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

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ
Декан, председатель совета
Факультета КТВТиЭ
_____ Ш.А.Юсуфов
18 10 2018

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ Н.С. Суракатов
21 10 2018

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.Б.32 Программно-аппаратные средства защиты информации
наименование дисциплины по ООП и код по ФГОС

Направлению 10.03.01- «Информационная безопасность
шифр и полное наименование направления

Профиль «Безопасность автоматизированных систем»

Факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, где ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) бакалавр
бакалавр (специалист)

Форма обучения очная, курс 3,4 семестр (ы) 6,7
очная, заочная, др.

Всего трудоемкость в зачетных единицах (часах) 8ЗЕТ (288 часа):
лекции 68 (час); экзамен 6,7 (2 зет=72 часа);
(семестр)

практические (семинарские) занятия - (час); зачет 1
(семестр)

лабораторные занятия 68 (час); самостоятельная работа 80 (час);

курсовой проект (работа, РГР)-(семестр)

Зав. кафедрой ИБ _____ Г.И. Качаева

Начальник УО _____ Э.В.Магомаева

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных 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

_____ Мещеряков В.Б
подпись, И.О.Ф.

15.10 2018

АВТОР ПРОГРАММЫ

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

_____
подпись

1. **Цели освоения дисциплины**

Дисциплина «Программно-аппаратные средства защиты информации» имеет целью ознакомление слушателей существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Задача дисциплины «Криптографические протоколы» – получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

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

Дисциплина «Программно-аппаратные средства защиты информации» относится к дисциплинам по выбору вариативной части. Изучение её базируется на следующих дисциплинах: «Математическая логика и теория алгоритмов», «Методы программирования», «Дискретная математика».

Дисциплина «Криптографические протоколы» обеспечивает изучение следующих дисциплин: «Основы проектирования защищенных компьютерных сетей», «Защита в операционных системах». Знания и практические навыки, полученные из дисциплины «Программно-аппаратные средства защиты информации», используются студентами при разработке курсовых и дипломных работ.

3. **Компетенции обучающегося, формируемые в результате освоения дисциплины «Программно-аппаратные средства защиты информации»**

Изучение дисциплины «Программно-аппаратные средства защиты информации» обеспечивает овладение следующими компетенциями:

- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);
- способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1).

В результате изучения дисциплины «Программно-аппаратные средства защиты информации» студенты должны:

знать:

- формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;
- криптографические стандарты;
- типовые криптографические протоколы и основные требования к ним;
- принципы построения криптографических хеш-функций;
- основные схемы цифровой подписи;
- протоколы идентификации;
- протоколы передачи и распределения ключей;

уметь:

- использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов;
- формулировать свойства безопасности криптографических протоколов;

- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;

владеть:

- криптографической терминологией;
- простейшими подходами к анализу безопасности криптографических протоколов.

4. Структура и содержание дисциплины (модуля) «Программно-аппаратные средства защиты информации»

Общая трудоемкость дисциплины составляет 8 зачетных единиц – 288 часов, в том числе: лекционных -68 часов, лабораторных - 68 часа, СРС – 80 часов, форма отчетности экзамены в 6 и 7 семестрах.

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 успеваемости *(по срокам текущих аттестаций в семестре)*
				ЛК	ПЗ	ЛР	СР	
1.	**Лекция № 1** Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности. Цели и задачи программно-аппаратной защиты информации. Место программно-аппаратной (ПА) защиты информации в системе комплексной защиты информации на объектах информатизации. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации. Классификация методов и средств ПА защиты информации	6	1	2		2	2	Вх. Контр.
2.	**Лекция № 2** Службы защиты информации: обеспечение, аутентичность субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации и т.д. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.		2	2		2	2	
3.	**Лекция №3** Принципы программно-аппаратной защиты информации от несанкционированного доступа.		3	2		2	2	
4.	**Лекция № 4** Основные подходы к ПА защите данных от несанкционированного доступа (НСД). Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам.		4	2		2	2	
5.	**Лекция № 5** Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта.		5	2		2	2	АКР №1
6.	**Лекция № 6** Разграничение и контроль доступа к информации. Защита сетевого файлового ресурса, фиксация		6	2		2	2	

