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

Экономический факультет

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

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

Образовательная программа специалитета

38.05.01 Экономическая безопасность

Направленность (профиль) программы:
Судебная экономическая экспертиза

Форма обучения
Очная, заочная

Статус дисциплины:
Входит в обязательную часть ОПОП

Махачкала, 2022

Рабочая программа дисциплины «Основы информационной безопасности» составлена в 2022 году в соответствии с требованиями ФГОС ВО – специалитет по специальности 38.05.01 Экономическая безопасность от 14 апреля 2021 г. № 293.

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» марта 2022 г., протокол № 7.

Председатель _____ Бакмаев А.Ш.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «17» марта 2022г. протокол № 7

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Основы информационной безопасности» входит в *обязательную* часть образовательной программы *специалитета* по направлению 38.05.01 Экономическая безопасность.

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

Содержание дисциплины охватывает круг вопросов, связанных с информационной безопасностью. 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 «Основы информационной безопасности» является формирование теоретических знаний и практических навыков по организации системы защиты информации в учреждениях.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных – **ОПК-5, ОПК-7.**

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме – *контрольная работа* и промежуточный контроль в форме - *зачета*.

Объем дисциплины 2 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 зачет	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
2	72	32	18		18			36	зачет

Заочная 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 зачет	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
2	72	8	6		2			64	зачет

1. Цели освоения дисциплины

Целью освоения дисциплины «Основы информационной безопасности» 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 специалитета

«Основы информационной безопасности» входит в *обязательную* часть образовательной программы *специалитета* по направлению 38.05.01 Экономическая безопасность.

Дисциплина «Основы информационной безопасности» включает в себя такие разделы, как основы информационной безопасности; программно-технические сервисы информационной безопасности.

Входными требованиями, необходимыми для освоения дисциплины «Основы информационной безопасности» 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 «Основы информационной безопасности» опираются дисциплины:

Оценка экономических рисков

Экономические преступления

Основы правоохранительной деятельностью

Национальная экономическая безопасность

Экономическая безопасность региона

Финансовая безопасность

Теневая экономика как угроза экономической безопасности

Защита государственной тайны

Защита персональных данных

Проблемы обеспечения экономической безопасности предприятия

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-5 Способен осуществлять профессиональную деятельность в соответствии с нормами профессиональной этики, нормами права, нормативными правовыми актами в сфере экономики, исключающими противоправное поведение.	ОПК-5. И-1. Демонстрирует знание норм профессиональной этики, норм права, нормативных правовых актов в сфере экономики, исключающих противоправное поведение. ОПК-5. И-2. Следует в своей профессиональной деятельности нормам профессиональной этики, нормам права, нормативным правовым актам в сфере экономики, исключающим противоправное поведение	Знает: нормы профессиональной этики, исключающие противоправное поведение; Знает: содержание, источники норм права, нормативные правовые акты в сфере экономики, институты права, состав субъектов правонарушений, квалифицирующие признаки преступлений и административных правонарушений в сфере экономики Умеет квалифицированно применять нормативные правовые документы в сфере экономики; умеет выявлять, фиксировать, предупреждать и пресекать правонарушения и преступления в сфере экономики. Умеет квалифицировать правонарушения и преступления в сфере экономики, определять основания и порядок привлечения к уголовной ответственности за экономические преступления.	Устный опрос, письменный опрос, практическое занятие.
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7. И-1. Понимает принципы работы современных информационных технологий. ОПК-7 И-2. Способен использовать современные информационные технологии для решения задач профессиональной деятельности	Знает: составляющие и принципы работы современных информационных технологий. Умеет: сопоставлять компоненты различных информационных технологий, осуществлять выбор информационной технологии, направленной на решение поставленных профессиональных задач. Умеет: применять для решения задач профессиональной деятельности современные информационные технологии Владеет: компьютерными методами сбора, хранения и обработки (редактирования) информации, применяемыми	Устный опрос, письменный опрос, практическое занятие.

		в сфере профессиональной деятельности	

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 2 зачетные единицы, 72 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	2	2	2			5	Устный и письменный опросы
2	Нормативно-правовое обеспечение информационной безопасности	2	2	2			5	Устный и письменный опросы
3	Защита персональных данных	2	2	2			5	Устный и письменный опросы
4	Экономика информационной безопасности	2	2	2			5	Устный и письменный опросы
	Итого по модулю 1:		**8**	**8**			**20**	
	Модуль 2. (***Программно-технические сервисы информационной безопасности***)							
5	Управление доступом в информационных системах	2	2	2			3	Устный и письменный опросы
6	Сервисы защиты персональных данных	2	2	2			4	Устный и письменный опросы
7	Программно-технические средства защиты информации	2	2	2			3	Устный и письменный опросы
8	Основы криптографии	2	2	2			3	Устный и письменный опросы
9	Организационное обеспечение системы защиты информации	2	2	2			3	Устный и письменный опросы
	Итого по модулю 2:		**10**	**10**			**16**	
	ИТОГО:		**18**	**18**			**36**	

4.2.2. Структура дисциплины в заочной 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	Нормативно-правовое обеспечение информационной безопасности	2	2	2			32	Устный и письменный опросы
	Итого по модулю 1:		**2**	**2**			**32**	
	Модуль 2. (***Программно-технические сервисы информационной безопасности***)							
2	Сервисы защиты персональных данных.	2	2				16	Устный и письменный опросы
3	Программно-технические средства защиты информации	2	2				16	Устный и письменный опросы
	Итого по модулю 2:		**4**				**32**	
	ИТОГО:		**6**	**2**			**64**	

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
	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	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.

