МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ГЕОГРАФИИ, ГЕОЛОГИИ, ТУРИЗМА И СЕРВИСА

УТВЕРЖДАЮ
Проректор по научной работе
Качеству образования первый
Проректор
_____Хагуров Т.А.
«30» _____ 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ФТД.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки *43.03.01 Сервис*

Направленность (профиль) *Менеджмент бизнеса в сфере сервиса, туризма и гостеприимства*

Форма обучения Очная

Квалификация Бакалавр

Краснодар 2025

Рабочая программа дисциплины ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 43.03.01 Сервис (Менеджмент бизнеса в сфере сервиса, туризма и гостеприимства)

код и наименование направления подготовки

Программу составил(и):
М.В. Кузякина, доцент, канд. физ-мат. наук
ИО. Фамилия, должность, ученая степень, ученое звание (подпись)

Рабочая программа обсуждена на заседании кафедры геоинформатики
протокол №10 «27» мая 2025 г.
Ио. зав. кафедрой (выпускающей) Комаров Д.А.
фамилия, инициалы (подпись)

Утверждена на заседании учебно-методической комиссии института географии, геологии, туризма и сервиса «22» мая 2025 г., протокол №6
Председатель УМК института Филобок А.А.

Рецензенты:

1. Гаркуша О.В., к.ф. – м.н., доцент кафедры информационных технологий ФГБОУ ВО «КубГУ»
2. Нетребин П.Б., к.г.н., генеральный директор ГИС и картографии ООО «Гискарт»

1 Цели и задачи изучения дисциплины

1.1Цель освоения дисциплины

Цель освоения учебной дисциплины «Информационная безопасность» – ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

1.2Задачи дисциплины

– сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;

– передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;

– сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

1.3Место дисциплины в структуре ООП ВО

Данная дисциплина относится к факультативной части блока ФТД «Факультативы» учебного плана. Дисциплина «Информационная безопасность» требует знаний по дисциплинам: системы искусственного интеллекта, анализ данных в профессиональной сфере и менеджмент в сфере сервиса, туризма и гостеприимства.

Курс необходим в качестве предшествующего для следующих дисциплин: «Бизнес-планирование в сфере сервиса, туризма и гостеприимства» и «Инновационный менеджмент».

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение учебной дисциплины «Информационная безопасность» направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ИОПК-8.1. Использует современные информационные технологии в организации профессиональной деятельности.	Знать источники возникновения информационных угроз; каналы утечки информации; направления и средства защиты информации; принципы национальной без-опасности; исследования, ведущиеся в области информационной безопасности..
	Уметь применять правовые, организационные, технические и программные средства защиты информации; вы-являть потенциальные каналы утечки информации и определять их характеристики; разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности;

Код и наименование индикатора*	Результаты обучения по дисциплине
	систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности.
	Владеть навыками противодействия утечке компьютер-ной информации; навыками использования электронной цифровой подписи; навыками проведения аудита ло-кальной политики безопасности, аудита доступа к объ-ектам; специальной терминологией, применяемой в процессе защиты информации; навыками профессио-нальной аргументации при разборе стандартных ситу-аций в сфере информационной безопасности
ИОПК-8.1. Применяет современные информационные технологии в решении задач профессиональной деятельности.	Знать порядок проведения анализа информационной безопасности объектов и систем
	Уметь проводить анализ информационной безопасности объектов информатизации.
	Владеть Навыками проведения анализа информацион-ной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Объем трудоемкости: 2 зачетных единицы (72 часа (в 6 семестре), из них – 28 часов аудиторной нагрузки: лекционных 14 ч., практических 14 ч.; 41,8 часов самостоятельной работы, в том числе 2 ч. КСР, 0,2 ч. ИКР), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры (часы)
			6
Контактная работа, в том числе:		30,2	30,2
Аудиторные занятия (всего)		28	28
В том числе:			
Занятия лекционного типа		14	14
Лабораторные занятия			
Занятия семинарского типа (семинары, практические занятия)		14	14
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		2	2
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа (всего)		41,8	41,8
В том числе:			
Курсовая работа			
Проработка учебного (теоретического) материала		15	15
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		13	13
Реферат		8	8
Подготовка к текущему контролю		5,8	5,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	**час.**	**72**	72
	в том числе контактная работа	**2,2**	2,2
	зач. ед	**2**	**2**

