МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ:
Декан, председатель совета
факультета ИС,ФиА
_____ Н.Л. Баламирзоев
15. 11 2018 г.

УТВЕРЖДАЮ:
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ Н.С.Суракатов_____
19. 11 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.В.ДВ.3 Техника защиты информации

Дляс пециальности 38.05.01 «Экономическая безопасность»

специализация Экономико-правовое обеспечение экономической безопасности

факультет Информационных систем, финансов и аудита

кафедра Информационная безопасность

Квалификация выпускника (степень) экономист

Форма обучения очная: курс 4:семестр(ы)8:

Всего трудоемкость в зачетных единицах (часах) 3ЗЕТ(108):

Лекции 17(час): Экзамен -

Практические (семинарские) занятия 34(час): Зачет 8 семестр):

Лабораторные занятия 17(час): Курсовая работа -(семестр):

Самостоятельная работа 40 (час).

Зав. кафедрой _____ Г.И. Качаева

Начальник УО _____ О.В.Магомаева

Программа составленав соответствии с требованиями ФГОСВОс учетом рекомендаций ООП ВО по специальности подготовки специалистов38.05.01 – Экономическая безопасность испециализации «Экономико – правовое обеспечение экономической безопасности».

Программа одобрена на заседании выпускающей кафедры ЭБНиБИ
от 14.11 2018 г., протокол № 3

Зав. выпускающей кафедрой по данному направлению _____ **Шахбанова И.К.**

ОДОБРЕНО:
Методической комиссией по
укрупненным группам специальностей
и направлению подготовки
38.00.00 – Экономика и управление

Председатель МК

_____ /А.М. Эсетова/
подпись И.О.Ф.
16.11.
2018г.

АВТОР(Ы) ПРОГРАММЫ:

Г.И. Качаева, к.э.н., ст. преп.
И.О.Ф., уч. степень, ученое звание

_____
подпись

1. **Цели освоения дисциплины**

Учебная дисциплина «Техника защиты информации» реализует требования федерального государственного образовательного стандарта высшего образования по специальности38.05.01 – Экономическая безопасностьи специализации «Экономико – правовое обеспечение экономической безопасности»

Цель дисциплины – ознакомить обучаемых с законодательными, организационными, программно – техническими мерами информационной безопасности, с действующими стандартами в этой области.

Задача дисциплины - знать правовые основы защиты компьютерной информации, технические и программные методы защиты информации в ИС, стандарты, модели и методы шифрования, методы защиты программ от вирусов

2. **Место дисциплины в структуре ООП специалитета**

Дисциплина «Техника защиты информации» относится к вариативной части учебного плана ФГОС ВО (дисциплина по выбору студента).

Для успешного усвоения данной дисциплины необходимо, чтобы обучаемый владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Информационная безопасность» и «Информатика».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Техника защиты информации»

В результате освоения дисциплины обучающийсядолжен обладать следующими общекультурными компетенциями:

- способностью понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы (ОК-1);
- способностью ориентироваться в политических, социальных и экономических процессах (ОК-3);
- способностью выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета (ОК-4);

способностью работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-5)

В результате освоения дисциплины обучающийсядолжен обладать следующими профессиональными компетенциями:

- способностью на основе статистических данных исследовать социально-экономические процессы в целях прогнозирования возможных угроз экономической безопасности (ПК-31);
- способностью проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности (ПК-32);
- способностью анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в учетно-отчетной документации, использовать полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности (ПК-33).

В результате изучения дисциплины обучаемый должен:

Знать:

- сущность информационной безопасности автоматизированных информационных систем (АИС);
- источники возникновения информационных угроз;
- методы защиты информации в АИС;
- модели и принципы защиты информации от несанкционированного доступа;
- приемы организации доступа и управления им в АИС;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации;

уметь:

- применять методы защиты информации в АИС;
- обеспечивать разноуровневый доступ к информационным ресурсам АИС;
- реализовывать политику безопасности в АИС;
- обеспечивать антивирусную защиту информации;

иметь представление:

- о роли и месте знаний по дисциплине в сфере профессиональной деятельности.

