Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ А.С. Авдеев

Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.Б.32 «Технологии защиты информации в глобальных сетях»**

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **обязательная часть (базовая)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	Е.В. Шарлаев
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОПК-7	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	- основные угрозы безопасности информации для защиты информации в глобальных сетях; - методы анализа объекта информатизации на предмет выявления угроз безопасности и имеющихся уязвимостей для защиты информации в глобальных сетях	- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите в глобальных сетях; - выявлять уязвимости информационно-технологических ресурсов информационных систем в глобальных сетях	- навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты в глобальных сетях; - методами выявления угроз и уязвимостей информационной безопасности информационных систем в глобальных сетях;
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации	- методы и средства проведения экспериментальных исследований по оценке эффективности работы систем защиты информации, в том числе в глобальных сетях ; - способы и средства защиты информации от утечки по техническим каналам, в том числе в глобальных сетях	-проводить экспериментальные исследования систем защиты информации в глобальных сетях; - проводить мониторинг угроз безопасности информационных систем в глобальных сетях.	- методами выявления уязвимостей автоматизированных систем в глобальных сетях
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	- методы и приемы администрирования подсистем информационной безопасности объекта защиты, как технологиеи защиты информации в глобальных сетях	- применять методы и приемы администрирования подсистем информационной безопасности объекта защиты, как технологии защиты информации в глобальных сетях	- навыками администрирования подсистемы информационной безопасности объекта защиты, как технологии защиты информации в глобальных сетях

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению	Аппаратные средства вычислительной техники, Информатика, Информационные технологии, Языки

дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	программирования
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Безопасность WEB-технологий, Выпускная квалификационная работа, Информационная безопасность автоматизированных систем, Преддипломная практика, Программно-аппаратные средства защиты информации, Сети и системы передачи информации, Технологическая практика, Эксплуатационная практика

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 6 / 216

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	34	68	0	114	110

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Форма обучения: очная

Семестр: 6

Объем дисциплины в семестре з.е. /час: 3 / 108

Форма промежуточной аттестации: Экзамен

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
17	34	0	57	56

Лекционные занятия (17ч.)

1. Введение в глобальные вычислительные сети.(4ч.)[5,6,9] Тема 1. Операционные возможности глобальных вычислительных сетей.

Мультисервисная (конвергентная) сеть. Основные задачи администратора при проектировании, построении и сопровождении сети. Назначение основных сервисов глобальных вычислительных сетей, их особенности реализации и использования.
Тема 2. Служба доменных имен. Терминология и принципы работы. Типы серверов доменных имен (Master, Slave, Cache, Stealth, Root). Понятие зон – прямая и обратная. Конфигурирование DNS в различных сетевых операционных системах. Протокол DNS.
2. Маршрутизация. {дискуссия} (6ч.)[5,6,9,11] Тема 1. Организация взаимодействия в глобальных вычислительных сетях. Маршрутизация. Пересылка пакетов. Маршрутизатор и принципы его работы. Интерфейсы маршрутизатора. Введение в таблицу маршрутизации. Directly-Connected сети. Next-hop и выходной интерфейс. Статическая маршрутизация. Протоколы ARP и RARP. Суммирование статических маршрутов. Маршрут по умолчанию. Тема 2. Динамическая маршрутизация. Протоколы динамической маршрутизации. Классификация протоколов динамической маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протоколы маршрутизации состояния связей. Классовая и без классовая маршрутизация. Тема 3. Понятие сходимости протокола маршрутизации. Принципы работы таблицы маршрутизации. Лучший маршрут и метрика. Распределение нагрузки. Административная дистанция. Дистанционно-векторные протоколы динамической маршрутизации RIP, EIGRP. Протоколы маршрутизации состояния связей OSPF.
3. Почтовая служба {дискуссия} (4ч.)[5,6,9,11] Тема 1. Организация почтовой службы. Основные способы организации (on-line, off-line). Средства реализации почтовой службы в различных сетевых операционных системах (sendmail, exim, postfix, Microsoft Exchange Server). Протоколы обмена почтовыми сообщениями (POP, SMTP, IMAP). Тема 2. Организация служб электронного общения в режиме on-line. Мессенджеры и VoIP сервис. Телеконференции. Группы новостей.
4. Программное обеспечение прикладного уровня. {дискуссия} (3ч.)[5,6,9,11] Тема 1. Приложения, сервисы. Модель «клиент-сервер». Point-to-Point сети и приложения. Протоколы прикладного уровня: Web - HTTP (80) и HTTPS (443), Протоколы файлового обмена – FTP (20, 21) и SMB (445), электронной почты – SMTP (25), POP (110) и IMAP (143), дистанционного управления – Telnet (23), RDP (3389) и SSH (22), система доменных имён – DNS (53), протокол динамической конфигурации узла DHCP (67, 68), протоколы управления – SNMP (161, 162). Формат данных HTTP, FTP, SMTP, POPv3, DNS, DHCP и принцип их работы. Тема 2. Уровень защищённых сокетов, протокол SSL и его применение. Принцип работы протокола SSL. Аутентификация и обмен ключами. Почтовая система (MUA, MTA, MDA). Виды конференцсвязи (аудио, видео), примеры организации конференций.