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
6 семестр						
1.	Введение в информационную безопасность	12	2	2		8
2.	Правовое обеспечение информационной безопасности	11	2	2		7
3.	Организационное обеспечение информационной безопасности	11	2	2		7
4.	Технические средства и методы защиты информации	12	2	2		8
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	12	4	2		6
6.	Криптографические методы защиты информации	14	2	4		8
	ИТОГО по разделам дисциплины	72	14	14	-	44
	Контроль самостоятельной работы (КСР)	2				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	-				
	Общая трудоемкость по дисциплине	72				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Введение в информационную безопасность	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.	К
2	Правовое обеспечение информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной	Т
3	Организационное обеспечение информационной безопасности	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.	У
4	Технические средства и методы защиты информации	Инженерная защита объектов. Защита информации от утечки по техническим каналам.	У
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи. Использование средств стеганографии для защиты файлов. Изучение настроек средств антивирусной защиты информации.	К

6	Криптографические методы защиты информации	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Создание защищенного канала связи средствами виртуальной частной сети	У

Примечание: Т – тестирование, Р – написание реферата; ПР – практическая работа; К – коллоквиум, У- устный опрос.

2.3.2 Занятия семинарского типа.

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1	Введение в информационную безопасность	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.	ПР
2	Правовое обеспечение информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной	
3	Организационное обеспечение информационной безопасности	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.	ПР

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
4	Технические средства и методы защиты информации	Инженерная защита объектов. Защита информации от утечки по техническим каналам.	ПР
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи. Использование средств стеганографии для защиты файлов. Изучение настроек средств антивирусной защиты информации.	ПР
6	Криптографические методы защиты информации	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Создание защищенного канала связи средствами виртуальной частной сети	ПР

Лабораторные занятия - не предусмотрены
Примерная тематика курсовых работ (проектов) – не предусмотрена

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного материала	1. Бабаш, А.В. Информационная безопасность (+ CD-ROM) [Текст] / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с. 2. Васильков, А.В. Безопасность и управление доступом в информационных системах [Текст] / А.В. Васильков, И.А. Васильков. – М.: Форум, 2015. - 368 с. 3. Гафнер, В. В. Информационная безопасность [Текст] / В.В. Гафнер. – М.: Феникс, 2014. – 336 с. 4. Степанов, Е.А. Информационная безопасность и защита информации: учебное пособие [Текст] / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2017. – 304 с. 5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] / В.Ф. Шаньгин. – М.: Форум, Инфра-М, 2017. – 416 с.
2	Написание реферата	Написание и оформление рефератов. Учебно-методические указания для студентов геоинформатиков, утвержденные на заседании кафедры геоинформатики протокол №10 от 2.06.2017 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В освоении программы дисциплины «Информационная безопасность» имеют место различные образовательные технологии. Прежде всего, это практические занятия, информационные, тестовые, а также дискуссии по основным темам программы, презентации. Во время аудиторных занятий обучение проводится преимущественно в виде практических занятий с использованием подходов проблемного обучения. Самостоятельная работа студентов осуществляется под руководством преподавателя и предполагает консультации, помощь в подготовке и написании рефератов и т.д.

Для реализация компетентного подхода предусматривается использование в учебном процессе активных и интерактивных форм проведения аудиторных и внеаудиторных занятий (интерактивного геоинформационного моделирования территорий, оптимизация пространственных размещений объектов, деловых и ролевых игр на примере разбора конкретных ситуаций – 20% объема аудиторных занятий) с целью формирования и развития профессиональных навыков обучающихся. Предусматриваются встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов. В процессе преподавания дисциплины применяются образовательные технологии лекционно-семинарско-зачетной системы обучения и развития критического мышления. При чтении курсов модуля применяются такие виды лекций, как вводная, обзорная, проблемная, лекция-презентация. Обязательны компьютерные практикумы по разделам дисциплины.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность». Оценочные средства включают контрольные материалы для проведения текущего контроля в форме тестирования, коллоквиума, доклада-реферата по проблемным вопросам, и промежуточной аттестации в форме вопросов к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИОПК-8.1. Использует современные информационные технологии в организации профессиональной деятельности.	Знать источники возникновения информационных угроз; каналы утечки информации; направления и средства защиты информации; принципы национальной безопасности; исследования, ведущиеся в области информационной безопасности. Уметь применять правовые, организационные, технические и программные средства защиты информации; выявлять потенциальные каналы утечки информации и	- Вопросы для коллоквиума, тестовые задания - Практические работы - Темы рефератов	Вопросы к зачету