4. Структура и содержание дисциплины (модуля) «Техника защиты информации»

Общая трудоемкость дисциплины составляет 3 зачетные единицы – 108 часов, в том числе: лекционных -17 часов, практических -34 часа, лабораторных - 17 часов, СРС -40 часов, форма отчетности зачет в 8 семестре.

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля (по срокам текущей аттестации)
				ЛК	ПЗ	ЛР	СРС	
1	2	8	4	5	6	7	8	9
3 семестр								
1.	**Лекция 1.** **Тема: Угрозы информационной безопасности и каналы утечки информации.** Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Противодействие угрозам.Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак.	3	1,2	2	4	2	5	Вх.контр. работа
2.	**Лекция 2.** **Тема: Организационно-правовое обеспечение информационной безопасности.** Понятия «организационная защита информации» и «режим защиты информации». Понятие «система организационной защиты информации»; субъекты и объекты системы. Анализ нормативных документов, регламентирующих основные принципы организации защиты информации. Проблемы защиты информации в автоматизированных системах.	3	3,4	2	4		5	
3.	**Лекция 3.** **Тема: Инженерно-технические методы и средства защиты информации.** Сущность и задачи комплексной системы	3	5,6	2	4		5	КР№1

	защиты информации (КСЗИ). Средства защиты информации в автоматизированных системах Экранирование для защиты информации в АС.							
4.	**Лекция 4.** **Тема: Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.** **Способы несанкционированного доступа к информации в информационных системах и защиты от него. Способы аутентификации пользователей.** Методы и способы защиты информации от несанкционированного доступа. Методы аутентификации. ААА.	3	7,8	2	4	2	4	
5.	**Лекция 5.** **Тема: Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.** Идентификация и установление личности. Разграничение доступа пользователей к ресурсам вычислительной системы. Защита ПК на уровне BIOS Средства защиты от несанкционированного доступа в ОС.	3	9,10	2	4	4	4	Кр№2
6.	**Лекция 6.** **Тема: Подсистема безопасности защищенных версий операционной системы Windows.Защита информации от несанкционированного доступа в операционных системах семейства Unix.** Обеспечение безопасности ОС Windows. Понятие защищенной операционной системы Типовая архитектура подсистемы защиты операционной системы Основные функции подсистемы защиты операционной системы. Основные защитные механизмы ос семейства unix Безопасность данных в ОС Unix.	3	11,12	2	4	3	4	
7.	**Лекция 7.** **Тема: Основные понятия криптологии. Симметричные и ассиметричные криптосистемы. Способы создания**	3	13,14	2	4	2	4	КР№3

	симметричных криптосистем. Абсолютно стойкий шифр. Криптографическая система DES и еѐ модификации. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.							
8.	**Лекция 8.** **Тема: Принципы построения ассиметричных криптографических систем. Электронная цифровая подпись и еѐ применение.** Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.	3	15,16	2	4	2	4	
9.	**Лекция 9.** **Тема: Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов.** Классификация вредоносных программ. Основы работы антивирусных программ.	3	17	1	2	2	5	
	Итого за семестр			**17**	**34**	**17**	**40**	Зачет

4.2. Содержание практических занятий

№	№ лекции из рабочей программы	Наименование и содержание лабораторной работы, практического занятия	Литература (№ источника из табл. прил. 12)	Кол-во часов
1	№ 1	**Угрозы информационной безопасности и каналы утечки информации.** Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Противодействие угрозам.Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак.	№ 1-3	4
2	№ 2	**Организационно-правовое обеспечение информационной безопасности.** Понятия «организационная защита информации» и «режим защиты информации». Понятие «система организационной защиты информации»; субъекты и объекты системы.	№ 1-5	4

