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

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ
Декан, председатель совета
Факультета КТВТиЭ
_____ Ш.А.Юсуфов
16 10 2018

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ Н.С. Суракатов
19 10 2018

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.В.ДВ.4 Информационно-аналитические работы по обеспечению ИБАС

Специальность 10.05.03-«Информационная безопасность автоматизированных систем»

Специализация «Безопасность открытых информационных систем»

Факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, с которым связана специальность

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) специалист по защите информации
название квалификации

Форма обучения очная; курс 5; семестр(ы) 9;

Всего трудоемкость в зачетных единицах (часах) 5 ЗЕТ(180);

Лекции 34 (час); Экзамен 9 (1ЗЕТ=36 ЧАСОВ);

Практические (семинарские) занятия - (час); Зачет - (семестр);

Лабораторные занятия 34 (час); Курсовая работа - (семестр);

Самостоятельная работа 76 (час).

Зав. кафедрой ИБ _____ Г.И. Качаева

Начальник УО _____ О.В.Матюшева

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры ИБ протокол № 2 от 15.10.2018г.

Зав. выпускающей кафедрой по данному направлению _____ **Г.И. Качаева**

ОДОБРЕНО
Методической комиссией по укрупненным группам специальностей и направлению подготовки
10.00.00 Информационная безопасность

Председатель МК

_____
подпись, Ф.И.О

15 10 2018

АВТОР ПРОГРАММЫ

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

_____
подпись

1. Цели освоения дисциплины

1.1 Цели дисциплины

Целью освоения дисциплины является формирование у студентов знаний и умений в области теории и практики информационной безопасности и защиты информации в компьютерных системах.

1.2 Задачи дисциплины

Задачи изучения дисциплины:

- сформировать у студентов знания принципов построения и функционирования пассивных и активных методов защиты информации от несанкционированного доступа с использованием современных информационных технологий в компьютерных системах;
- дать знания основ криптографических методов и средств защиты информации в компьютерных системах;
- раскрыть структуры основных видов безопасности сетевых технологий в компьютерных системах;
- обеспечить приобретение умений и навыков анализа возможных каналов утечки информации как хранящейся в ЭВМ, так и передаваемой по информационным каналам.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Информационно-аналитические работы по обеспечению ИБАС» относится к дисциплинам базовой части. Изучение её базируется на следующих дисциплинах: «Математическая логика и теория алгоритмов», «Методы программирования», «Дискретная математика».

Дисциплина «Информационно-аналитические работы по обеспечению ИБАС» обеспечивает изучение следующих дисциплин: «Основы проектирования защищенных компьютерных сетей», «Защита в операционных системах». Знания и практические навыки, полученные из дисциплины «Криптографические протоколы и стандарты», используются студентами при разработке дипломных работ.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Информационно-аналитические работы по обеспечению ИБАС»

Изучение дисциплины «Информационно-аналитические работы по обеспечению ИБАС» обеспечивает овладение следующими компетенциями:

- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);

В результате изучения дисциплины «Информационно-аналитические работы по обеспечению ИБАС» студенты должны:

знать:

- базовые понятия современных методов оценки безопасности компьютерных систем;
- проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации (ЗИ) в компьютерных системах;
- принципы и способы использования существующих средств ЗИ в компьютерных системах.

- принципы применения современных методов оценки безопасности компьютерных систем;

уметь:

- выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем;
- применять наиболее эффективные методы обеспечения безопасности компьютерных систем;
- применять современные Информационно-аналитические работы по обеспечению ИБАС;

владеть:

- практическими навыками применения методов обеспечения безопасности компьютерных систем;
- навыками применения современных методов оценки безопасности компьютерных систем.

4.

4. Структура и содержание дисциплины (модуля) «Информационно-аналитические работы по обеспечению ИБАС »

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 180 часав, в том числе: лекционных -34 часа, лабораторных - 34 часа, СРС – 76 часов, форма отчетности экзамен в 9 семестре.

