопасности организации
			РД9	Знание	современных технологий, методик и средств защиты информации

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	Формирование ценностей	Целевые ориентиры
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Дисциплинированность
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Высокие нравственные идеалы	Осознание ценности профессии
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Служение Отечеству и ответственность за его судьбу	Соблюдение моральных принципов
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Взаимопомощь и взаимоуважение	Способность находить, анализировать и структурировать информацию

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)	Трудо-емкость	Объем контактной работы (час)			СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная	Внеауди-торная		

						лек.	прак.	лаб.	ПА	КСР		
01.03.04 Прикладная математика	ОФО	Б1.Б	5	3	73	36	36	0	1	0	35	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, РД6	2	0	0	2	Собеседование
2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	РД1	0	2	0	3	отчет по практической работе
3	Правовое обеспечение информационной безопасности	РД1, РД2	6	0	0	3	Собеседование
4	Использование криптографических средств защиты информации	РД3, РД4, РД6, РД8, РД9	0	6	0	3	отчет по практической работе
5	Организационное обеспечение информационной безопасности	РД2, РД4, РД7, РД8, РД10	6	0	0	3	Собеседование
6	Реализация работы инфраструктуры открытых ключей	РД2, РД4, РД6, РД7, РД9, РД10, РД11	0	6	0	3	отчет по практической работе
7	Технические средства и методы защиты информации	РД3, РД4, РД5, РД6, РД7, РД9	6	0	0	3	Собеседование
8	Средства стеганографии для защиты информации	РД5, РД9	0	6	0	3	отчет по практической работе
9	Программно-аппаратные средства и методы обеспечения информационной безопасности	РД3, РД4, РД5, РД7, РД8, РД9, РД11	8	0	0	3	Собеседование

10	Настройка безопасного сетевого соединения	РД3, РД4, РД5, РД8, РД9, РД11	0	8	0	3	отчет по практической работе
11	Криптографические методы защиты информации	РД5, РД8, РД9, РД11	8	0	0	3	Собеседование
12	Антивирусные средства защиты информации	РД3, РД4, РД5, РД9, РД11	0	8	0	3	отчет по практической работе
Итого по таблице			36	36	0	35	

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 миниэссе, 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 асимметричный шифр? Какие асимметричные шифры используются сейчас?
4. Принцип построения симметричных шифров.
5. Принцип построения асимметричных 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-Гамала.
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) - < 61 условных баллов.

Приведенные цифры говорят о том, что на любой стадии обучения 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. 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 - 05.09.2025)

2. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/427130> (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.

3. Романьков В.А. Введение в криптографию : Учебное пособие [Электронный ресурс] : Издательство ФОРУМ , 2022 - 240 - Режим доступа: <https://znanium.com/catalog/document?id=400556>

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: 04.08.2025)

2. Бабаш, А. В., Информационная безопасность. Лабораторный практикум + Приложение : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2022. — 131 с. — ISBN 978-5-406-10084-4. — URL: <https://book.ru/book/944619> (дата обращения: 09.09.2025). — Текст : электронный.

3. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2021. — 267 с. — ISBN 978-5-406-08259-1. — URL: <https://book.ru/book/939292> (дата обращения: 09.09.2025). — Текст : электронный.

4. 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 "BOOK.ru"
4. Электронно-библиотечная система "ZNANIUM.COM"
5. Электронно-библиотечная система "ЛАНЬ"
6. Электронно-библиотечная система "РУКОНТ"
7. Open Academic Journals Index (ОАИ). Профессиональная база данных - Режим доступа: <http://oaji.net/>
8. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: <https://www.prilib.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
- Мульти-медийный комплект № 2: Проектор Panasonic PT-LX26HE, потолочное крепление Tuarex Corsa, клеммный модуль Kramer WX -1N, коннектор VGA, экран Lumien Escopicture
- 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-РЗ.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 and Windows