		Анализ нормативных документов, регламентирующих основные принципы организации защиты информации. Проблемы защиты информации в автоматизированных системах.		
3	№ 3	**Инженерно-технические методы и средства защиты информации.** Сущность и задачи комплексной системы защиты информации (КСЗИ). Средства защиты информации в автоматизированных системах Экранирование для защиты информации в АС.	№1-7	4
4	№ 4	**Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.** **Способы несанкционированного доступа к информации в информационных системах и защиты от него. Способы аутентификации пользователей.** Методы и способы защиты информации от несанкционированного доступа. Методы аутентификации. AAA.	№ 1-9	4
5	№ 5	**Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.** Идентификация и установление личности. Разграничение доступа пользователей к ресурсам вычислительной системы. Защита ПК на уровне BIOS Средства защиты от несанкционированного доступа в ОС.	№ 3-11	4
6	№ 6	**Подсистема безопасности защищенных версий операционной системы Windows.Защита информации от несанкционированного доступа в операционных системах семейства Unix.** Обеспечение безопасности ОС Windows. Понятие защищенной операционной системы Типовая архитектура подсистемы защиты операционной системы Основные функции подсистемы защиты операционной системы. Основные защитные механизмы ос семейства unix Безопасность данных в ОС Unix.	№ 4-12	4
7	№ 7	**Основные понятия криптологии. Симметричные и ассиметричные**	№ 3-17	4

		криптосистемы. Способы создания симметричных криптосистем. Абсолютно стойкий шифр. Криптографическая система DES и еѐ модификации. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.		
8	№ 8	**Принципы построения ассиметричных криптографических систем. Электронная цифровая подпись и еѐ применение.** Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.	№3-19	4
9	№ 9	**Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов.** Классификация вредоносных программ. Основы работы антивирусных программ.	№ 1-19	2
Итого				**34**

4.3. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов	Рекомендуемая литература и методические разработки(№источника из списка литературы)
8 семестр				
1	№1	Угрозы информационной безопасности и каналы утечки информации.	2	№1 - №7
2	№4	Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. Способы несанкционированного доступа к информации в информационных системах и защиты от него.	2	№1 - №5
3	№5	Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.	4	№1 - №6
4	№6	Подсистема безопасности защищенных версий операционной системы Windows. Защита информации от несанкционированного доступа в операционных системах семейства Unix.	3	№1-№4, №6
5	№ 7	Основные понятия криптологии.	2	

		Симметричные и ассиметричные криптосистемы. Криптографическая система DES и еѐ модификации.		
6	№ 8	Принципы построения ассиметричных криптографических систем. Электронная цифровая подпись и еѐ применение. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.	2	
7	№ 9	Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов. Работа с антивирусами. Сравнительный анализ антивирусных программ.	2	
Итого за 8 семестр			**17**	

4.4. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
8 семестр				
1	**Угрозы информационной безопасности и каналы утечки информации.**	5	№1-№6	АКР
2	**Организационно-правовое обеспечение информационной безопасности.**	5	№1, №2, №7	АКР
3	**Инженерно-технические методы и средства защиты информации.**	5	№1, №2, №5	АКР
4	**Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.**	4	№1-№4	АКР

	Способы несанкционированного доступа к информации в информационных системах и защиты от него. Способы аутентификации пользователей.			
5	**Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.**	4	№6	АКР
6	**Подсистема безопасности защищенных версий операционной системы Windows.Защита информации от несанкционированного доступа в операционных системах семейства Unix.**	4	№1-№4	АКР
7	**Основные понятия криптологии. Симметричные и ассиметричные криптосистемы. Способы создания симметричных криптосистем. Абсолютно стойкий шифр.**	4	№1-№4	АКР
8	**Принципы построения ассиметричных криптографических систем. Электронная цифровая подпись и еѐ применение.**	4	№7	АКР
9	**Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов.**	5	№1-7	АКР
Итого за 8 семестр		**40**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать

изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно–методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля

1. Запишите в двоичной системе счисления заданное в десятичной системе число.
2. Что показывает кодовая таблица ЭВМ?
3. Что понимается под байтовым алфавитом?
4. В каком виде существует информация в ЭВМ?
5. По какому правилу текстовая информация превращается в цифровую для ввода в ЭВМ?

Аттестационная контрольная работа №1

1. Организационно-правовое обеспечение информационной безопасности.
2. Понятия «организационная защита информации» и «режим защиты информации».
3. Понятие «система организационной защиты информации»; субъекты и объекты системы.
4. Анализ нормативных документов, регламентирующих основные принципы организации защиты информации.
5. Проблемы защиты информации в автоматизированных системах.
6. Инженерно-технические методы и средства защиты информации.
7. Сущность и задачи комплексной системы защиты информации (КСЗИ).
8. Средства защиты информации в автоматизированных системах
9. Экранирование для защиты информации в АС.