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
		определять их характеристики; разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности; систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности. Владеть навыками противодействия утечке компьютер-ной информации; навыками использования электронной цифровой подписи; навыками проведения аудита локальной политики безопасности, аудита доступа к объектам; специальной терминологией, применяемой в процессе защиты информации; навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности		
2	ИОПК-8.1. Применяет	Знать порядок проведения анализа	- Вопросы для коллоквиума,	Вопросы к зачету

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
	современные информационные технологии в решении задач профессиональной деятельности.	информационной безопасности объектов и систем. Уметь проводить анализ информационной безопасности объектов информатизации. Владеть Навыками проведения анализа информацио-ной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	тестовые задания - Практические работы - Темы рефератов	

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

4.1 Фонд оценочных средств для проведения текущего контроля

Текущий контроль осуществляется в ходе проведения практических занятий в виде устного опроса, выполнения практических работ, рефератов. Перечень заданий к практическим занятиям приведен в фонде оценочных средств по дисциплине «Информационная безопасность».

Темы рефератов

1. Проведение анализа информационной системы. Выявление угроз и уязвимостей, каналов утечки информации

2. Построение системы защиты информации в информационной системе.

3. Разработка или подбор алгоритмов для использования в реальных информационных системах.

4. Программирование привязки ПО к аппаратному обеспечению.

5. Настройка межсетевых экранов.

6. Взлом систем защиты.

7. Исследование алгоритмов вирусов и антивирусов.

8. Классификация информации. Виды данных и носителей.

9. Ценность информации. Цена информации.

10. Количество и качество информации.

11. Виды защищаемой информации.

12. Демаскирующие признаки объектов защиты.

13. Классификация источников и носителей информации.

14. Мероприятия по управлению доступом к информации.

15. Функциональные источники сигналов. Опасный сигнал.

16. Основные средства и системы, содержащие потенциальные источники опасных сигналов.

17. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.

18. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

19. Виды угроз безопасности информации.

20. Основные принципы добывания информации.

21. Процедура идентификации, как основа процесса обнаружения объекта.

22. Методы синтеза информации.

23. Методы несанкционированного доступа к информации.

24. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

25. Способы наблюдения с использованием технических средств.

26. Каналы утечки информации. Технические каналы утечки

27. Классификация технических каналов утечки по физической природе носителя.

28. Классификация технических каналов утечки по информативности.

29. Классификация технических каналов утечки по времени функционирования.

30. Классификация технических каналов утечки по структуре.

31. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.

32. Перехват электромагнитных излучений.

33. Акустическое подслушивание. Эффекты, возникающие при подслушивании.

34. Понятия скрытия информации, виды скрытий. Информационный портрет.

35. Противодействие наблюдению. Способы маскировки.

36. Способы и средства противодействия подслушиванию.

37. Нейтрализация закладных устройств.

38. Состав инженерной защиты и технической охраны объектов.

39. Инженерные конструкции и сооружения для защиты информации. Их классификация.

40. Средства идентификации личности.

41. Классификация датчиков охранной сигнализации.

42. Классификация извещателей.

43. Телевизионные системы наблюдения.

44. Основные средства системы видеоконтроля.

45. Защита личности как носителя информации.

46. Системный подход к защите информации.

47. Параметры системы защиты информации.

48. Этапы проектирования системы защиты информации.

49. Потенциальные каналы утечки информации.

50. Этапы разработки мер по предотвращению угроз утечки информации.

Контрольные вопросы для устного опроса

1. Основные определения и критерии классификации угроз.

2. Угроза и их классификация.

3. Атака.

4. Окно опасности.

5. Наиболее распространенные угрозы доступности.

6. Угрозы доступности, классифицированные по компонентам ИС, на которые нацелены, угрозы.

7. Примеры угроз доступности.

8. Вредоносное программное обеспечение.

9. Грани вредоносного ПО.

10. Основные угрозы целостности.

11. Основные угрозы конфиденциальности.

12. Что такое законодательный уровень информационной безопасности и почему он важен?

13. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.