	доступа к файлам, доступ к данным со стороны процесса. Способы фиксации факта доступа. Контроль и управление доступом средствами операционной системы. Система SecretNet 6.0. Надежность систем ограничения доступа.							
7.	**Лекция № 7** Построение аппаратных компонент криптозащиты данных. Защита файлов от изменения. Электронная цифровая подпись.	7	2		2	2		
8.	**Лекция № 8** Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратных средств криптозащиты.	8	2		2	2		
9.	**Лекция № 9** Программно-аппаратные методы и средства ограничения доступа к компонентам инфокоммуникационных систем. Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа.	9	2		2	2		
10.	**Лекция № 10** Средства защиты программного обеспечения от несанкционированной загрузки. ПА защита программ от несанкционированного копирования, пароли и ключи.	10	2		2	2	АКР №2	
11.	**Лекция № 11** Организация хранения ключей. Защита программ от излучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям. Защита информации на машинных носителях. Защита остатков информации	11	2		2	2		
12.	**Лекция № 12** Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня.	12	2		2	2		
13.	**Лекция № 13** Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.	13	2		2	2		
14.	**Лекция № 14** Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник.	14	2		2	2		

	Электронная почта и документооборот.							
15.	**Лекция № 15** Web-приложения. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC). Управление ключами.	6	15	2		2	4	АКР №3
16.	**Лекция № 16** Компьютерные вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.		16	2		2	4	
17.	**Лекция № 17** Основные направления и перспективы развития методов и средств ПА защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи. Современные системы ПА защиты информации на объектах информатизации. Возможности современных ПА средств защиты.		17	2		2	4	
	Итого за 7 семестр			**34**		**34**	**40**	**Экзамен (1 зет=36 час)**
1.	**Лекция № 1** Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы	7	1	2		2	2	Вх. КР
2.	**Лекция № 2** Программное обеспечение для моделирования сетей передачи данных.		2	2		2	2	
3.	**Лекция № 3** Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.		3	2		2	2	
4.	**Лекция № 4** Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.		4	2		2	2	
5.	**Лекция № 5** Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.		5	2		2	2	АКР №1
6.	**Лекция № 6** Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга. Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных.		6	2		2	2	
7.	**Лекция №7** Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга.		7	2		2	2	

	Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных							
8.	**Лекция № 8** Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика.		8	2		2	2	
9.	**Лекция №9** Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика.		9	2		2	2	
10.	**Лекция № 10** Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.		10	2		2	2	АКР №2
11.	**Лекция № 11** Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.		11	2		2	2	
12.	**Лекция № 12** Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.	7	12	2		2	4	
13.	**Лекция № 13** Основы работы в ОС семейства Linux. Управление правами доступа. Администрирование пользователей. Управление файлами и каталогами. Ссылки. Архивирование и резервное копирование системы. Восстановление системы после критических сбоев из архивов.		13	2		2	4	
14.	**Лекция № 14** Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.		14	2		2	2	
15.	**Лекция № 15** Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.		15	2		2	2	АКР №3
16.	**Лекция № 16** Административные меры обеспечения комплексной безопасности в информационных системах.		16	2		2	2	

17.	**Лекция № 17** Перспективные технологии обеспечения безопасности информации в информационных технологиях.	7	14	2		2	4	
	Итого за 7 семестр			**34**		**34**	**40**	**Экзамен (1 зет=36 час)**
	Итого по дисциплине			**68**		**68**	**80**	

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	Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности.	№1-11	2
2	Лк№2	Службы защиты информации: обеспечение, аутентичность субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации.	№1-11	2
3	Лк№ 2	Принципы программно-аппаратной защиты информации от несанкционированного доступа.	№1-11	2
4	Лк№ 3	Основные подходы к ПА защите данных от несанкционированного доступа (НСД). Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам.	№1-11	2
5	Лк№4 и5	Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта.	№1-11	2
6	Лк№ 5	Разграничение и контроль доступа к информации. Защита сетевого файлового ресурса, фиксация доступа к файлам, доступ к данным со стороны процесса. Способы фиксации факта доступа. Контроль и управление доступом средствами операционной системы. Система SecretNet 6.0. Надежность систем ограничения доступа.	№1-11	2
7	Лк№ 6,7	Построение аппаратных компонент криптозащиты данных. Защита файлов от изменения. Электронная цифровая подпись.	№1-11	2
8	Лк№ 7,8	Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратных средств криптозащиты.	№1-11	2
9	Лк№ 9	Программно-аппаратные методы и средства ограничения доступа к компонентам инфокоммуникационных систем.	№1-11	2

		Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа.		
10	Лк№10	Средства защиты программного обеспечения от несанкционированной загрузки. ПА защита программ от несанкционированного копирования, пароли и ключи.	№1-11	2
11	Лк№ 11	Организация хранения ключей. Защита программ от излучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям. Защита информации на машинных носителях. Защита остатков информации	№1-11	2
12	Лк№ 12	Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня.	№1-11	2
13	Лк№ 13	Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.	№1-11	2
14	Лк№ 14	Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник. Электронная почта и документооборот.	№1-11	2
15	Лк№ 15	Web-приложения. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC). Управление ключами.	№1-11	2
16	Лк№ 16	Компьютерные вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.	№1-11	2
17	Лк№ 17	Основные направления и перспективы развития методов и средств ПА защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи. Современные системы ПА защиты информации на объектах информатизации. Возможности современных ПА средств защиты.	№1-11	2
Итого за 6 семестр				**34**
18	Лк№ 1	Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы	№1-11	2
19	Лк№ 2	Программное обеспечение для моделирования сетей передачи данных.	№1-11	2
20	Лк№ 3	Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.	№1-11	2

21	Лк№ 4	Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.	№1-11	2
22	Лк№ 5	Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.	№1-11	2
23	Лк№ 6	Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга. Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных.	№1-11	2
24	Лк№ 7	Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга. Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных	№1-11	2
25	Лк№ 8	Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика.	№1-11	2
26	Лк№ 9	Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика.	№1-11	2
27	Лк№ 10	Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.	№1-11	2
28	Лк№ 11	Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.	№1-11	2
29	Лк№ 12	Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.	№1-11	2
30	Лк№ 13	Основы работы в ОС семейства Linux. Управление правами доступа. Администрирование пользователей. Управление файлами и каталогами. Ссылки. Архивирование и резервное копирование системы. Восстановление системы после критических сбоев из архивов.	№1-11	2
31	Лк№ 14	Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.	№1-11	2
32	Лк№ 15	Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.	№1-11	2
33	Лк№ 16	Административные меры обеспечения комплексной	№1-11	2

		безопасности в информационных системах.		
34	Лк№ 17	Перспективные технологии обеспечения безопасности информации в информационных технологиях.	№1-11	2
Итого за 7 семестр				**34**
Итого по дисциплине				**68**

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	Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности.	2	№1-11	Опрос, реферат, статья
2	Службы защиты информации: обеспечение, аутентичность субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации.	2	№1-11	Опрос, реферат, статья
3	Принципы программно-аппаратной защиты информации от несанкционированного доступа.	2	№1-11	Опрос, реферат, статья
4	Основные подходы к ПА защите данных от несанкционированного доступа (НСД). Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам.	2	№1-11	Опрос, реферат, статья
5	Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта.	2	№1-11	Опрос, реферат, статья
6	Разграничение и контроль доступа к информации. Защита сетевого файлового ресурса, фиксация доступа к файлам, доступ к данным со стороны процесса. Способы фиксации факта доступа. Контроль и управление доступом средствами операционной системы. Система SecretNet 6.0. Надежность систем ограничения доступа.	2	№1-11	Опрос, реферат, статья
7	Построение аппаратных компонент криптозащиты данных. Защита файлов от изменения. Электронная цифровая подпись.	2	№1-11	Опрос, реферат, статья
8	Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратных средств криптозащиты.	2	№1-11	Опрос, реферат, статья