Лабораторные работы (34ч.)

1. Установка и администрирование сервера LDAP. {работа в малых группах}

(4ч.)[1,2,3,11] Цель работы: настройка и администрирование сервера Ldap.
Указания к выполнению работы: Для начала необходимо определиться, что у нас есть: -имя хоста: dc01; -полное доменное имя: dc01.example.local; -после настройки содержимое файла /etc/hostname будет изменено на dc01.example.local; -LDAP домен: example.local -он транслируется в Base DN: dc=example,dc=local; -адрес DNS-сервера: 192.168.1.60; -для простоты определимся, что все пароли будут: 12345. Администрирование подсистемы информационной безопасности объекта защиты

2. Сервисы удаленного терминального доступа (Telnet, rlogin, RDP, SSH). Организация FTP-сервиса. {работа в малых группах} (4ч.)[1,2,3,11] Задачи лабораторной работы: -закрепление, углубление и расширение знаний в процессе выполнения конкретных практических задач; -развитие профессиональных навыков, практическое овладение методами экспериментальных исследований в области администрирования компьютерных сетей, обработки и представления результатов проведенных исследований и формирования выводов; -приобретение умений и навыков в настройке FTP сервера; -приобретение умений и навыков в работе с сервисами удаленного управления (Telnet, rlogin, RDP). Описание лабораторной установки: -Лабораторная работа выполняется в локальной вычислительной сети на рабочих станциях под управлением операционной системы Linux с версией ядра 2.4-2.6, имеющих выход в Интернет. Лабораторная работа состоит из 2 частей: -настройка и использования сервисов удаленного управления (Telnet, rlogin, RDP); -настройка и администрирование FTP сервера.

3. Обеспечение Безопасности протокола IP с помощью средства IPsec. {работа в малых группах} (4ч.)[1,2,3,11] Цель работы: научиться настраивать защищенное соединение с помощью протокола IPsec. Задание: -настроить защищенное соединение между двумя компьютерами в сети с помощью IPSec; -запустить программу MMC (Пуск\Выполнить в поле Открыть (Open) введите mmc. Нажмите OK); -добавить оснастки Управление политикой безопасности IP и Монитор безопасности (Консоль\Добавить или удалить оснастку).

4. Овладение навыками работы с прикладной криптосистемой PGP {работа в малых группах} (4ч.)[1,2,3,11] Методические указания к выполнению лабораторной работы с использованием PGP: 1.Осуществить защищённый обмен почтовыми сообщениями. 2.Сгенерировать ключевую пару. 3.Обменяться открытыми ключами с получателем. 4.Зашифровать текстовое сообщение (различными способами). 5.Зашифровать не текстовый файл. 6.Передать зашифрованные материалы получателю и получить от него другие зашифрованные материалы. 7.Расшифровать полученные материалы.

5. Статическая маршрутизация. Протоколы ARP и RARP. Динамическая маршрутизация. Протоколы RIP, OSPF, BGP. {работа в малых группах} (4ч.)[1,2,3,11] Указания к выполнению лабораторной работы:
1.С помощью протокола ARP собрать сведения по сегменту сети. 2.Используя три узла имеющийся сети осуществить статическую маршрутизацию. 3.Результаты выполнения предыдущего пункта задокументировать. 4.Настроить маршрутизацию с помощью Quagga аналогично пункта 2. 5.Результаты