14. Закон «об информации, информатизации и защите информации» и устанавливаемые им основные определения.

15. Цели защиты информации согласно закону «об информации, информатизации и защите информации».

16. Закон «О лицензировании отдельных видов деятельности» и его определения.

17. Электронный документ, электронная цифровая подпись, владелец сертификата ключа подписи, средства электронной цифровой подписи, сертификат средств электронной цифровой подписи.

18. Закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой. подписи, сертификат ключа подписи, подтверждение подлинности электронной цифровой. подписи в электронном документе, информационная система общего пользования,

19. Корпоративная информационная система.

20. Особенности зарубежного законодательства в области информационной безопасности.

21. Текущее состояние российского законодательства в области информационной безопасности.

22. Оценочные стандарты и технические спецификации. Основные понятия.

23. Какими двумя основным критериям оценивается степень доверия?

24. Механизмы безопасности.

25. Классы безопасности.

26. Информационная безопасность распределенных систем.

27. Сервисы безопасности и исполняемые ими роли.

28. Сетевые механизмы безопасности.

29. Администрирование средств безопасности.

30. Стандарт iso/iec 15408 «Критерии оценки безопасности информационных технологий» основные понятия.

31. Классы функциональных требований «оранжевой книги».

32. Требования доверия безопасности.

33. Европейские критерии информационной безопасности.

34. Интерпретация «оранжевой книги» для сетевых конфигураций.

35. Руководящие документы гостехкомиссии России в области информационной безопасности.

Пример теста для контроля знаний обучающихся

1. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

а) со стороны злоумышленника;

б) со стороны законного отправителя сообщения;

в) со стороны законного получателя сообщения.

2. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?

а) асимметричный;

б) симметричный;

в) правильного ответа нет.

3. Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:

а) шифрование;

б) дешифровка;

в) расшифровка.

4. В каких основных форматах существует симметричный алгоритм?

а) блока и строки;

б) потока и блока;

в) потока и данных

5. Открытым текстом в криптографии называют:

а) расшифрованный текст;

б) любое послание;

в) исходное послание.

6. Какой ключ известен только приемнику?

а) открытый;

б) закрытый.

7. Наука, занимающаяся защитой информации, путем преобразования этой информации это:

а) Криптография;

б) криптология;

в) криптоанализ.

8. В каких шифрах результат шифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных?

а) в потоковых;

б) в блочных.

9. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:

а) шифр функциональных преобразований;

б) шифр замен;

в) шифр перестановок.

10. Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:

а) функция шифрования шага преобразования;

б) инвариант стандартного шага шифрования.

11. Шифрование – это:

а) процесс создания алгоритмов шифрования;

б) процесс сжатия информации;

в) процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется.

12. В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?

а) при шифровании с помощью асимметричного алгоритма;

б) при шифровании с помощью симметричного алгоритма;

в) арбитр необходим всегда.

13. Можно ли отнести слабую аутентификацию к проблемам безопасности?

а) нет;

б) да;

в) в редких случаях.

14. Возможно ли расшифровывать информацию без знания ключа?

а) нет;

б) да;

в) в редких случаях.

15. Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?

а) нет;

б) да;

в) в редких случаях.

16. Характерная черта алгоритма Эль-Гамаля состоит в:

а) протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя;

б) в точной своевременной передаче сообщения;

в) алгоритм не имеет особенностей и идентичен RSA.

17. Аутентификацией называют:

а) процесс регистрации в системе;

б) способ защиты системы;

в) процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов.

18. Аутентификация бывает:

а) Статическая;

б) устойчивая;

в) постоянная;

г) все варианты правильные;

д) правильного варианта нет.

19. Стойкость ключа характеризуется

а) Длинной;

б) непредсказуемостью;

в) все варианты правильные;

г) правильного варианта нет.

20. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:

а) на основе произвольно выбранного шифротекста;

б) на основе произвольно выбранного открытого текста;

в) на основе только шифротекста.

21. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:

а) на основе произвольно выбранного шифротекста;

б) на основе произвольно выбранного открытого текста;

в) правильного ответа нет.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы к зачету

1. Определение информационной безопасности, защиты информации. Цели защиты информации. Современные задачи защиты информации.
2. Угрозы и риски информационной безопасности. Основные элементы описания угроз безопасности информации. Классификация угроз безопасности информации.
3. Основные положения Доктрины информационной безопасности Российской Федерации. Стратегия национальной безопасности РФ.
4. Лицензирование, сертификация и аттестация в области защиты информации.
5. Основные положения законов РФ «О персональных данных», «О коммерческой тайне».
6. Преступления в области защиты информации. Виды ответственности за правонарушения в информационной сфере в соответствии с

Уголовным кодексом РФ, Гражданским кодексом РФ, Кодексом об административных правонарушениях.

7. Порядок использования криптографических методов и средств для обеспечения секретности, подлинности, целостности и неотказуемости от авторства.

8. Определение криптографической системы, подходы к классификации криптографических систем. Государственное регулирование в области защиты информации с использованием средств криптографической защиты информации.

9. Понятие о криптографическом протоколе. Свойства протокола.

10. Криптографические хэш-функции.

11. Методы идентификации и аутентификации, общее понятие аутентификации.

12. Методы реализации контроля и разграничения доступа. Системы контроля и разграничения доступа.

13. Модель нарушителя при защите автоматизированных систем от несанкционированного доступа.

14. Программно-аппаратные средства защиты информации от несанкционированного доступа.

15. Технические каналы утечки информации при передаче информации по каналам связи. Основные характеристики типовых технических каналов утечки информации.

16. Технические каналы утечки информации средств вычислительной техники. Классификация технических каналов утечки информации.

17. Методы и средства антивирусной защиты. Организационно-правовые меры защиты информации.

18. Методы и способы активной/пассивной защиты информации от вирусной активности.

19. Антивирусная политика безопасности на объекте информатизации.

20. Системный подход при комплексной защите информации. Объект защиты. Различие комплексного и системного подхода к защите информации.

21. Управление информационной безопасностью. Роль и место процессов управления информационной безопасностью в составе современных систем защиты информации.

22. Организационно-правовые меры защиты информации.

23. Специфика обеспечения информационной безопасности в сетях связи. Политика обеспечения безопасности при осуществлении сетевого взаимодействия, включая случаи использования сетей связи общего пользования.

24. Программно-аппаратные средства обеспечения информационной безопасности в сетях.

25. Уязвимости, угрозы и средства защиты в интернете.

26. Типы ограничений целостности. Реляционная модель данных.

27. Защита информации в государственных информационных системах Российской Федерации. Основные положения и последовательность организации (выполнения) работ.

28. Проектирование автоматизированных систем в защищенном исполнении. Стадии проектирования автоматизированных систем.

29. Модель угроз безопасности информации. Использование банка данных угроз ФСТЭК России при построении модели угроз безопасности информации.

30. Классификация информационных систем. Порядок проведения классификации государственных информационных систем. Множественная классификация систем.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

11. Бабаш, А.В. Информационная безопасность (+ CD-ROM) [Текст] / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с.

2. Васильков, А.В. Безопасность и управление доступом в информационных системах [Текст] / А.В. Васильков, И.А. Васильков. – М.: Форум, 2015. - 368 с.

3. Гафнер, В. В. Информационная безопасность [Текст] / В.В. Гафнер. – М.: Феникс, 2014. – 336 с.

4. Степанов, Е.А. Информационная безопасность и защита информации: учебное пособие [Текст] / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2017. – 304 с.

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] / В.Ф. Шаньгин. – М.: Форум, Инфра-М, 2017. – 416 с.

5.2 Дополнительная литература:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. – М.: Наука, 2015. – 552 с.

2. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности: моногр. – М.: Международный гуманитарный фонд «Знание», 2014. – 416 с.

3. Рассел, Джесси Honeypot (информационная безопасность) [Текст] / Джесси Рассел. – М.: VSD, 2013. – 686 с.

4. Сальная, Л.К. Английский язык для специалистов в области информационной безопасности [Текст] / Л.К. Сальная, А.К. Шилов, Ю.А. Королева. – М.: Гелиос АРВ, 2016. – 208 с.

5. Федоров, А.В. Информационная безопасность в мировом политическом процессе [Текст] / А.В. Федоров. – М.: МГИМО-Университет, 2017. – 220 с.

6. Чипига, А.Ф. Информационная безопасность автоматизированных систем [Текст] / А.Ф. Чипига. – М.: Гелиос АРВ, 2013. – 336 с.