Аттестационная контрольная работа №2

1. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
2. Способы несанкционированного доступа к информации в информационных системах и защиты от него. Способы аутентификации пользователей.
3. Методы и способы защиты информации
4. от несанкционированного доступа. Методы аутентификации. ААА.
5. Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.
6. Идентификация и установление личности. Разграничение доступа пользователей к ресурсам вычислительной системы. Защита ПК на уровне BIOS Средства защиты от несанкционированного доступа в ОС.

Аттестационная контрольная работа №3

1. Подсистема безопасности защищенных версий операционной системы Windows. Защита информации от несанкционированного доступа в операционных системах семейства Unix.
2. Обеспечение безопасности ОС Windows. Понятие защищенной операционной системы
3. Типовая архитектура подсистемы защиты операционной системы Основные функции подсистемы защиты операционной системы.
4. Основные защитные механизмы ос семейства unix
5. Безопасность данных в ОС Unix.
6. Основные понятия криптологии. Симметричные и ассиметричные криптосистемы. Способы создания симметричных криптосистем. Абсолютно стойкий шифр.
7. Криптографическая система DES и еѐ модификации.
8. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.

Вопросы на зачет

1. Организационно-правовое обеспечение информационной безопасности.
2. Понятия «организационная защита информации» и «режим защиты информации».
3. Понятие «система организационной защиты информации»; субъекты и объекты системы.
4. Анализ нормативных документов, регламентирующих основные принципы организации защиты информации.
5. Проблемы защиты информации в автоматизированных системах.
6. Инженерно-технические методы и средства защиты информации.
7. Сущность и задачи комплексной системы защиты информации (КСЗИ).
8. Средства защиты информации в автоматизированных системах
9. Экранирование для защиты информации в АС.
10. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
11. Способы несанкционированного доступа к информации в информационных системах и защиты от него. Способы аутентификации пользователей.
12. Методы и способы защиты информации
13. от несанкционированного доступа. Методы аутентификации. AAA.
14. Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.
15. Идентификация и установление личности. Разграничение доступа пользователей к ресурсам вычислительной системы. Защита ПК на уровне BIOS
    Средства защиты от несанкционированного доступа в ОС.
16. Подсистема безопасности защищенных версий операционной системы Windows. Защита информации от несанкционированного доступа в операционных системах семейства Unix.
17. Обеспечение безопасности ОС Windows. Понятие защищенной операционной системы
18. Типовая архитектура подсистемы защиты операционной системы Основные функции подсистемы защиты операционной системы.
19. Основные защитные механизмы ос семейства unix

20. Безопасность данных в ОС Unix.
21. Основные понятия криптологии. Симметричные и ассиметричные криптосистемы. Способы создания симметричных криптосистем. Абсолютно стойкий шифр.
22. Криптографическая система DES и еѐ модификации.
23. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.
24. Принципы построения ассиметричных криптографических систем. Электронная цифровая подпись и еѐ применение.
25. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.
26. Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов.
27. Классификация вредоносных программ.
28. Основы работы антивирусных программ.

Контрольные вопросы для проверки остаточных знаний.

1. Организационно-правовое обеспечение информационной безопасности.
2. Инженерно-технические методы и средства защиты информации.
3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
4. Способы несанкционированного доступа к информации в информационных системах и защиты от него. Способы аутентификации пользователей.
5. Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах.
6. Подсистема безопасности защищенных версий операционной системы Windows. Защита информации от несанкционированного доступа в операционных системах семейства Unix.
7. Обеспечение безопасности ОС Windows. Понятие защищенной операционной системы
8. Типовая архитектура подсистемы защиты операционной системы Основные функции подсистемы защиты операционной системы.
9. Основные защитные механизмы ос семейства unix
10. Безопасность данных в ОС Unix.
11. Принципы построения ассиметричных криптографических систем. Электронная цифровая подпись и еѐ применение.
12. Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Рекомендуемая литература и источники информации