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Недели 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	3	4	5	6	7	8	9
1.	**Лекция № 1 Тема: «Введение»** Основные понятия курса. Модель нарушителя. Организационно-правовые вопросы защиты информации.	9	1	2		2	4	Вх. Контр.
2.	**Лекция № 2 Тема: «Защита информации от ПЭМИН»** Каналы утечки информации из компьютерных систем: пассивные и активные методы защиты		2	2		2	4	
3.	**Лекция № 3 Тема: «Основы криптографии»** Понятия и определения: классификация шифров: блочные и поточные шифры.		3	2		2	4	
4.	**Лекция № 4 Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»** Основные понятия теории защиты информации: угрозы безопасности: математические модели политики безопасности: общие критерии безопасности информационных технологий.		4	2		2	4	
5.	**Лекция № 5 Тема: «Специфические особенности защиты информации в компьютерных сетях»** Разделение совместно используемых ресурсов. Расширение зоны контроля. Комбинация различных программно-аппаратных средств. Неизвестный периметр. Множество точек атаки. Сложность управления и контроля доступа к системе. Средства защиты информации от НСД. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах.		5	2		2	4	АКР №1
6.	**Лекция № 6 Тема: «Методы и средства защиты информационно-программного обеспечения на уровне операционных систем»** Классы защищенности СВТ от НСД		6	2		2	4	

	Требования безопасности информации к операционным системам. Профили защиты операционных систем. Разграничение полномочий для групп и учетных записей пользователей. Локальная групповая политика.	9						
7.	**Лекция № 7 Тема: «Применение симметричных криптосистем для защиты компьютерной информации»** Поля Фейстеля: стандарт шифрования данных DES: отечественный стандарт шифрования данных.		7	2		2	4	
8.	**Лекция № 8 Тема: «Технологии идентификации и аутентификации в компьютерных сетях»** Управление доступом. Сервисы безопасности.		8	2		2	4	
9.	**Лекция № 9 Тема: «Методы защиты внешнего периметра компьютерных сетей»** Фильтры пакетов. Шлюзы сеансового уровня. Шлюзы прикладного уровня Межсетевые экраны экспертного уровня Системы обнаружения вторжений. IDS уровня сети. IDS уровня хоста.		9	2		2	4	
10.	**Лекция № 10 Тема: «Безопасность компьютерных систем»** Задачи информационной безопасности. Конфиденциальность, целостность, доступность данных и программ. Понятие политики безопасности.		10	2		2	4	АКР №2
11.	**Лекция № 11 Тема: «Методы обеспечения информационной безопасности»** Криптография. Модели безопасности. Контроль поведения. Программные уязвимости, виды уязвимостей.		11	2		2	6	
12.	**Лекция № 12 Тема: «Эксплуатация уязвимостей»** Инструменты. Информация о процессах в системе.		12	2		2	6	
13.	**Лекция № 13 Тема: «Основы технологии виртуальных защищенных сетей VPN»** Основы технологии виртуальных защищенных сетей VPN. Технологии виртуальных защищенных сетей VPN. Концепция построения виртуальных защищенных сетей VPN. Основные понятие и функции сети VPN. Методы реализации безопасности VPN.		13	2		2	4	
14.	**Лекция № 14 Тема: «Мероприятия по выявлению каналов утечки информации»**	9	14	2		2	4	

	Специальные проверки. Порядок проведения специальной проверки технических средств.						
15.	**Лекция № 15 Тема: «Технологии обнаружения вторжений в компьютерных сетях»** Способ сбора информации. Метод анализа информации. Способ реагирования на угрозы. Требования к IDS. Использование уязвимостей. Тестирование систем IDS.	15	2		2	6	АКР №3
16.	**Лекции № 16 Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»** Аутентификация данных: алгоритмы безопасного хеширования: ЭЦП криптосистем RSA и Эль Гамаля: алгоритм цифровой подписи DSA: отечественные алгоритмы цифрой подписи.	16	2		2	4	
17.	**Лекция № 17 Тема: «Адаптивное управление безопасностью в компьютерных сетях»** Особенности современных подходов к анализу информационной безопасности. Анализ методов функционирования современного Вредоносного программного обеспечения. Способы определения нарушений информационной безопасности. Программно-конфигурируемые сети	17	2		2	6	
	Итого		**34**		**34**	**76**	Экзамен 1 ЗЕТ =36 часов

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	№ литер. источника из списка литературы	Кол-во часов
1.	Лк№1	Модель нарушителя. Организационно-правовые вопросы защиты информации.	№ 1-17	2
2.	Лк№ 2	Защита информации от ПЭМИН. Каналы утечки информации из компьютерных систем: пассивные и активные методы защиты	№ 1-17	2
3.	Лк№ 3	Классификация шифров. Блочные и поточные шифры.	№ 1-17	2
4.	Лк№ 4	Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности.	№ 1-17	2
5.	Лк№ 5	Специфические особенности защиты информации в компьютерных сетях.	№ 1-17	2
6.	Лк№ 6	Методы и средства защиты информационно-программного обеспечения на уровне	№ 1-17	2

