Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ
_____ **Ш. А. Юсуфов**
«18» 10 **2018 г.**

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ **Н. С. Суракатов**
«24» 10 **2018 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.30 Программно-аппаратные средства обеспечения ИБ

для специальности 10.05.03-«Информационная безопасность автоматизированных систем»

специализация «Безопасность открытых информационных 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) Специалист по защите информации
бакалавр (специалист)

Форма обучения очная ; курс4; семестр 8;

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

Лекции 51 (час); Экзамен 8 семестр (1 зет=36 часов)

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

лабораторные занятия 34 (час); самостоятельная работа 59 (час);

курсовой проект (работа, РГР)-(семестр).

Зав. кафедрой ИБ _____ **Г.И. Качаева**
подпись

Начальник УО _____ **Э.В. Магомаева**
подпись

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 от 15.10.2018г., протокол № 2

Зав. выпускающей кафедрой по данной специальности _____ **Г.И. Качаева**

ОДОБРЕНО
Методической комиссией по укрупненным группам специальностей и направлению подготовки
10.00.00- «Информационная безопасность»
Председатель МК
_____ Мелехин В.Б.
подпись ИОФ

«15» 10 2018г.

АВТОР ПРОГРАММЫ

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

_____

1. Цели и задачи дисциплины

1.1 **Цели дисциплины**

Формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств, а также навыков и умения в применении знаний для конкретных условий.

Развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

1.2 Задачи дисциплины

Задачи изучения дисциплины:

- Дать знания по концепции обеспечения информационной безопасности компьютерных систем;
- программно-аппаратным средствам, реализующим отдельные функциональные требования по защите;
- методам и средствам хранения ключевой информации;
- методам и средствам ограничения доступа к компонентам вычислительных систем;
- защите программ от изменения и контролю целостности;
- задачам и технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Техническая защита информации» относится к базовой части ФГОС ВО.

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность операционных систем, Безопасность систем баз данных, Дискретная математика, Математическая логика и теория алгоритмов, Моделирование автоматизированных информационных систем.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика, Разработка и эксплуатация защищенных автоматизированных систем, Защита программ и данных.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;
- ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

В результате изучения дисциплины студент должен:

В результате освоения дисциплины обучающийся должен:

знать: программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; типовые архитектуры и принципы построения современных защищенных информационных систем; угрозы и атаки, характерные для распределенных информационных систем;

уметь: проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;

владеть: навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

4. Структура и содержание дисциплины «Техническая защита информации»

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 180 часов, в том числе: лекционных -51 час, лабораторных - 34 часа, СРС – 59 часов, форма отчетности экзамен 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 успеваемости *(по срокам текущих аттестаций в семестре)*
				ЛК	ПЗ	ЛР	СР	
1.	**Лекция № 1** Программное обеспечение для моделирования сетей передачи данных.	5	1	2		2	4	Вх. Контр.
2.	**Лекция № 2** Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.		1	2		2	2	
3.	**Лекция № 3** Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.		2	2			2	
4.	**Лекция № 4** Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.		3	2		2	2	
5.	**Лекция № 5** Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.		3	2			2	
6.	**Лекция № 6** Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.		4	2		2	4	
7.	**Лекция № 7** Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.	6	5	2			2	
8.	**Лекция № 8** 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.	8	5	2		2	4	АКР №1
9.	**Лекция № 9** Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-		6	2		2	2	

	спуфинга. Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных							
10. 7	**Лекция № 10** 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.		7	2		2	4	
11.	**Лекция № 11** 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.		7	2		2	2	
12.	**Лекция № 12** 1. Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.		8	2			2	
13.	**Лекция № 13** 2. Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.		9	2		2	4	
14.	**Лекция № 14** 3. Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.		9	2			2	
15.	**Лекция № 15** Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.		10	2		2	4	АКР №2
16.	**Лекция № 16** Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.		11	2			2	
17.	**Лекция № 17** Основы работы в ОС семейства Linux. Управление правами доступа. Администрирование пользователей. Управление файлами и каталогами. Ссылки.		11	2		2	4	

	Архивирование и резервное копирование системы. Восстановление системы после критических сбоев из архивов.							
18.	**Лекция № 18** 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.		12	2		2	4	
19.	**Лекция № 19** Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.		13	2		2	4	
20.	**Лекция № 20** Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.		13	2		2	4	
21.	**Лекция № 21** Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.		14	2		2	4	
22.	**Лекция № 22** Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.		15	2			4	
23.	**Лекция № 23** Административные меры обеспечения комплексной безопасности в информационных системах.		15	2		2	2	АКР №3
24.	**Лекция №24** Административные меры обеспечения комплексной безопасности в информационных системах.		16	2			2	
25.	**Лекция № 25** Перспективные технологии обеспечения безопасности информации в информационных технологиях.		17	2		2	2	
26.	**Лекция № 26** Перспективные технологии обеспечения безопасности информации в информационных технологиях.		17	1			2	
	Итого по дисциплине			**51**		**34**	**76**	**зачет**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции израбочей программы	Наименование лабораторных заняти1	Рекомендуемая литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1.	Лк № 1	Программное обеспечение для моделирования сетей передачи данных.	№№ 1-11	2
2.	Лк № 2,3	Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.	№№ 1-11	2
3.	Лк № 4,5	Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.	№№ 1-11	2
4.	Лк №6,7	Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.	№№ 1-11	2
5.	Лк №8	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
6.	Лк №9	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
7.	Лк №10	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
8.	Лк №11,12	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
9.	Лк №13,14	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
10.	Лк № 15,16	Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и	№№ 1-11	2

		настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.		
11.	Лк № 17	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
12.	Лк №18	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
13.	Лк №19	Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.	№№ 1-11	2
14.	Лк № 20	Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.	№№ 1-11	2
15.	Лк № 21,22	Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.	№№ 1-11	2
16.	Лк № 23	Административные меры обеспечения комплексной безопасности в информационных системах.	№№ 1-11	2
17.	Лк № 24,25	Перспективные технологии обеспечения безопасности информации в информационных технологиях.	№№ 1-11	2
Итого по дисциплине				**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	Формаконтроля СРС
1.	Программное обеспечение для моделирования сетей передачи данных.	4	№№ 1-11	Опрос, реферат, статья
2.	Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh.	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	2	№№ 1-11	Опрос, реферат,

	передаче данных по сети. Сравнительный анализ. Протокол настройки времени.			статья
5.	Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени.	2	№№ 1-11	Опрос, реферат, статья
6.	Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF.	4	№№ 1-11	Опрос, реферат, статья
7.	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
8.	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.	4	№№ 1-11	Опрос, реферат, статья
9.	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
10.	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.	4	№№ 1-11	Опрос, реферат, статья
11.	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
12.	18. 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
13.	19. Изучение технологии ACL (AccessControlList). Типы ACL. Создание списков доступа. Общие принципы VirtualPrivateNetwork (VPN).	4	№№ 1-11	Опрос, реферат, статья

	Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE.			
14.	20. 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
15.	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
16.	Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSLVPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco.	2	№№ 1-11	Опрос, реферат, статья
17.	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
18.	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
19.	Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.	4	№№ 1-11	Опрос, реферат, статья
20.	Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД.	4	№№ 1-11	Опрос, реферат, статья
21.	Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.	4	№№ 1-11	Опрос, реферат, статья
22.	Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности.	4	№№ 1-11	Опрос, реферат, статья
23.	Административные меры обеспечения комплексной безопасности в	2	№№ 1-11	Опрос, реферат, статья

	информационных системах.			
24.	Административные меры обеспечения комплексной безопасности в информационных системах.	2	№№ 1-11	Опрос, реферат, статья
25.	Перспективные технологии обеспечения безопасности информации в информационных технологиях.	2	№№ 1-11	Опрос, реферат, статья
26.	Перспективные технологии обеспечения безопасности информации в информационных технологиях.	2	№№ 1-11	Опрос, реферат, статья
Итого		**76**		

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 для проверки знаний студентов

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

10. Программное обеспечение для моделирования сетей передачи данных.
11. Эмулятор GNS3.
12. Основы работы и моделирование простых схем.
13. Протоколы удаленного доступа. Протоколы telnet, ssh.
14. Обеспечение безопасности при передаче данных по сети.
15. Сравнительный анализ.
16. Протокол настройки времени.
17. Динамическая IP-маршрутизация.
18. Внутренние протоколы маршрутизации.
19. Пограничный шлюзовой протокол маршрутизации.
20. Протоколы RIP, IGRP и EIGRP.
21. Протокол динамической маршрутизации OSPF.
22. Атака типа «Отказ в обслуживании» (DoS-атака).
23. Механизмы защиты от некоторых типов DoS-атак.
24. Антиспуфинг. Защита от IP-спуфинга.
25. Защита от ARP-спуфинга.
26. 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.
21. Изучение технологии ACL (AccessControlList).
22. Типы ACL.
23. Создание списков доступа.
24. Общие принципы VirtualPrivateNetwork (VPN).
25. Сравнительный анализ протоколов VPN.
26. Настройка VPN соединения через протокол GRE.
27. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco.
28. Применение SSLVPN

29. 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) «Программно-аппаратные средства обеспечения ИБ»

7.1. Рекомендуемая литература и источники информации

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 c	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 c.	http://www.iprbookshop.ru/61529.html	
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.

7.2. Программное обеспечение

Интегрированные среды разработки программ Borland Developer Studio и Visual Studio . NET, базы данных, информационно – справочные и поисковые системы; вузовские электронно-библиотечные системы учебной литературы.

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 (работодателя) 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

по специальности _____ З.Р. Рагимханова

подпись. ФИО