выполнения задания 4 задокументировать. 6.Ответить на вопросы преподавателя.
6. Администрирование сети средствами технологии Cisco {работа в малых группах} (4ч.)[1,2,3,11] Цели и задачи работы: Закрепление навыков настройки сетевого оборудования Cisco. Для выполнения необходим консольный кабель (получить у преподавателя), маршрутизатор Cisco 1841 (получить у преподавателя), компьютер для настройки маршрутизатора, программа эмулятор iOS GNS3, PuTTY. Указания к выполнению лабораторной работы: - Включить в сеть маршрутизатор. -Подключить Ethernet-кабель одним концом в порт маршрутизатора FastEthernet 0, другим концом в порт локальной сети аудитории. -Подключить консольный кабель в COM-порт компьютера и в console-порт маршрутизатора. -Собрать схему сети согласно методическим указаниям к выполнению лабораторной работы.
7. Настройка точки доступа Cisco Aironet 1200 Series {работа в малых группах} (4ч.)[1,2,3,11] Цели и задачи работы: Закрепление навыков настройки сетевого оборудования Cisco. Приобретение навыков настройки Wi-Fi точек доступа Cisco. Оборудование и ПО:
Для выполнения необходим консольный кабель (получить у преподавателя), маршрутизатор Cisco 1841 (получить у преподавателя), точка доступа Cisco Aironet (получить у преподавателя), компьютер для настройки точки доступа, программа PuTTY. Указания к выполнению лабораторной работы: 1.Включить в сеть точку доступа. 2.Подключить Ethernet-кабель одним концом в порт точки доступа, другим концом в свободный порт маршрутизатора. 3.Подключить консольный кабель в COM-порт компьютера и в console-порт точки доступа. 4.Собрать предложенную преподавателем схему провести ее настройку и тестирование, предоставить результаты отчета.
8. Персональный межсетевой экран. {работа в малых группах} (6ч.)[1,2,3,11] Цель работы: приобретение практических навыков работы при на-стройке прокси-сервера, фаервола и биллинга Интернет трафика в корпоративной сети с помощью Kerio WinRoute Firewall.

Самостоятельная работа (57ч.)
1. Подготовка к лекционным занятиям, СРС {использование общественных ресурсов} (17ч.)[5,6,9,12]
2. Подготовка к текущему контролю (выполнение и защита лабораторных работ {использование общественных ресурсов} (13ч.)[1,2,3,11]
3. Подготовка к промежуточной аттестации (экзамен). {использование общественных ресурсов} (27ч.)[1,2,3,4,5,6,9]

Семестр: 7
Объем дисциплины в семестре з.е. /час: 3 / 108
Форма промежуточной аттестации: Экзамен

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем
Лекции	Лабораторные	Практические	Самостоятельная	

	работы	занятия	работа	(час)
17	34	0	57	54

Лекционные занятия (17ч.)

5. Обеспечение безопасности межсетевого взаимодействия. {беседа} (6ч.)[5,6,9] Тема 1. Межсетевое взаимодействие. Основы сетевого и межсетевого взаимодействия. Классификация сетевых атак. Информационная безопасность.

Тема 2. Политика безопасности. Шаблоны политики безопасности. Сетевая политика безопасности. Эшелонированная оборона

Тема 3. Управление рисками. Основные понятия. Процесс оценки рисков. Уменьшение рисков. Аудит информационной безопасности. Механизмы и службы защиты.

Тема 4. Определение информационных ресурсов, подлежащих защите, угроз безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

6. Межсетевые экраны. {беседа} (4ч.)[5,6,9] Тема 1. Классификация межсетевых экранов. Пакетные фильтры. Пример набора правил пакетного фильтра. Пакетный фильтр с учетом контекста (Stateful Packet Inspection). Межсетевые экраны host-based. Прокси-сервер прикладного уровня.

Тема 2. Различные типы окружений межсетевых экранов. Основные принципы построения окружения межсетевого экрана. Конфигурация с одной DMZ-сетью. Конфигурация Service Leg. Конфигурация с двумя DMZ-сетями.

7. Виртуальные частные сети. {беседа} (4ч.)[5,6,7,8,9] Тема 1. Виртуализация. Гипервизоры (Microsoft Hyper-V, VMware ESX, VirtualBOX). Технологии распределённых вычислений. Облачные вычисления. Кластеры. Диагностика сетей (программные, аппаратные и программно-аппаратные комплексы для тестирования и сопровождения сетей).

Тема 2. Виртуальные частные сети (VPN). Туннелирование. Протоколы VPN канального уровня. Протокол PPTP. Протокол L2TP. Протокол IPSec. Ассоциация обеспечения безопасности.

Тема 3. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Совместное использование протоколов ESP и AH. Основные типы защищенных связей. Протоколы VPN транспортного уровня. Протокол SSL. Протокол SOCKS.

8. Системы обнаружения вторжений (Intrusion Detection Systems). {беседа} (3ч.)[5,6,7,8,9] Тема 1. Типы IDS. Архитектура IDS. Способы управления. Информационные источники. Анализ, выполняемый IDS. Возможные ответные действия IDS. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. Цели и задачи использования IDS. Существующая политика безопасности. Развертывание IDS. Сильные стороны и ограниченность IDS. Тема 2. Участие в проведении экспериментальных исследований системы защиты информации.