7. Шаньгин, Владимир Федорович Информационная безопасность и защита информации [Текст] / Шаньгин Владимир Федорович. – М.: ДМК Пресс, 2017. – 249 с.

8. Ярочкин, В. Безопасность информационных систем [Текст] / В. Ярочкин. – М.: Ось-89, 2016.– 320 с.

8. Ярочкин, В.И. Информационная безопасность [Текст] / В.И. Ярочкин. – М.: Академический проект, 2014. – 544 с.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com
6. Электронная библиотека КубГУ. – Режим доступа: http://docspace.kubsu.ru/docspace/handle/1/28.
7. Официальный сайт научно-технической библиотеки СГГА. – Режим доступа: http://lib.ssga.ru/.
8. Электронно-библиотечная система научно-издательского центра «ИНФРАМ». –Режим доступа: http://znanium.com/.

9. Электронно-библиотечная система издательства «Лань». – Режим доступа: http://e.lanbook.com/.

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. «Лекториум ТВ» http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

19. Научная электронная библиотека. – Режим доступа: http://elibrary.ru/.

Ресурсы свободного доступа:

1. КиберЛенинка (http://cyberleninka.ru/);
2. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
3. Федеральный портал "Российское образование" http://www.edu.ru/;
4. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
5. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
6. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
7. Служба тематических толковых словарей http://www.glossary.ru/;
8. Словари и энциклопедии http://dic.academic.ru/;
9. Образовательный портал "Учеба" http://www.ucheba.com/;
10. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала «ШКОЛЬНЫЕ ГОДЫ» http://icdau.kubsu.ru/

7. Методические указания для обучающихся по освоению дисциплины

По курсу предусмотрено проведение лекционных и семинарских занятий, на которых дается основной систематизированный материал по тематике дисциплины. Проводятся практические занятия, на которых изучается инструментарий основных интернет-ресурсов и специализированного программного обеспечения для работы с пространственными данными, размещенными в сети Интернет. По каждому разделу выполняется ряд практических заданий.

Важнейшим этапом курса является самостоятельная работа по дисциплине «Информационная безопасность», позволяющая студентам полноценно изучить отдельные темы, используя учебную литературу и ресурсы сети Интернет.

Лекционные занятия посвящены рассмотрению ключевых, базовых положений курса и разъяснению учебных заданий, выносимых на самостоятельную проработку.

Практические занятия предназначены для приобретения опыта практической реализации основной профессиональной образовательной программы. Методические указания к практическим работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется перед проведением практических работ.

Самостоятельная работа студентов включает следующие виды: проработка учебного материала лекций, подготовка к лабораторным работам, подготовка к текущему контролю и другие виды самостоятельной работы.

Результаты всех видов работы студентов формируются в виде их личного рейтинга, который учитывается на промежуточной аттестации.

Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников.

Текущий контроль успеваемости проводится в течение каждого раздела. Освоение дисциплины и ее успешное завершение на стадии промежуточной аттестации возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля. Набрать рейтинг по всем разделам дисциплины в каждом семестре, пройти плановые контрольные мероприятия в течение экзаменационной сессии невозможно. Для завершения работы в семестре студент должен выполнить все контрольные мероприятия. Промежуточная аттестация по дисциплине «Информационная безопасность» проходит в форме зачета

В процессе выполнения практических работ студенты закрепляют полученные на предварительно теоретические знания, приобретают навыки их практического применения, готовятся к итоговой аттестации. Важным аспектом является также привитие навыков самостоятельной организации работы и выполнения поставленных задач на начальном этапе обучения картографированию.

Контроль выполнения в полном объеме и в надлежащем качестве практических заданий позволяет оценить активность работы студента в течение семестра, а также его продвижение в изучении дисциплины. Кроме того, такой подход позволяет контролировать развитие практических навыков студента.

При подготовке к занятию студенты в первую очередь должны использовать материал лекций и соответствующих литературных и картографических источников.

В начале практических занятий студенты получают общую информацию о формах проведения занятий и формах контроля знаний. Одновременно

студентам предоставляется список тем практических заданий, а также тематика рефератов.

Контроль качества подготовки к каждому занятию осуществляется путем разнообразной проверки знаний, в частности, путем диалога, задавая вопросы по соответствующей теме. В качестве одной из наиболее удобных форм промежуточной аттестации практикуется тестирование.

