МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет Информатики и Информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Кафедра
Информационных технологий и безопасности компьютерных систем
факультета Информатики и информационных технологий

Образовательная программа бакалавриата

09.03.02 Информационные системы и технологии

Направленность (профиль) программы:
Технологии разработки безопасного программного обеспечения
информационных систем

Форма обучения
Очная

Статус дисциплины:
Входит в обязательную часть ОПОП

Махачкала, 2022

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в 2022 году в соответствии с требованиями ФГОС ВО – бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии от «19» сентября 2017 г. № 926.

Разработчик: Карапац Александр Николаевич, к. ф.-м. н.,

старший преподаватель кафедры ИТиБКС

Рабочая программа дисциплины одобрена:

на заседании кафедры ИТиБКС от «16» марта 2022 г., протокол № 8.

Зав. кафедрой _____ Ахмедова З.Х.
(подпись)

на заседании Методической комиссии факультета ИиИТ

от «17» 03 2022 г., протокол № 7.

Председатель _____ Бакмаев А.Ш.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «31» 03 2022 г. _____

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Информационная безопасность и защита информации» входит в *обязательную* часть образовательной программы *бакалавриата* по направлению 09.03.02 Информационные системы и технологии.

Дисциплина реализуется на факультете Информатики и информационных технологий кафедрой Информационных технологий и безопасности компьютерных систем**.**

Содержание дисциплины охватывает круг вопросов, связанных с информационной безопасностью и защитой информации. Изучаются составляющие информационной безопасности, угрозы и риски, стандарты и спецификации, нормативно-правовые документы, регламентирующие информационную деятельность, меры по защите персональных данных и информационных систем, основы криптографии, вопросы обеспечения безопасности компьютерных сетей и так далее.

Целью освоения дисциплины «Информационная безопасность и защита информации» является формирование теоретических знаний и практических навыков по организации системы защиты информации в учреждениях.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных – **ОПК-2**, профессиональных – **ПК-2.**

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия, лабораторные занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме – *контрольная работа, отчеты по лабораторным работам* и промежуточный контроль в форме - *зачета, экзамена*.

Объем дисциплины 4 зачетные единицы, в том числе в академических часах по видам учебных занятий:

Очная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
5	108	56	28	28				52	зачет

1. Цели освоения дисциплины

Целью освоения дисциплины «Информационная безопасность и защита информации» является получение базовой подготовки в области информационной безопасности и защиты информации, навыков по применению стандартов и нормативно-правовых документов по информационной безопасности для организации системы защиты информации в учреждениях и последующей самостоятельной работы со специальной литературой и изучения профильных материалов.

Задачи освоения дисциплины состоят в получении знаний, составляющих основу представлений об информации, информационной безопасности, системах защиты информации, мерах и принципах информационной защиты; приобретении практических навыков работы с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий (ИКТ); выработке навыков применения средств ИКТ в повседневной жизни, при выполнении индивидуальных и коллективных проектов, в учебной деятельности, дальнейшем освоении специальностей, востребованных на рынке труда.

2.Место дисциплины в структуре ОПОП бакалавриата

«Информационная безопасность и защита информации» входит в *обязательную* часть образовательной программы *бакалавриата* по направлению 09.03.02 Информационные системы и технологии.

Дисциплина «Информационная безопасность и защита информации» включает в себя такие разделы, как основы информационной безопасности и защиты информации; стандарты обеспечения информационной безопасности; программно-технические сервисы информационной безопасности.

Входными требованиями, необходимыми для освоения дисциплины «Информационная безопасность и защита информации» является наличие у обучающихся компетенций, сформированных на предыдущем уровне образования.

Требования к первоначальному уровню подготовки обучающихся для успешного освоения дисциплины:

Уровень «знать»:

История развития информатики и вычислительной техники;

Основные принципы компьютерной обработки информации.

Процедурный подход и основные понятия программирования;

Основные понятия и конструкции языков программирования высокого уровня;

Простые модели описания информационных процессов;

Уровень «уметь»:

Реализовывать простые программы на одном из языков программирования высокого уровня;

Строить информационные модели обработки информации;

Применять базовые модели и технологии к созданию программ.