		операционных систем.		
7.	Лк№ 7	Применение симметричных криптосистем для защиты компьютерной информации.	№ 1-17	2
8.	Лк№ 8	Технологии идентификации и аутентификации в компьютерных сетях.	№ 1-17	2
9.	Лк№ 9	Методы защиты внешнего периметра компьютерных сетей.	№ 1-17	2
10.	Лк№ 10	Безопасность компьютерных систем.	№ 1-17	2
11.	Лк№ 11	Методы обеспечения информационной безопасности.	№ 1-17	2
12.	Лк№ 12	Эксплуатация уязвимостей	№ 1-17	2
13.	Лк№ 13	Основы технологии виртуальных защищенных сетей VPN.	№ 1-17	2
14.	Лк№ 14	Мероприятия по выявлению каналов утечки информации	№ 1-17	2
15.	Лк№ 15	Технологии обнаружения вторжений в компьютерных сетях.	№ 1-17	2
16.	Лк№ 16	Методы идентификации и аутентификации пользователей компьютерных систем.	№ 1-17	2
17.	Лк№ 17	Адаптивное управление безопасностью в компьютерных сетях.	№ 1-17	2
Итого				**34**

4.3. 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
1.	Основные понятия курса. Модель нарушителя. Организационно-правовые вопросы защиты информации.	4	№ 1-17	Опрос, реферат, статья
2.	Защита информации от ПЭМИН	4	№ 1-17	Опрос, реферат, статья
3.	Основы криптографии	4	№ 1-17	Опрос, реферат, статья
4.	Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности.	4	№ 1-17	Опрос, реферат, статья
5.	Специфические особенности защиты информации в компьютерных сетях.	4	№ 1-17	Опрос, реферат, статья
6.	Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.	4	№ 1-17	Опрос, реферат, статья
7.	Применение симметричных криптосистем для защиты компьютерной информации.	4	№ 1-17	Опрос, реферат, статья

8.	Технологии идентификации и аутентификации в компьютерных сетях.	4	№ 1-17	Опрос, реферат, статья
9.	Методы защиты внешнего периметра компьютерных сетей.	4	№ 1-17	Опрос, реферат, статья
10.	Безопасность компьютерных систем.	4	№ 1-17	Опрос, реферат, статья
11.	Методы обеспечения информационной безопасности .	6	№ 1-17	Опрос, реферат, статья
12.	Эксплуатация уязвимостей.	6	№ 1-17	Опрос, реферат, статья
13.	Основы технологии виртуальных защищенных сетей VPN.	4	№ 1-17	Опрос, реферат, статья
14.	Мероприятия по выявлению каналов утечки информации	4	№ 1-17	Опрос, реферат, статья
15.	Технологии обнаружения вторжений в компьютерных сетях.	6	№ 1-17	Опрос, реферат, статья
16.	Методы идентификации и аутентификации пользователей компьютерных систем	4	№ 1-17	Опрос, реферат, статья
17.	Адаптивное управление безопасностью в компьютерных сетях.	6	№ 1-17	Опрос, реферат, статья
	Итого	**76**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки 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 для проверки знаний студентов

1. Основные положения теории защиты информации.
2. Математическое моделирование в проектировании защищённых телекоммуникационных систем.
3. Классификация угроз безопасности информации в телекоммуникационных системах и их элементах.
4. Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
5. Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
6. Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем.
7. Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов.

Аттестационная контрольная работа №1

1. Основные понятия. Модель нарушителя.
2. Организационно-правовые вопросы защиты информации
3. Защита информации от ПЭМИН.
4. Каналы утечки информации из компьютерных систем.
5. Пассивные и активные методы защиты
6. Основы криптографии.
7. Понятия и определения: классификация шифров.
8. Блочные и поточные шифры.
9. Основы теории защиты информации в компьютерных системах.
10. Критерии информационной безопасности
11. Основные понятия теории защиты информации.
12. Угрозы безопасности: математические модели политики безопасности.
13. Общие критерии безопасности информационных технологий
14. Специфические особенности защиты информации в компьютерных сетях
15. Разделение совместно используемых ресурсов.
16. Расширение зоны контроля.
17. Комбинация различных программно-аппаратных средств.
18. Неизвестный периметр.
19. Множество точек атаки.
20. Сложность управления и контроля доступа к системе.
21. Средства защиты информации от НСД.
22. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах

Аттестационная контрольная работа №2

1. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
2. Классы защищенности СВТ от НСД.
3. Требования безопасности информации к операционным системам.
4. Профили защиты операционных систем.
5. Разграничение полномочий для групп и учетных записей пользователей.
6. Локальная групповая политика.
7. Применение симметричных криптосистем для защиты компьютерной информации.