9	Программно-аппаратные методы и средства ограничения доступа к компонентам инфокоммуникационных систем. Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа.	2	№1-11	Опрос, реферат, статья
10	Средства защиты программного обеспечения от несанкционированной загрузки. ПА защита программ от несанкционированного копирования, пароли и ключи.	2	№1-11	Опрос, реферат, статья
11	Организация хранения ключей. Защита программ от излучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям. Защита информации на машинных носителях. Защита остатков информации	2	№1-11	Опрос, реферат, статья
12	Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня.	2	№1-11	Опрос, реферат, статья
13	Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.	2	№1-11	Опрос, реферат, статья
14	Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Компоненты ИОК и их функции. Центр Сертификации. Центр Регистрации. Конечные пользователи. Сетевой справочник. Электронная почта и документооборот.	2	№1-11	Опрос, реферат, статья
15	Web-приложения. Стандарты в области ИОК. Стандарты PKIX. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC). Управление ключами.	4	№1-11	Опрос, реферат, статья
16	Компьютерные вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.	4	№1-11	Опрос, реферат, статья
17	Основные направления и перспективы развития методов и средств ПА защиты информации и управления правами использования информационных ресурсов при передаче	4	№1-11	Опрос, реферат, статья

	конфиденциальной информации по каналам связи. Современные системы ПА защиты информации на объектах информатизации. Возможности современных ПА средств защиты.			
Итого за 6 семестр		**40**		
1	Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы	2	№1-11	Опрос, реферат, статья
2	Программное обеспечение для моделирования сетей передачи данных.	2	№1-11	Опрос, реферат, статья
3	Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.	2	№1-11	Опрос, реферат, статья
4	Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.	2	№1-11	Опрос, реферат, статья
5	Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.	2	№1-11	Опрос, реферат, статья
6	Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга. Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных.	2	№1-11	Опрос, реферат, статья
7	Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга. Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных	2	№1-11	Опрос, реферат, статья
8	Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика.	2	№1-11	Опрос, реферат, статья
9	Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика.	2	№1-11	Опрос, реферат, статья
10	Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.	2	№1-11	Опрос, реферат, статья
11	Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие	2	№1-11	Опрос, реферат,

	принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.			статья
12	Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.	4	№1-11	Опрос, реферат, статья
13	Основы работы в ОС семейства Linux. Управление правами доступа. Администрирование пользователей. Управление файлами и каталогами. Ссылки. Архивирование и резервное копирование системы. Восстановление системы после критических сбоев из архивов.	4	№1-11	Опрос, реферат, статья
14	Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.	2	№1-11	Опрос, реферат, статья
15	Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.	2	№1-11	Опрос, реферат, статья
16	Административные меры обеспечения комплексной безопасности в информационных системах.	2	№1-11	Опрос, реферат, статья
17	Перспективные технологии обеспечения безопасности информации в информационных технологиях.	4	№1-11	Опрос, реферат, статья
Итого за 7 семестр		**40**		
Итого по дисциплине		**80**		

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 6 семестр

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

Контрольные вопросы для проверки текущих знаний студентов
Аттестационная контрольная работа №1

1. Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности.
2. Цели и задачи программно-аппаратной защиты информации.
3. Место программно-аппаратной (ПА) защиты информации в системе комплексной защиты информации на объектах информатизации.
4. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации.
5. Классификация методов и средств ПА защиты информации
6. Службы защиты информации: обеспечение, аутентичность субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации и т.д.
7. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
8. Принципы программно-аппаратной защиты информации от
9. несанкционированного доступа.
10. Основные подходы к ПА защите данных от несанкционированного доступа (НСД).
11. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам.
12. Идентификация, аутентификация и авторизация.
13. Аутентификация субъекта.
14. Парольные схемы защиты.
15. Симметричные методы аутентификации.
16. Несимметричные методы аутентификации субъекта.
17. Аутентификация объекта.

Аттестационная контрольная работа №2

1. Разграничение и контроль доступа к информации.
2. Защита сетевого файлового ресурса, фиксация доступа к файлам, доступ к данным со стороны процесса.
3. Способы фиксации факта доступа.
4. Контроль и управление доступом средствами операционной системы.
5. Система SecretNet 6.0. Надежность систем ограничения доступа.
6. Построение аппаратных компонент криптозащиты данных.
7. Защита файлов от изменения. Электронная цифровая подпись.
8. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.
9. Необходимые и достаточные функции аппаратных средств криптозащиты.