На данную дисциплину «Информационная безопасность и защита информации» опираются дисциплины:

Моделирование систем

Архитектура информационных систем

Информационные технологии

Системное программирование

Управление данными

Методы и средства проектирования информационных систем и технологий

Надежность информационных систем

Управление ИТ-проектами

Техническая защита информации

Научно-исследовательская работа;

Итоговая государственная аттестация.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Код и наименование компетенции из ОПОП	**Код и наименование индикатора достижения компетенций** *(в соответствии с ОПОП)*	**Планируемые результаты обучения**	**Процедура освоения**
ОПК-2. Способен понимать принципы работы информационных технологии и программных средств, в том числе отечественного	ИД1.ОПК-2.1. Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной	Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Устный опрос, письменный опрос, лабораторная работа

производства, и использовать их при решении задач профессиональной деятельности;	деятельности. ИД2.ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ИД3. ОПК-2.3.Имеет навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	
ПК-2. Способность готовить презентации, оформлять научно-технические отчеты по результатам выполненной работы, публиковать результаты исследований в виде статей и докладов на научно-технических конференциях.	ПК-2.1. Знает современные программные продукты по подготовке презентаций и оформлению научно-технических отчетов ПК-2.2. Умеет готовить презентации и оформлять научные отчеты ПК-2.3. Имеет навыки по подготовки статей и докладов на научно-технических конференциях	Знает современные программные продукты по подготовке презентаций и оформлению научно-технических отчетов. Умеет готовить презентации и оформлять научные отчеты. Имеет навыки по подготовки статей и докладов на научно-технических конференциях.	Устный опрос, письменный опрос, лабораторная работа

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетные единицы, 144 академических часа.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме

№ п/п	Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости и промежуточной аттестации
			Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. ***(Основы информационной безопасности и защиты информации)***							
1	Введение в информационную безопасность и защиту информации	5	2		2		5	Лабораторно-практические задания, устный и письменный опросы
2	Нормативно-правовое обеспечение информационной	5	2		2		5	Лабораторно-практические задания, устный и письменный опросы

	безопасности							
3	Защита персональных данных	5	2		2		5	Лабораторно-практические задания, устный и письменный опросы
4	Компьютерные вирусы и защита от них	5	2		2		5	Лабораторно-практические задания, устный и письменный опросы
	Итого по модулю 1:		**8**		**8**		**20**	
	Модуль 2**.** (***Стандарты обеспечения информационной безопасности***)							
5	Стандарты и спецификации в области информационной безопасности	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
6	Экономика информационной безопасности	5	2		2		4	Лабораторно-практические задания, устный и письменный опросы
7	Идентификация и аутентификация	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
8	Управление доступом, протоколирование и аудит	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
9	Организационное обеспечение системы защиты информации	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
	Итого по модулю 2:		**10**		**10**		**16**	
	Модуль 3. (***Программно-технические сервисы информационной безопасности***)							
10	Сервисы защиты персональных данных	5	2		2		4	Лабораторно-практические задания, устный и письменный опросы
11	Программно-технические средства защиты информации	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
12	Основы криптографии	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
13	Модели и методики безопасности	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
14	Экранирование и анализ защищенности, туннелирование и управление	5	2		2		3	Лабораторно-практические задания, устный и письменный опросы
	Итого по модулю 3:		**10**		**10**		**16**	
	ИТОГО:		28		28		52	

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1. Основы информационной безопасности и защиты информации

1	Введение в информационную безопасность и защиту информации
	Общие понятия и определения. Информация и данные. Свойства информации. Единицы измерения информации. Функции информации. Информация как товар и как субъект управления. Задачи информационной безопасности для разных категорий субъектов. Направления информационной безопасности. Составляющие информационной безопасности.
2	Нормативно-правовое обеспечение информационной безопасности
	Конституция РФ и Стратегия национальной безопасности – основополагающие документы по информационной безопасности. Защита информации - Закон №149-ФЗ. Государственная тайна - Закон №5485-1. КИИ - Закон № 187-ФЗ.