8. Поля Фейстеля: стандарт шифрования данных DES.
9. Отечественный стандарт шифрования данных.
10. Технологии идентификации и аутентификации в компьютерных сетях.
11. Идентификация и аутентификация.
12. Управление доступом.
13. Сервисы безопасности.
14. Методы защиты внешнего периметра компьютерных сетей.
15. Фильтры пакетов.
16. Шлюзы сеансового уровня.
17. Шлюзы прикладного уровня.
18. Межсетевые экраны экспертного уровня.
19. Системы обнаружения вторжений.
20. IDS уровня сети.
21. IDS уровня хоста.

Аттестационная контрольная работа №3

1. Безопасность компьютерных систем
2. Задачи информационной безопасности.
3. Конфиденциальность, целостность, доступность данных и программ.
4. Понятие политики безопасности.
5. Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
6. Программные уязвимости, виды уязвимостей.
7. Эксплуатация уязвимостей.
8. Инструменты.
9. Информация о процессах в системе.
10. Основы технологии виртуальных защищенных сетей VPN.
11. Технологии виртуальных защищенных сетей VPN.
12. Концепция построения виртуальных защищенных сетей VPN.
13. Основные понятие и функции сети VPN.
14. Методы реализации безопасности VPN.
15. Мероприятия по выявлению каналов утечки информации. Специальные проверки. Порядок проведения специальной проверки технических средств.

Перечень экзаменационных вопросов

1. Основные понятия. Модель нарушителя.
2. Организационно-правовые вопросы защиты информации
3. Защита информации от ПЭМИН.
4. Каналы утечки информации из компьютерных систем.
5. Пассивные и активные методы защиты
6. Основы криптографии.
7. Понятия и определения: классификация шифров.
8. Блочные и поточные шифры.
9. Основы теории защиты информации в компьютерных системах.
10. Критерии информационной безопасности
11. Основные понятия теории защиты информации.
12. Угрозы безопасности: математические модели политики безопасности.
13. Общие критерии безопасности информационных технологий
14. Специфические особенности защиты информации в компьютерных сетях
15. Разделение совместно используемых ресурсов.
16. Расширение зоны контроля.
17. Комбинация различных программно-аппаратных средств.

18. Неизвестный периметр.
19. Множество точек атаки.
20. Сложность управления и контроля доступа к системе.
21. Средства защиты информации от НСД.
22. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах
23. Безопасность компьютерных систем
24. Задачи информационной безопасности.
25. Конфиденциальность, целостность, доступность данных и программ.
26. Понятие политики безопасности.
27. Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
28. Программные уязвимости, виды уязвимостей.
29. Эксплуатация уязвимостей.
30. Инструменты.
31. Информация о процессах в системе.
32. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
33. Классы защищенности СВТ от НСД.
34. Требования безопасности информации к операционным системам.
35. Профили защиты операционных систем.
36. Разграничение полномочий для групп и учетных записей пользователей.
37. Локальная групповая политика.
38. Применение симметричных криптосистем для защиты компьютерной информации.
39. Поля Фейстеля: стандарт шифрования данных DES.
40. Отечественный стандарт шифрования данных.
41. Технологии идентификации и аутентификации в компьютерных сетях.
42. идентификация и аутентификация
43. Управление доступом.
44. Сервисы безопасности.
45. Методы защиты внешнего периметра компьютерных сетей.
46. Фильтры пакетов.
47. Шлюзы сеансового уровня.
48. Шлюзы прикладного уровня.
49. Межсетевые экраны экспертного уровня.
50. Системы обнаружения вторжений.
51. IDS уровня сети.
52. IDS уровня хоста.
53. Основы технологии виртуальных защищенных сетей VPN.
54. Технологии виртуальных защищенных сетей VPN.
55. Концепция построения виртуальных защищенных сетей VPN.
56. Основные понятие и функции сети VPN.
57. Методы реализации безопасности VPN.
58. Мероприятия по выявлению каналов утечки информации
59. Специальные проверки. Порядок проведения специальной проверки технических средств.
60. Технологии обнаружения вторжений в компьютерных сетях.
61. Способ сбора информации.
62. Метод анализа информации.
63. Способ реагирования на угрозы.
64. Требования к IDS.
65. Использование уязвимостей.
66. Тестирование систем IDS.