18. Программно-аппаратные методы и средства ограничения доступа к компонентам инфокоммуникационных систем.
19. Дискреционный метод организации разграничения доступа.
20. Мандатный метод организации разграничения доступа.
21. Средства защиты программного обеспечения от несанкционированной загрузки.
22. ПА защита программ от несанкционированного копирования, пароли и ключи.

Аттестационная контрольная работа №3

1. Организация хранения ключей.
2. Защита программ от излучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям.
3. Защита информации на машинных носителях.
4. Защита остатков информации.
5. Классификация способов несанкционированного доступа и жизненный цикл атак.
6. Способы противодействия несанкционированному межсетевому доступу.
7. Функции межсетевого экранирования.
8. Особенности межсетевого экранирования на различных уровнях модели OSI.
9. Режим функционирования межсетевых экранов и их основные компоненты.
23. Маршрутизаторы.
24. Шлюзы сетевого уровня.
25. Основные схемы сетевой защиты на базе межсетевых экранов.
26. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов.
27. Построение защищенных виртуальных сетей.
28. Способы создания защищенных виртуальных каналов.
29. Обзор протоколов. Инфраструктура на основе криптографии с открытыми ключами (ИОК).
30. Цифровые сертификаты.
31. Управление цифровыми сертификатами.
32. Компоненты ИОК и их функции. Центр Сертификации.
33. Центр Регистрации. Конечные пользователи. Сетевой справочник.
34. Электронная почта и документооборот. Web-приложения.
35. Стандарты в области ИОК. Стандарты PKIX.
36. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
37. Управление ключами.

Перечень вопросов на экзамен

1. Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности.
2. Цели и задачи программно-аппаратной защиты информации.
3. Место программно-аппаратной (ПА) защиты информации в системе комплексной защиты информации на объектах информатизации.
4. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации.
5. Классификация методов и средств ПА защиты информации
6. Службы защиты информации: обеспечение, аутентичность субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации и т.д.
7. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
8. Принципы программно-аппаратной защиты информации от
9. несанкционированного доступа.
10. Основные подходы к ПА защите данных от несанкционированного доступа (НСД).
11. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам.

12. Идентификация, аутентификация и авторизация.
13. Аутентификация субъекта.
14. Парольные схемы защиты.
15. Симметричные методы аутентификации.
16. Несимметричные методы аутентификации субъекта.
17. Аутентификация объекта.
18. Разграничение и контроль доступа к информации.
19. Защита сетевого файлового ресурса, фиксация доступа к файлам, доступ к данным со стороны процесса.
20. Способы фиксации факта доступа.
21. Контроль и управление доступом средствами операционной системы.
22. Система SecretNet 6.0. Надежность систем ограничения доступа.
23. Построение аппаратных компонент криптозащиты данных.
24. Защита файлов от изменения. Электронная цифровая подпись.
25. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.
26. Необходимые и достаточные функции аппаратных средств криптозащиты.
27. Программно-аппаратные методы и средства ограничения доступа к компонентам инфокоммуникационных систем.
28. Дискреционный метод организации разграничения доступа.
29. Мандатный метод организации разграничения доступа.
30. Средства защиты программного обеспечения от несанкционированной загрузки.
31. ПА защита программ от несанкционированного копирования, пароли и ключи.
32. Организация хранения ключей.
33. Защита программ от излучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям.
34. Защита информации на машинных носителях.
35. Защита остатков информации.
36. Классификация способов несанкционированного доступа и жизненный цикл атак.
37. Способы противодействия несанкционированному межсетевому доступу.
38. Функции межсетевого экранирования.
39. Особенности межсетевого экранирования на различных уровнях модели OSI.
40. Режим функционирования межсетевых экранов и их основные компоненты.
41. Маршрутизаторы.
42. Шлюзы сетевого уровня.
43. Основные схемы сетевой защиты на базе межсетевых экранов.
44. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Критерии оценки межсетевых экранов.
45. Построение защищенных виртуальных сетей.
46. Способы создания защищенных виртуальных каналов.
47. Обзор протоколов. Инфраструктура на основе криптографии с открытыми ключами (ИОК).
48. Цифровые сертификаты.
49. Управление цифровыми сертификатами.
50. Компоненты ИОК и их функции. Центр Сертификации.
51. Центр Регистрации. Конечные пользователи. Сетевой справочник.
52. Электронная почта и документооборот. Web-приложения.
53. Стандарты в области ИОК. Стандарты PKIX.
54. Стандарты, основанные на ИОК (S/MIME, SSL и TLS, SET, IPSEC).
55. Управление ключами.
56. Компьютерные вирусы как особый класс разрушающих программных воздействий.
57. Необходимые и достаточные условия недопущения разрушающего воздействия.
58. Понятие изолированной программной среды.