	Ответственность за нарушения в сфере информационной безопасности.
3	Защита персональных данных
	Понятие персональных данных. Операторы персональных данных. Закон РФ «О персональных данных» №152-ФЗ. Регуляторы в области защиты персональных данных. Нормативно-правовые акты по защите персональных данных. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
4	Компьютерные вирусы и защита от них
	Понятие компьютерных вирусов. Классификация вирусов. Способы защиты от вирусов. Виды антивирусных программ. Профилактика и лечение компьютерных вирусов.

Модуль 2. Стандарты обеспечения информационной безопасности

5	Стандарты и спецификации в области информационной безопасности
	Оценочные стандарты и технические спецификации. Информационная безопасность распределенных систем. «Критерии оценки безопасности информационных технологий». Гармонизированные критерии Европейских стран. Руководящие документы ФСТЭК России.
6	Экономика информационной безопасности
	Понятие угрозы и риска. Источники угроз. Виды угроз. Систематизация рисков. Измерение рисков, шкалы рисков. Формирование качественных и количественных оценок рисков. Оценки потерь. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь, обоснование прогноза потерь и ущерба. Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации.
7	Идентификация и аутентификация
	Понятие идентификации и аутентификации. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos. Идентификация /аутентификация с помощью биометрических данных.
8	Управление доступом, протоколирование и аудит
	Логическое управление доступом. Ролевое управление доступом. Управление доступом в распределенной объектной среде. Понятия протоколирования и аудита. Активный аудит.
9	Организационное обеспечение системы защиты информации
	Особенности работы с персоналом, владеющим конфиденциальной информацией. Персонал как основная опасность утраты конфиденциальной информации. Особенности приема на работу, связанную с владением конфиденциальной информацией. Идентификация и установление подлинности объекта. Идентификация и установление подлинности личности. Идентификация и установление подлинности документов.

Модуль 3. Программно-технические сервисы информационной безопасности

10	Сервисы защиты персональных данных
	Виды сервисов защиты персональных данных. Облачные сервисы. Электронный документооборот. Автоматизированная разработка организационно-распорядительной документации. Сервис «Альфа-док». Готовность к проверкам регуляторов в области защиты персональных данных.
11	Программно-технические средства защиты информации
	Основные понятия программно-технического уровня информационной безопасности. Технические средства защиты объектов. Системы охранной сигнализации на территории и в помещениях объекта обработки информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий и аварийных ситуаций.
12	Основы криптографии
	Основные понятия. Классификация шифров. Симметричное и асимметричное шифрование, поточное и блочное шифрование. Протоколы и алгоритмы шифрования. Системы управления ключами. Электронная подпись.
13	Модели и методики безопасности
	Модели безопасности и их применение. Модель матрицы доступа. Модель распространения прав доступа. Модель многоуровневой защиты данных. Управление рисками. Методики оценки рисков. Модель качественной оценки. Количественная модель рисков. Использование списков уязвимостей в управлении рисками.
14	Экранирование и анализ защищенности, туннелирование и управление
	Основные понятия экранирования. Архитектурные аспекты экранирования. Классификация межсетевых экранов. Анализ защищенности. Туннелирование и управление.

4.3.3. Содержание лабораторных занятий по дисциплине.

№	час.	Название, содержание
1	2	Методы поиска и сбора информации.
		Поиск требуемой информации в интернете с использованием различных поисковых систем.
2	2	Защита информации в интернете.
		Изучение методов и программного обеспечения для защиты информации в интернете.
3	2	Сравнительный анализ понятийных аппаратов различных источников в области защиты информации.
		Ознакомление с различными подходами к определению ключевых понятий в области защиты информации путем поиска в интернете.
4	2	Анализ нормативно-правовых документов по информационной безопасности.
		Изучение ответственности за нарушения в области информационной безопасности.
5	2	Анализ нормативно-правовых документов в области защиты персональных данных.
		Изучение ответственности за нарушения в области защиты персональных