Модуль 2. Программно-технические сервисы информационной безопасности

5	Управление доступом в информационных системах
	Понятие идентификации и аутентификации. Парольная аутентификация. Одноразовые пароли. Идентификация /аутентификация с помощью биометрических данных. Логическое управление доступом. Ролевое управление доступом. Управление доступом в распределенной объектной среде. Понятия протоколирования и аудита. Активный аудит.
6	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.
7	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.
8	Основы криптографии
	Основные понятия. Классификация шифров. Симметричное и асимметричное шифрование, поточное и блочное шифрование. Протоколы и алгоритмы шифрования. Системы управления ключами. Электронная подпись.
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.

4.3.2. Содержание практических занятий по дисциплине.

1	Основные понятия информационной безопасности
	Информация и данные. Свойства информации. Функции информации. Задачи и направления информационной безопасности. Составляющие информационной

	безопасности.
2	Нормативно-правовое обеспечение информационной безопасности
	Основополагающие документы по информационной безопасности. Закон о защите информации. Закон «О государственной тайне». Закон о КИИ. Ответственность за нарушения в сфере информационной безопасности.
3	Защита персональных данных
	Понятие персональных данных. Операторы персональных данных. Закон «О персональных данных». Регуляторы в области защиты персональных данных. Нормативно-правовые акты по защите персональных данных. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
4	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. Экономические проблемы информационных ресурсов.
5	Управление доступом в информационных системах
	Идентификация и аутентификация. Парольная аутентификация. Одноразовые пароли. Управление доступом. Протоколирование и аудит.
6	Сервисы защиты персональных данных
	Виды сервисов защиты персональных данных. Облачные сервисы. Электронный документооборот. Автоматизированная разработка организационно-распорядительной документации.
7	Программно-технические средства защиты информации
	Программно-технический уровень информационной безопасности. Технические средства защиты объектов. Методы и средства защиты информации от случайных воздействий и аварийных ситуаций.
8	Основы криптографии
	Основные понятия. Классификация шифров. Симметричное и асимметричное шифрование, поточное и блочное шифрование. Протоколы и алгоритмы шифрования. Системы управления ключами. Электронная подпись.
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.

5. Образовательные технологии

Рекомендуемые образовательные технологии: лекции, практические 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, индивидуальных домашних заданий, рефератов, курсовых работ и др., советует использование основных и дополнительных источников литературы.

ЭОР ДГУ. Направление 38.05.01 Экономическая безопасность.
http://eor.dgu.ru/Default/NProfileUMK/?code=38.05.01&profileId=4582

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	***12***		***20***
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	***4***		***8***
самостоятельное изучение разделов дисциплины	***4***		***8***
выполнение домашних заданий, домашних контрольных работ			
подготовка к лабораторным работам, к практическим и семинарским занятиям	*8*		***12***
подготовка к контрольным работам, коллоквиумам, зачётам	*4*		***8***
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	***4***		***8***
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:	***36***		***64***

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. Информационная безопасность и защита информации. Задачи информационной безопасности.
3. Направления информационной безопасности.
4. Составляющие информационной безопасности.
5. Нормативно-правовое обеспечение информационной безопасности. Основные документы.

6. Государственная тайна и ее защита.
7. Ответственность за нарушения в сфере информационной безопасности.
8. Защита персональных данных. Понятия и основные документы.
9. Регуляторы в области защиты персональных данных. Их функции и требования.
10. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
11. Угрозы и риски информационной безопасности. Источники угроз. Виды угроз.
12. Риски нарушения информационной безопасности. Систематизация рисков. Измерение рисков, шкалы рисков.
13. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь.
14. Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации.
15. Основные понятия программно-технического уровня информационной безопасности. Технические средства защиты объектов.
16. Системы охранной сигнализации на территории и в помещениях объекта обработки информации.
17. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Защита от случайных воздействий и аварийных ситуаций.
18. Понятие идентификации и аутентификации. Парольная аутентификация. Одноразовые и многоразовые пароли.
19. Идентификация и аутентификация с помощью биометрических данных.
20. Логическое и ролевое управление доступом.
21. Понятия протоколирования и аудита. Активный аудит.
22. Виды сервисов защиты персональных данных. Электронный документооборот.
23. Автоматизированная разработка организационно-распорядительной документации. Сервис «АльфаДок».
24. Выходные документы в сервисе «АльфаДок». Дополнительные функции сервиса «АльфаДок».
25. Криптография и шифрование. Классификация шифров.
26. Протоколы и алгоритмы шифрования. Системы управления ключами.
27. Электронная подпись. Принцип работы, применение и порядок получения.
28. Особенности работы с персоналом, владеющим конфиденциальной информацией.
29. Особенности приема на работу, связанную с владением конфиденциальной информацией.
30. Идентификация и установление подлинности объекта, личности, документов.

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 - _40_ баллов,
- выполнение лабораторных заданий - ___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.

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) Сайт 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 зачету, 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.

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.