59. Основные направления и перспективы развития методов и средств ПА защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи.
60. Современные системы ПА защиты информации на объектах информатизации.
61. Возможности современных ПА средств защиты

Вопросы входного контроля для проверки знаний студентов 7 семестр

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

Контрольные вопросы для проверки текущих знаний студентов

Аттестационная контрольная работа №1

1. Программное обеспечение для моделирования сетей передачи данных.
2. Эмулятор GNS3.
3. Основы работы и моделирование простых схем.
4. Протоколы удаленного доступа. Протоколы telnet, ssh.
5. Обеспечение безопасности при передаче данных по сети.
6. Сравнительный анализ.
7. Протокол настройки времени.
8. Динамическая IP-маршрутизация.
9. Внутренние протоколы маршрутизации.
10. Пограничный шлюзовой протокол маршрутизации.
11. Протоколы RIP, IGRP и EIGRP.
12. Протокол динамической маршрутизации OSPF.
13. Атака типа «Отказ в обслуживании» (DoS-атака).
14. Механизмы защиты от некоторых типов DoS-атак.
15. Антиспуфинг. Защита от IP-спуфинга.
16. Защита от ARP-спуфинга.
17. Защита внутреннего периметра сети передачи данных.

Аттестационная контрольная работа №2

1. Атака типа «Отказ в обслуживании» (DoS-атака).
2. Механизмы защиты от некоторых типов DoS-атак.
3. Антиспуфинг.
4. Защита от IP-спуфинга.
5. Защита от ARP-спуфинга.
6. Защита внутреннего периметра сети передачи данных
7. Сегментация сетей п-ередачи данных.
8. Технология VLAN.
9. Передача трафика между VLAN.
10. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней.
11. Технологии VTP-сервер и Port-security.
12. Фильтрация трафика.
13. Изучение технологии ACL (AccessControlList).
14. Типы ACL.
15. Создание списков доступа.
16. Общие принципы VirtualPrivateNetwork (VPN).

17. Сравнительный анализ протоколов VPN.
18. Настройка VPN соединения через протокол GRE.
19. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
20. Применение SSLVPN
21. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.

Аттестационная контрольная работа №3

1. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
2. Применение SSLVPN
3. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.
4. Основы работы в ОС семейства Linux.
5. Управление правами доступа.
6. Администрирование пользователей.
7. Управление файлами и каталогами.
8. Ссылки.
9. Архивирование и резервное копирование системы.
10. Восстановление системы после критических сбоев из архивов.
11. Администрирование БД MSSQL.
12. Управление правами доступа.
13. Архивирование и восстановление БД.
14. Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных.
15. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.
16. Административные меры обеспечения комплексной безопасности в информационных системах

Перечень вопросов на экзамен

1. Программное обеспечение для моделирования сетей передачи данных.
2. Эмулятор GNS3.
3. Основы работы и моделирование простых схем.
4. Протоколы удаленного доступа. Протоколы telnet, ssh.
5. Обеспечение безопасности при передаче данных по сети.
6. Сравнительный анализ.
7. Протокол настройки времени.
8. Динамическая IP-маршрутизация.
9. Внутренние протоколы маршрутизации.
10. Пограничный шлюзовой протокол маршрутизации.
11. Протоколы RIP, IGRP и EIGRP.
12. Протокол динамической маршрутизации OSPF.
13. Атака типа «Отказ в обслуживании» (DoS-атака).
14. Механизмы защиты от некоторых типов DoS-атак.
15. Антиспуфинг. Защита от IP-спуфинга.
16. Защита от ARP-спуфинга.
17. Защита внутреннего периметра сети передачи данных.
18. Атака типа «Отказ в обслуживании» (DoS-атака).
19. Механизмы защиты от некоторых типов DoS-атак.
20. Антиспуфинг.
21. Защита от IP-спуфинга.
22. Защита от ARP-спуфинга.
23. Защита внутреннего периметра сети передачи данных
24. Сегментация сетей передачи данных.
25. Технология VLAN.