		данных.
6	2	Программное обеспечение для анализа управления рисками информационной системы.
		Изучение программного обеспечения для анализа управления рисками информационной системы.
7	4	Изучение программного комплекса «Альфа-док».
		Регистрация для тестовой работы в сервисе по защите персональных данных «Альфа-док» и изучение возможностей программного комплекса.
8	4	Разработка организационно-распорядительной документации по защите персональных данных в программном комплексе «Альфа-док».
		Разработка организационно-распорядительной документации по защите персональных данных, используя тестовую регистрацию в сервисе «Альфа-док».
9	2	Организационные меры для защиты информации при работе с персоналом.
		Изучение организационных мер для защиты информации при работе с персоналом.
10	2	Исследование возможностей Windows по формированию политики безопасности парольной системы аутентификации.
		Ознакомление с политикой безопасности парольной системы аутентификации в ОС Windows.
11	2	Исследование возможностей Windows по настройке параметров регистрации и аудита.
		Изучение настроек параметров системы регистрации и аудита событий в ОС Windows и анализ результатов по журналам ОС Windows.
12	2	Изучение программно-технических средств защиты информации.
		Изучение методов программно-технической защиты информации и применяемого программного обеспечения.

5. Образовательные технологии

Рекомендуемые образовательные технологии: лекции, лабораторные занятия, самостоятельная работа студентов.

В соответствии с требованиями ФГОС ВПО по направлению подготовки реализация компетентного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 30% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ОПОП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 30% аудиторных занятий (определяется соответствующим ФГОС)).

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Методические материалы для обеспечения СРС готовятся преподавателем и могут размещаться на персональном сайте преподавателя, либо на платформе электронного обучения. Кроме того, на основе рабочей программы дисциплины может составляться план-график, где преподаватель устанавливает рекомендуемые сроки предоставления на проверку результатов самостоятельной работы студента: контрольных работ, отчетов по лабораторным практикумам, индивидуальных

домашних заданий, рефератов, курсовых работ и др., советует использование основных и дополнительных источников литературы.

ЭОР ДГУ. Направление 09.03.02 Информационные системы и технологии.
http://eor.dgu.ru/Default/NProfileUMK/?code=09.03.02&profileId=4197

Примерное распределение времени самостоятельной работы студентов

Вид самостоятельной работы	Примерная трудоёмкость, а.ч.		
	Очная	Очно-заочная	Заочная
Текущая СРС			
работа с лекционным материалом, с учебной литературой	***14***		
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	***4***		
самостоятельное изучение разделов дисциплины	***4***		
выполнение домашних заданий, домашних контрольных работ			
подготовка к лабораторным работам, к практическим и семинарским занятиям	*8*		
подготовка к контрольным работам, коллоквиумам, зачётам	*20*		
подготовка к экзамену (экзаменам)			
другие виды СРС (указать конкретно)			
Творческая проблемно-ориентированная СРС			
выполнение расчётно-графических работ			
выполнение курсовой работы или курсового проекта			
поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	***2***		
исследовательская работа, участие в конференциях, семинарах, олимпиадах			
анализ данных по заданной теме, выполнение расчётов, составление схем и моделей на основе собранных данных			
другие виды ТСРС (указать конкретно)			
Итого СРС:	***52***		

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания

Примерные вопросы для зачета:

1. Информация и данные. Свойства информации. Функции информации.
2. Понятие информационной безопасности. Составляющие информационной безопасности.
3. Понятие защиты информации. Направления защиты информации.
4. Концепция информационной безопасности. Задачи информационной безопасности.
5. Система защиты информации. Уровни формирования режима информационной безопасности
6. Служба информационной безопасности. Основные понятия, задачи, функции, структура.
7. Подготовка специалистов по информационной безопасности. Оценка эффективности службы информационной безопасности.
8. Нормативно-правовое обеспечение информационной безопасности. Основные документы.
9. Государственная тайна и ее защита.
10. Ответственность за нарушения в сфере информационной безопасности.
11. Защита персональных данных. Понятия и основные документы.
12. Регуляторы в области защиты персональных данных. Их функции и требования.
13. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
14. Угрозы и риски информационной безопасности. Источники угроз. Виды угроз.
15. Риски нарушения информационной безопасности. Систематизация рисков.