Типовой план практических занятий выглядит следующим образом:

1. Изложение преподавателем темы занятия, его целей и задач.
2. Необходимые пояснения по структурным частям задания.
3. Выполнение задания студентами под руководством преподавателя.
4. Анализ полученных результатов. Коллективное обсуждение результатов. Резюме преподавателя.

Итоговый контроль по конкретной практической работе осуществляется преподавателем посредством проверки качества и полноты выполненного задания.

Методические рекомендации для подготовки к зачету

Итоговым контролем уровня усвоения материала студентами является зачет. Зачет проводится по вопросам, из материала изученного курса. Для эффективной подготовки к зачету процесс изучения материала курса предполагает достаточно интенсивную работу не только на лекциях, но и с различными текстами, нормативными документами и информационными ресурсами.

Особое внимание надо обратить на то, что подготовка к зачету требует обращения не только к учебникам, но и к информации, содержащейся в СМИ, а также в Интернете.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

– Использование электронных презентаций при проведении лекционных занятий

– Выполнение интерактивных заданий на компьютере как в локальном ПО, так и в сети интернет

– Проверка домашних заданий и консультирование посредством электронной почты.

8.2 Перечень необходимого программного обеспечения.

– Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»).

– Программы для демонстрации и создания презентаций («Microsoft Power Point»).

– Дистрибутив пакета прикладных программ Statistica.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) 1. Аудитория лекционно-семинарского типа (ауд.200), ул. Ста 149 (Мультимедийная аудитория с выходом в ИНТЕРНЕТ: ко стульев; доска учебная.; проектор Mitsubishi XD500U; экран; B570 i3-2370M/4G500/nV410M/1G/DVDRW/Cam/W7HB/15,6 2. Аудитория лекционно-семинарского типа (ауд.201), ул. Ста 149 (Мультимедийная аудитория с выходом в ИНТЕРНЕТ: ко доска учебная.; проектор ViewSonic PJ562; комплекс мультим Smart Board; ноутбук Lenovo B570 i3-2370M/4G500/nV410M/1G/DVDRW/Cam/W7HB/15,6HD) 3. Аудитория лекционного типа (ауд.204), ул. Ставропольская (Мультимедийная лаборатория с выходом в ИНТЕРНЕТ: 13 рабочих станций с графикой 256 GB) + монитор Aquarius TF1910W, 24 стула, 10 компьютерных столов, 1 стол для сервера) и соот (Microsoft Windows 7, Microsoft Office 2007, ERSI ArcGIS 10. станций и серверов: Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Education Renewal License.)
2.	Семинарские занятия	Специальное помещение, оснащенное персональными компьютерами с доступом к сети Интернет и соответствующим программным обеспечением (ПО), указанным в п. 8.2 1. Аудитория лекционно-семинарского типа (ауд.200), ул (Мультимедийная аудитория с выходом в ИНТЕРНЕТ: компл + 40 стульев; доска учебная.; проектор Mitsubishi XD500U; эк трибуна; ноутбук Lenovo B570 i3-2370M/4G500/nV410M/1G/D 2. Аудитория лекционно-семинарского типа (ауд.201), ул. Ставрополь- ская, 149 (Мультимедийная аудитория с выходом в ИНТЕРНЕТ: комплект учебной мебели – 21 стол + 42 стула; доска учебная.; проектор ViewSonic PJ562; комплекс мультимедийный интерактивный демонстрационный Smart Board; ноутбук Lenovo B570 i3-2370M/4G500/nV410M/1G/DVDRW/Cam/W7HB/15,6HD)
3.	Лабораторные занятия	Не предусмотрены
4.	Курсовое проектирование	Кабинет для выполнения курсовых работ
5.	Групповые	Аудитория, (кабинет)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
	(индивидуальные) консультации	
6.	Текущийконтроль, промежуточная аттестация	Аудитория, (кабинет)
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета. Аудитория лекционного типа (ауд.204), ул. Ставропольская, презентационной техникой (Мультимедийная лаборатория с ИНТЕРНЕТ: 13 рабочих станций с графикой Aquarius EltE50 4 GB, HDD 256 GB) + монитор Aquarius TF1910W, 24 стула, 10 компьютерных столов, 1 стол для сервера) и соо программным обеспечением (Microsoft Windows 7, Microsoft ERSI ArcGIS 10. Антивирусная защита физических рабочих серверов: Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educatior License.)