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)
01.03.04 Прикладная математика. Интеллектуальный анализ данных

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
01.03.04 «Прикладная математика» (Б-ПМ)	УК-8 : Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.2в : Владеет навыками культуры безопасности и риск ориентированным мышлением по вопросам безопасности и сохранения окружающей среды

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 УК-8 «Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код	Тип	Результат	
УК-8.2в : Владеет навыками культуры безопасности и риск ориентированным мышлением по вопросам безопасности и сохранения окружающей среды	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
	РД 2	Знание	требований к защите информации определенного типа	Сформировавшееся систематическое знание требований к защите информации определенного типа
	РД 3	Умение	использовать современные программно-аппаратные средства защиты информации	Сформировавшееся систематическое умение использовать современные программно-аппаратные средства защиты информации
	РД 4	Умение	обеспечивать защиту информации	Сформировавшееся систематическое умение обеспечивать защиту информации

	РД 5	Навык	владения современными методами обеспечения защиты информации	Сформировавшееся систематическое владение современными методами обеспечения защиты информации
	РД 6	Знание	современных методов и средств защиты информации	Сформировавшееся систематическое знание современных методов и средств защиты информации
	РД 7	Умение	анализировать информационную безопасность организации	Сформировавшееся систематическое умение анализировать информационную безопасность организации
	РД 8	Навык	владения современными технологиями и методами обеспечения информационной безопасности организации	Сформировавшееся систематическое владение современными технологиями и методами обеспечения информационной безопасности организации
	РД 9	Знание	современных технологий, методик и средств защиты информации	Сформировавшееся систематическое знание современных технологий, методик и средств 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

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

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : современных законов, стандартов, методов и технологий в области защиты информации	1.1. Введение в информационную безопасность	Практическая работа	Собеседование
			Тест	Собеседование
		1.2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
			Практическая работа	Собеседование

		1.3. Правовое обеспечение информационной безопасности	Тест	Собеседование
РД2	Знание : требований к защите информации определенного типа	1.3. Правовое обеспечение информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
			Тест	Собеседование
РД3	Умение : использовать современные программно-аппаратные средства защиты информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
			Тест	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
РД4	Умение : обеспечивать защиту информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
			Тест	Собеседование

		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
			Тест	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
РД5	Навык : владения современными методами обеспечения защиты информации	1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.8. Средства стеганографии для защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
			Тест	Собеседование
		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
РД6	Знание : современных методов и средств защиты информации	1.1. Введение в информационную безопасность	Практическая работа	Собеседование
			Тест	Собеседование
		1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
			Тест	Собеседование

		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
			Тест	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
РД7	Умение : анализировать информационную безопасность организации	1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.6. Реализация работы инфраструктуры открытых ключей	Практическая работа	Собеседование
			Тест	Собеседование
		1.7. Технические средства и методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
РД8	Навык : владения современными технологиями и методами обеспечения информационной безопасности организации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.5. Организационное обеспечение информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.9. Программно-аппаратные средства и методы обеспечения информационной безопасности	Практическая работа	Собеседование
			Тест	Собеседование
		1.10. Настройка безопасного сетевого соединения	Практическая работа	Собеседование
			Тест	Собеседование
		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
РД9	Знание : современных технологий, методик и средств защиты информации	1.4. Использование криптографических средств защиты информации	Практическая работа	Собеседование
			Тест	Собеседование

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

		1.11. Криптографические методы защиты информации	Практическая работа	Собеседование
			Тест	Собеседование
		1.12. Антивирусные средства защиты информации	Практическая работа	Собеседование
			Тест	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			
	Тест	Практические задания	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		40		60
Промежуточная аттестация			20	20
Итого	40	40	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, обладает 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

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.