16. Типовые модели нападения. Классификация атак.
17. Понятие компьютерных вирусов. Хронология развития вирусов.
18. Классификация вирусов. Вирусоподобные программы.
19. Антивирусные программы. Их классификация.
20. Профилактика и лечение компьютерных вирусов.
21. Стандарты и спецификации информационной безопасности. Их развитие.
22. Задачи ФСТЭК России по информационной безопасности и основные документы.
23. Особенности работы с персоналом, владеющим конфиденциальной информацией.
24. Особенности приема на работу, связанную с владением конфиденциальной информацией.
25. Идентификация и установление подлинности объекта, личности, документов.
26. Понятие идентификации и аутентификации. Парольная аутентификация. Одноразовые и многоразовые пароли.
27. Идентификация и аутентификация с помощью биометрических данных.
28. Логическое и ролевое управление доступом.
29. Понятия протоколирования и аудита. Активный аудит.
30. Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка. Модель угроз.
31. Измерение рисков, шкалы рисков. Формирование качественных и количественных оценок рисков.
32. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь.
33. Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации.
34. Модели безопасности. Модель матрицы доступа.
35. Модель распространения прав доступа. Модель многоуровневой защиты данных.
36. Методики и программные продукты для оценки рисков информационной безопасности.
37. Виды сервисов защиты персональных данных. Электронный документооборот.
38. Автоматизированная разработка организационно-распорядительной документации. Сервис «АльфаДок».
39. Выходные документы в сервисе «АльфаДок». Дополнительные функции сервиса «АльфаДок».
40. Основные понятия программно-технического уровня информационной безопасности. Технические средства защиты объектов.
41. Системы охранной сигнализации на территории и в помещениях объекта обработки информации.
42. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Защита от случайных воздействий и аварийных ситуаций.
43. Криптография и шифрование. Классификация шифров.
44. Протоколы и алгоритмы шифрования. Системы управления ключами.
45. Электронная подпись. Принцип работы, применение и порядок получения.
46. Средства защиты информации в автоматизированных системах.
47. Межсетевое экранирование. Классификация межсетевых экранов.
48. Анализ защищенности информационных систем.
49. Понятие доступности. Основы мер обеспечения высокой доступности.
50. Понятие туннелирования и управления. Их применение.

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающая из текущего

контроля - _50___% и промежуточного контроля - __50___%.
Текущий контроль по дисциплине включает:
- посещение занятий - _10_ баллов,
- участие на практических занятиях - __ баллов,
- выполнение лабораторных заданий - _40__баллов,
- выполнение домашних (аудиторных) контрольных работ - __ баллов.
Промежуточный контроль по дисциплине включает:
- устный опрос - _50_ баллов,
- письменная контрольная работа - __ баллов,
- тестирование - ___ баллов.

8. Учебно-методическое обеспечение дисциплины.

а) Адрес сайта:
кафедра ИТиБКС http://cathedra.dgu.ru/?id=2583

б) основная литература:

1. **Галатенко В. А.** Стандарты информационной безопасности : курс лекций: учеб.пособие / Галатенко, Владимир Антонович ; под ред. В.Б.Бетелина; Интернет-ун-т информ. технологий. - 2-е изд. - М. : ИНТУИТ.ру, 2006. - 263 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 : 176-00.

2. **Мельников В. П.** Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обуч. по специальности "Информ. системы и технологии" / Мельников, Владимир Павлович, С. А. Клейменов ; под ред. С.А.Клейменова. - 5-е изд., стер. - М. : Академия, 2011, 2010. - 330,[6] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Допущено УМО. - ISBN 978-57695-7738-3 : 401-06.

3. **Проскурин В. Г.** Защита программ и данных : учеб. пособие для студентов вузов / Проскурин, Вадим Геннадьевич. - 2-е изд., стер. - М. : Академия, 2012. - 198,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - ISBN 978-5-7695-9288-1 : 486-20

4. **Шаньгин В.Ф.** Защита компьютерной информации. Эффективные методы и средства : учебное пособие / В. Ф. Шаньгин ; Шаньгин В. Ф. - М. : ДМК Пресс, 2010. - 544. - ISBN 978-5-94074-518-1

5. **Бабаш А. В.** Информационная безопасность: лаб. практикум; учеб. пособие / Бабаш, Александр Владимирович, Е. К. Баранов. - 2-е изд., стер. - И. : Кнорус, 2016, 2011. - 306-00.

6. **Вострецова Е.В.** Основы информационной безопасности: учебное пособие для студентов вузов. / Е.В.Вострецова. – Екатеринбург: Изд-во Урал. Ун-та, 2019. – 204 с.