67. Методы идентификации и аутентификации пользователей компьютерных систем.
68. Аутентификация данных.
69. Алгоритмы безопасного хеширования.
70. ЭЦП криптосистем RSA и Эль Гамаля.
71. Алгоритм цифровой подписи DSA; отечественные алгоритмы цифрой подписи.
72. Адаптивное управление безопасностью в компьютерных сетях.
73. Особенности современных подходов к анализу информационной безопасности.
74. Анализ методов функционирования современного Вредоносного программного обеспечения.
75. Способы определения нарушений информационной безопасности.

Вопросы проверки остаточных знаний

1. Основные понятия. Модель нарушителя.
2. Безопасность компьютерных систем.
3. Методы обеспечения информационной безопасности.
4. Основные понятия теории защиты информации.
5. Сложность управления и контроля доступа к системе.
6. Средства защиты информации от НСД.
7. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах
8. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.
9. Классы защищенности СВТ от НСД.
10. Сервисы безопасности.
11. Методы защиты внешнего периметра компьютерных сетей.
12. Мероприятия по выявлению каналов утечки информации.
13. Алгоритм цифровой подписи DSA; отечественные алгоритмы цифрой подписи.
14. Адаптивное управление безопасностью в компьютерных сетях.
15. Особенности современных подходов к анализу информационной безопасности.
16. Анализ методов функционирования современного Вредоносного программного обеспечения.
17. Способы определения нарушений информационной безопасности.

7. Учебно-методическое и информационное обеспечение дисциплины «Информационно-аналитические работы по обеспечению ИБАС»

7.1. Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой

№	Виды занятий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк. лб. срс	Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем	В. А. Заляжных, А. В. Гирик	Санкт-Петербург: Университет ИТМО, 2014. – 139 с. — ISBN 2227-8397	http://www.iprbookshop.ru/65733.html	
2.	Лк. лб. срс	Защита информации в компьютерных системах.	Мельников В.В.	Финансы и статистика, 2014 368.	http://www.iprbookshop.ru/61558	
3.	Лк. пр. срс	Защита информации в компьютерных системах и сетях.	Романец Ю.В.	М.: Радио и связь, 2001. — 328 с.	http://www.iprbookshop.ru/29257	
4.	Лк. пр. срс	Криптографические методы защиты информации в компьютерных системах и сетях.	Иванов М.А.	Электрон. текстовые дан. 2001 г. «Кудиц-образ», 386с Москва :	http://www.iprbookshop.ru/24451	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
5.	Лк. лб. срс	Средства вычислительной техники		Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992	http://www.iprbookshop.ru/73733.html	
6.	Лк. лб. срс	Защита информации в автоматизированных системах обработки данных	Герасименко В. А.	М.: Энергоатомиздат, 2016	http://www.iprbookshop.ru/426 3215	
7.	Лк, лб, срс	Вероятностные методы оценки состояния информационной безопасности: учебное пособие	Н. Н. Червяков, М. Г. Бабенко, А. В. Галкин	Ставрополь: Северо-Кавказский федеральный университет, 2017. – 182 с. – ISBN 2227-8397	http://www.iprbookshop.ru/92536.html	
ИНТЕРНЕТ РЕСУРСЫ						

8.	ЛЗ,ЛБ, СРС	http: www.edu.ru - веб-сайт системы федеральных образовательных порталов
9.	ЛЗ,ЛБ, СРС	http: www.sec.ru - каталог организаций в сфере информационной безопасности
10.	ЛЗ,ЛБ, СРС	базы данных, информационно-справочные и поисковые системы: правовые справочно-поисковые системы «Гарант», «Консультант Плюс»). www.fstec.ru;www.gost.ru/wps/portal/tk362.

8.Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий и лабораторного практикума на основе интерактивных методов обучения необходим доступ в Интернет из компьютерного зала, наличие цифрового проектора для применения современных обучающих мультимедиа – технологий.

Программное обеспечение:

- операционная система Microsoft Windows;
- текстовый процессор Microsoft Word;
- web-браузер;
- среда программирования.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

Рецензент от выпускающей кафедры по специальности 10.05.03- «Информационная безопасность автоматизированных систем

подпись З.Р. Рагимова ФИО

Дополнения и изменения в рабочей программе
на 20 учебный год