3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Право. Источники права.
6. Какие основные законы в области защиты информации в РФ?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна? Что такое служебная тайна?
9. Что такое коммерческая тайна?
10. Какие основные международные стандарты в области информационной безопасности?
11. «Оранжевая книга» ISO/IEC 15408.
12. Как связаны международные стандарты и стандарты РФ?
13. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
14. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
15. Что такое политика безопасности?
16. Что такое инженерная защита объектов?
17. Биометрия. Биометрические характеристики.
18. Что такое технические каналы утечки информации?
19. Перечислите основные виды технических каналов утечки информации?
20. Что такое спецпроверка?
21. Что такое специсследование?
22. Что такое спецобследование?
23. Что такое программно-аппаратные средства защиты информации?
24. Какие механизмы реализуют программно-аппаратные средства защиты информации?
25. Какие компьютерные угрозы безопасности существуют?
26. Что такое сетевая разведка? Какие методы защиты против нее существуют?
27. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
28. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
29. Основные виды программных уязвимостей.
30. Что такое шифр? Какие виды шифров существуют?
31. Что такое симметричный шифр?
32. Какие симметричные шифры используются сейчас?
33. Что такое асимметричный шифр? Какие асимметричные шифры используются сейчас?
34. Принцип построения симметричных шифров.
35. Принцип построения асимметричных шифров.
36. Стандартные шифры.
37. Поточные шифры.

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	32–40	Студент предоставляет отчет попрактической работе оформленный в строгом соответствии с требованиями вуза. Демонстрирует ход выполнения задания, отвечает на вопросы по заданию.
4	26–31	Студент предоставляет отчет попрактической работе оформленный в строгом соответствии с требованиями вуза. Демонстрирует ход выполнения задания, но не отвечает на вопросы по заданию.
3	18–25	Студент предоставляет отчет попрактической работе оформленный в строгом соответствии с требованиями вуза. Но не способен продемонстрировать ход выполнения задания, отвечает на вопросы по заданию.
2	11–24	Студент предоставляет отчет попрактической работе оформленный с ошибками соответствующими с требованиями вуза. не демонстрирует ход выполнения задания, отвечает на вопросы по заданию с неточностями.
1	0–10	Студентом демонстрируется отчет, но не может рассказать ни о выполнении задания, ни ответить на вопросы по нему. Либо отчет не предоставлен

5.3 Контрольный тест

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

- а) Разработка аппаратных средств обеспечения правовых данных
- б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанные в списке:

- а) Хищение жестких дисков, подключение к сети, инсайдерство
- б) Перехват данных, хищение данных, изменение архитектуры системы
- в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:

- а) Персональная, корпоративная, государственная
- б) Клиентская, серверная, сетевая
- в) Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- а) Несанкционированного доступа, воздействия в сети
- б) Инсайдерства в организации
- в) Чрезвычайных ситуаций

5. Основные объекты информационной безопасности:

- а) Компьютерные сети, базы данных
- б) Информационные системы, психологическое состояние пользователей
- в) Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:

- а) Искажение, уменьшение объёма, перекодировка информации
- б) Техническое вмешательство, выведение из строя оборудования сети
- в) Потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:

- а) Экономической эффективности системы безопасности
- б) Многоплатформенной реализации системы
- в) Усиления защищённости всех звеньев системы

8. Основными субъектами информационной безопасности являются:

- а) Руководители, менеджеры, администраторы компаний
- б) Органы права, государства, бизнеса
- в) Сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести всё перечисленное:

- а) Установление регламента, аудит системы, выявление рисков
- б) Установка новых офисных приложений, смена хостинг-компаний
- в) Внедрение аутентификации, проверка контактных данных пользователей

10. Принципом информационной безопасности является принцип недопущения:

- а) Неоправданных ограничений при работе в сети (системе)
- б) Рисков безопасности сети, системы
- в) Презумпции секретности

11. Принципом политики информационной безопасности является принцип:

- а) Невозможности миновать защитные средства сети (системы)
- б) Усиления основного звена сети, системы
- в) Полного блокирования доступа при риск-ситуациях

12. Принципом политики информационной безопасности является принцип:

- а) Усиления защищённости самого незащищённого звена сети (системы)

- **б)** Перехода в безопасное состояние работы сети, системы
- **в)** Полного доступа пользователей ко всем ресурсам сети, системы

13. Принципом политики информационной безопасности является принцип:

- **а)** Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- **б)** Одноуровневой защиты сети, системы
- **в)** Совместимых, однотипных программно-технических средств сети, системы

14. К основным типам средств воздействия на компьютерную сеть относится:

- **а)** Компьютерный сбой
- **б)** Логические закладки («мины»)
- **в)** Аварийное отключение питания

15. Когда получен спам по e-mail с приложенным файлом, следует:

- **а)** Прочитать приложение, если оно не содержит ничего ценного – удалить
- **б)** Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама
- **в)** Удалить письмо с приложением, не раскрывая (не читая) его

16. Принцип Кирхгофа:

- **а)** Секретность ключа определена секретностью открытого сообщения
- **б)** Секретность информации определена скоростью передачи данных
- **в)** Секретность закрытого сообщения определяется секретностью ключа

17. ЭЦП – это:

- **а)** Электронно-цифровой преобразователь
- **б)** Электронно-цифровая подпись
- **в)** Электронно-цифровой процессор

18. Наиболее распространены угрозы информационной безопасности корпоративной системы:

- **а)** Покупка нелегального ПО
- **б)** Ошибки эксплуатации и неумышленного изменения режима работы системы
- **в)** Сознательное внедрение сетевых вирусов

19. Наиболее распространены угрозы информационной безопасности сети:

- **а)** Распределённый доступ клиента, отказ оборудования
- **б)** Моральный износ сети, инсайдерство
- **в)** Сбой (отказ) оборудования, нелегальное копирование данных

20. Наиболее распространены средства воздействия на сеть офиса:

- **а)** Слабый трафик, информационный обман, вирусы в интернет
- **б)** Вирусы в сети, логические мины (закладки), информационный перехват
- **в)** Компьютерные сбои, изменение администрирования, топологии

21. Утечкой информации в системе называется ситуация, характеризующаяся:

- а) Потерей данных в системе
- б) Изменением формы информации
- в) Изменением содержания информации

22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- а) Целостность
- б) Доступность
- в) Актуальность

23. Угроза информационной системе (компьютерной сети) – это:

- а) Вероятное событие
- б) Детерминированное (всегда определённое) событие
- в) Периодически повторяющееся событие

24. Информация, которую следует защищать (по нормативам, правилам сети, системы), называется:

- а) Регламентированной
- б) Правовой
- в) Защищаемой

25. Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:

- а) Программные, технические, организационные, технологические
- б) Серверные, клиентские, спутниковые, наземные
- в) Личные, корпоративные, социальные, национальные

26. Окончательно, ответственность за защищённость данных в компьютерной сети несёт:

- а) Владелец сети
- б) Администратор сети
- в) Пользователь сети

27. Политика безопасности в системе (сети) – это комплекс:

- а) Руководств, требований обеспечения необходимого уровня безопасности
- б) Инструкций, алгоритмов поведения пользователя в сети
- в) Норм информационного права, соблюдаемых в сети

28. Наиболее важным при реализации защитных мер политики безопасности является:

- а) Аудит, анализ затрат на проведение защитных мер
- б) Аудит, анализ безопасности
- в) Аудит, анализ уязвимостей, риск-ситуаций

Краткие методические указания

Перед решением тестов внимательно следует ознакомиться с каждым вопросом и предлагаемыми вариантами ответов. Затем необходимо опираясь на теоретический материал, связанный с темой вопроса сопоставить его с приведёнными вариантами. Выбирается тот ответ, который точно отражает изложенные факты.

Шкала оценки

№	Баллы	Описание
2	1	Студент дал верный ответ на тестовый вопрос
1	0	Студент дал не верный ответ на тестовый вопрос