7. **Закиров Р.Ш.** Информационная безопасность: конспект лекций / Р.Ш. Закиров. – Челябинск: Издательский центр ЮУрГУ, 2014 – 73 с.

8. **Карапац А.Н., Ахмедова З.Х.** Информационная безопасность: лабораторный практикум / Карапац А.Н., Ахмедова З.Х. – Махачкала: Изд-во ДГУ, 2022. – 26 с.

в) дополнительная литература:

1. **Расторгуев С. П.** Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телеком. систем" / Расторгуев, Сергей Павлович. - М. : Академия, 2007. - 186,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено

УМО. - ISBN 978-5-7695-3098-2 : 150-70.

2. **Шаньгин В. Ф.** Информационная безопасность компьютерных систем и сетей : учеб. пособие для студентов учреждений сред. проф. образования, обуч. по группе специальностей 2200 "Информатика и вычислительная техника" / Шаньгин, Владимир Фёдорович. - М. : ФОРУМ: ИНФРА-М, 2008. - 415 с. - (Профессиональное образование). - Рекомендовано МО РФ. - 194-92

3. **Анисимов А. А.** Менеджмент в сфере информационной безопасности : учеб. пособие / Анисимов, Александр Александрович. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2010. - 175 с. - (Основы информационных технологий). - ISBN 978-5-9963-0237-6 : 227-70.

4. **Богомолов В. А.** Экономическая безопасность : учеб. пособие для вузов / Богомолов, Виктор Александрович. - М. : ЮНИТИ-ДАНА, 2006. - 303 с. - Рекомендовано УМО. - ISBN 5-238-00971-2 : 110-00.

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

1) Электронный каталог Научной библиотеки ДГУ: http://elib.dgu.ru
2) Электронно-библиотечная система «Университетская библиотека онлайн»(архив): www.biblioclub.ru
3) Единое окно доступа к образовательным ресурсам. http://window.edu.ru/
4) Википедия http://www.wikipedia.org
5) Сайте электронных образовательных ресурсов ДГУ http://eor.dgu.ru

10. Методические указания для обучающихся по освоению дисциплины.

Лекционный курс. Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционного курса проводится систематическое изложение современных научных материалов по данной дисциплине.

Студенту необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях. Конспекты лекций следует использовать при подготовке к экзамену, практическим и лабораторным занятиям, контрольным тестам, коллоквиумам, при выполнении самостоятельных заданий.

Практические занятия. Практические занятия по информационной безопасности имеют целью получение закрепление и углубленную проработку лекционного материала, и развитие у студентов навыков самостоятельной подготовки.

Лабораторные занятия. Лабораторные занятия по информационной безопасности и защите информации имеют целью получение навыков самостоятельной работы с информационными ресурсами.

Прохождение всего цикла лабораторных занятий является обязательным условием допуска студента к экзамену. В случае пропуска занятий по уважительной причине пропущенное занятие подлежит отработке.

Специальное руководство, облегчающее работу студента по изучению темы, выдается для пользования на каждом занятии.

Изучив глубоко содержание учебной дисциплины, целесообразно разработать матрицу наиболее предпочтительных методов обучения и форм самостоятельной работы студентов, адекватных видам лекционных и лабораторных занятий.

Необходимо предусмотреть развитие форм самостоятельной работы, выводя студентов к завершению изучения учебной дисциплины на ее высший уровень.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Программные продукты

1. Операционная система Windows
2. Microsoft Office.
3. Программные средства сжатия данных WinRAR. WinArj. WinZip.
4. Распознавание текста ABBYY FineReader

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Реализация учебной дисциплины требует наличия типовой учебной аудитории с возможностью подключения технических средств. Учебная аудитория должна иметь следующее оборудование:

1) Компьютер, медиа-проектор, экран.
2) Программное обеспечение для демонстрации слайд-презентаций.

Лабораторные занятия по дисциплине проводятся в специально оборудованном информационном классе факультета ИиИТ. Помещение для работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ДГУ.

К каждой лабораторной работе имеются методические указания и рекомендации. Студенту дается задание, о выполнении которого он должен отчитаться перед преподавателем в конце занятия.