26. Передача трафика между VLAN.
27. Маршрутизация трафика между VLAN на основе коммутаторов 2- го и 3-го уровней.
28. Технологии VTP-сервер и Port-security.
29. Фильтрация трафика.
30. Изучение технологии ACL (AccessControlList).
31. Типы ACL.
32. Создание списков доступа.
33. Общие принципы VirtualPrivateNetwork (VPN).
34. Сравнительный анализ протоколов VPN.
35. Настройка VPN соединения через протокол GRE.
36. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
37. Применение SSLVPN
38. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.
39. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
40. Применение SSLVPN
41. Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.
42. Основы работы в ОС семейства Linux.
43. Управление правами доступа.
44. Администрирование пользователей.
45. Управление файлами и каталогами.
46. Ссылки.
47. Архивирование и резервное копирование системы.
48. Восстановление системы после критических сбоев из архивов.
49. Администрирование БД MSSQL.
50. Управление правами доступа.
51. Архивирование и восстановление БД.
52. Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных.
53. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.
54. Административные меры обеспечения комплексной безопасности в информационных системах.

.

Вопросы проверки остаточных знаний

1. Угрозы безопасности компьютерных систем.
2. Противодействие угрозам безопасности.
3. Защита компьютерной системы от взлома.
4. Модель КС.
5. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.
6. Реализация механизмов безопасности на аппаратном уровне Безопасность компьютерной сети.
7. Защита от анализаторов протоколов.
8. Технология защиты информации на основе смарт-карт.
9. Состав комплекса «Аккорд».
10. Принцип работы комплекса «Аккорд».
11. Механизм замкнутой программной среды Secret Net.

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

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

Зав. библиотекой _____

№	Виды заня-тий (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	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс]: учебно-методическое пособие	Фомин Д.В.	Саратов: Вузовское образование, 2018.— 218 c.	http://www.iprbookshop.ru/77317.html	
2.	Лк, пр, срс	Информационная безопасность и защита информации	Шаньгин, В. Ф.	Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс]: учебно-методическое пособие	Помешкин А.А., Коротких И.В.	Новосибирск: Новосибирский государственный технический университет, 2012.— 47 c	http://www.iprbookshop.ru/45015.html	
4.	Лк, пр, срс	Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие	Прокушев Я.Е.	Санкт-Петербург: Интермедия, 2017.— 160 c.	http://www.iprbookshop.ru/66799.html	
5.	Лк, пр, срс	Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность»	Л.Х. Мифтахова [и др.].	Санкт-Петербург: Интермедия, 2018.— 408 c.	http://www.iprbookshop.ru/73644.html	
6.	Лк, пр, срс	Программно-аппаратные средства защиты информационных систем [Электронный ресурс]: учебное пособие	Ю.Ю. Громов [и др.].	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017.— 193 c.	http://www.iprbookshop.ru/85968.html	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
7.	Лк, лб, срс	Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание	А.И. Астайкин [и др.]	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015.— 224 c.	http://www.iprbookshop.ru/60959.html.	

8.	Лк, лб, срс	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс]		Москва: Московский технический университет связи и информатики, 2016.— 31 с.	http://www.iprbookshop.ru/61529.html
ИНТЕРНЕТ - РЕСУРСЫ					
9.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka/ – образовательный портал университета			
10.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека			
11.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.			

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 с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».

Рецензент рабочей программы от выпускающей кафедры по направлению 10.03.01 – «Информационная безопасность», профилю «Безопасность автоматизированных систем».

	ст. преп.	З.Р. Рагимова
подпись	должность	ФИО