№	Виды занятий (лк, пз, лб, срс, ирс)	Комплект необходимой учебной литературы по дисциплинам (наименование учебника, учебного пособия, конспект лекций, учебно-методической литературы)	Автор	Издат. и год издания	Кол-во пособий, учебников и прочей литературы	
					в библиотеке	на кафедре
Основная литература						
1.	Лк,лб, срс	Методы и средства инженерно-технической защиты информации. Учебное пособие	Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р.	Брянск: Брянский государственный технический университет, 2012.— 187 с.	http://www.iprbookshop.ru/7000	
2.	Лк,лб, срс	Системы защиты информации в ведущих зарубежных странах. Учебное пособие для вузов	Аверченков В.И	Брянский государственный технический университет, 2012.— 224 с	http://www.iprbookshop.ru/7007	
3.	Лк,лб, срс	Технические средства защиты информации.	Литвинов Р.В.	Томск: Томский государственный университет систем управления и радиоэлектроники, 2006.— 170 с.	http://www.iprbookshop.ru/14027	
4.	Лк,лб, срс	Техники кодирования аудиовизуальной информации. Учебное пособие.	Ермакова А.В.	Саратов: Саратовский государственный технический университет имени Ю.А. Гагарина, ЭБС АСВ, 2012.— 78 с	http://www.iprbookshop.ru/76521.html.	
5.	ЛК,СР, КР	Инженерно-техническая защита информации [Электронный ресурс]	Рагозин Ю. Н.	СПб.: Интермедия, 2018. — 168 с. — 978-5-4383-0161-5.	http://www.iprbookshop.ru/73641.html	

6.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. — 95 с. — 2227-8397	http://www.iprbookshop.ru/17925.html
7.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. — 104 с. — 2227-8397	http://www.iprbookshop.ru/17926.html
8.	ЛК,СР, КР	Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие	Креопалов В. В.	М.: Евразийский открытый институт, 2011. — 278 с. — 978-5-374-00507-3.	http://www.iprbookshop.ru/10871.html
9.	ЛК,СР, КР	Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие	Башлы П. Н.	М.: Евразийский открытый институт, 2012. — 311 с. — 978-5-374-00301-7.	http://www.iprbookshop.ru/10677.html
10.	ЛК,СР, КР	Методы и средства криптографической защиты информации [Электронный ресурс] :	Алексеев В. А.	Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — 2227-8397.	http://www.iprbookshop.ru/17710.html
Дополнительная литература					
11.	Лк,лб, срс	Защита речевой информации от утечки по акустоэлектрическим каналам. Учебное пособие.	Иванов А.В.	Новосибирск: Новосибирский государственный технический университет, 2012.— 43 с.	http://www.iprbookshop.ru/44919
12.	Лк,лб,срс	Защита личной информации в Интернете, смартфоне и компьютере	Камский В.А.	Санкт-Петербург: Наука и Техника, 2017.— 272 с.	http://www.iprbookshop.ru/73046
Интернет - источники					
13.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka/ – образовательный портал университета			

14.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека
15.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

8.Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным основным образовательным программам.

Перечень материально-технического обеспечения, необходимого для реализации программы включает в себя лаборатории и специализированные кабинеты (классы, аудитории), оснащенные лабораторным оборудованием, в зависимости от степени его сложности.

Перечень материально-технического обеспечения включает в себя: лабораторию в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенную средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации;

Компьютерные классы и лаборатории оборудованы современной вычислительной техникой из расчета одно рабочее место па каждого обучаемого при проведении занятий в данных классах (лабораториях), а также комплектом проекционного оборудования для преподавателя.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Программа составлена в соответствии с требованиями ФГОС ВОс учетом рекомендаций и ООП ВО по специальности 38.05.01 – Экономическая безопасностьи специализации «Экономико-правовое обеспечение экономической безопасности».

Рецензент рабочей программы от выпускающей кафедры по специальности 38.05.01 – Экономическая безопасность и специализации «Экономико-правовое обеспечение экономической безопасности»

подпись	к.э.н., доцент должность	/Гирчев В.К./ ФИО