Лабораторные работы (34ч.)

9. Защита сети и сокрытие ее топологии. FireWall & Proxy-сервис. {работа в малых группах} (6ч.)[1,2,3,4,15] Цели и задачи работы: Обеспечить защиту локальной сети со стороны сети общего доступа путем установки и настройки межсетевого экрана Iptables и proxy сервера squid.

Задачи лабораторной работы:

-закрепление, углубление и расширение знаний в процессе выполнения конкретных практических задач

-развитие профессиональных навыков, практическое овладение методами экспериментальных исследований в области администрирования компьютерных сетей, обработки и представления результатов проведенных исследований и формирования выводов;

-приобретение умений и навыков в настройке прокси сервера;

-приобретение умений и навыков в настройке межсетевого экрана – фаервола Iptables.

10. Настройка системы обнаружения сетевых атак Snort {работа в малых группах} (4ч.)[2,3,5,7] Цели и задачи работы: изучение и практическое применение системы обнаружения сетевых атак Snort

Задание к работе: Настроить систему обнаружения сетевых атак Snort

Методика выполнения работы:

Установить на сервер необходимую оснастку.

В соответствие с вариантом настроить на сервере правила.

Проверить работоспособность созданного сервера.

11. Организация VPN средствами СЗИ Vipnet. {работа в малых группах} (4ч.)[2,3,5,7,10] Цели и задачи работы: изучение принципов построения виртуальных частных сетей средствами СЗИ Vipnet.

Методика выполнения работы:

Установить на сервер необходимую оснастку.

В соответствие с вариантом настроить на сервере правила.

Проверить работоспособность созданного сервера.

12. Защита сети средствами DLP {работа в малых группах} (4ч.)[2,3,5,7]

Методика выполнения работы:

Установить на сервер необходимую оснастку.

В соответствие с вариантом настроить на сервере правила.

Проверить работоспособность созданного сервера.

13. Сканер уязвимостей OpenVas 8.0 {работа в малых группах} (4ч.)[2,3,4,7,10] Цель: Приобретение навыков сканирования компьютера с целью поиска и устранения уязвимостей.

Указания к выполнению лабораторной работы.

1) Установить OpenVas на компьютер.

2) Создать новую политику и задачу сканирования.

3) Провести сканирование одного или нескольких компьютеров.

4) Просмотреть результаты сканирования.
5) Проанализировать результаты.
6) По результату выполнения составить отчет по лабораторной работе.

14. Тестирование безопасности паролей системных служб и приложений путем эмуляции атак. {работа в малых группах} (4ч.)[2,3,4,7,10] Цель: Приобретение навыков проверки безопасности паролей системных служб и приложений на предмет подверженности взлому.

Указания к выполнению лабораторной работы.

1) На компьютере под управлением операционной системы Windows XP/7 создать 3 учетные записи, для администратора и одного пользователя установить пароли, второго пользователя создать без пароля. Так же на этом компьютере нужно развернуть FTP-сервер и создать двух клиентов: root и обычного пользователя.
2) С помощью программы Hydra с компьютера под управлением Kali Linux произвести тесты по перехвату паролей по SMB и FTP протоколу с помощью созданного и скаченного словаря паролей.
3) Установить на учетные записи более сложные пароли и повторить пункт 2, затем установить ограничения на количество попыток ввода пароля при аутентификации ОС и повторить пункт 2.
4) Сделать отчет по проделанной работе.
5) Ответить на контрольные вопросы.

15. Тесты на проникновения СУБД MySQL {работа в малых группах} (4ч.)[3,4,7] Цель: Приобретение навыков проверки безопасности СУБД MysSQL на предмет подверженности взлому.

Указания к выполнению лабораторной работы.

1) Установить и настроить MySQL Server 5.1
2) Создать базу данных с 2 двумя таблицами, наполнить их информацией, а так же создать дополнительного пользователя admin без пароля, чтобы он мог подключаться только из localhost.
3) С помощью утилит Metaslpoit Framework и HexorBase получить доступ к MySQL серверу.
4) Подключиться к серверу с нескольких пользователей.
5) Показать пример работы с базой данных (удаление записей, таблиц, добавление и удаление пользователей, сохранение базы на компьютер).
6) Усложнить пароль для администратора и повторить пункты 3-5.
7) Сделать отчет по проделанной работе.
8) Ответить на контрольные вопросы.

17. Обеспечение защиты от DoS-атак {работа в малых группах} (4ч.)[3,4,7] Цель: Приобретение навыков обеспечения защиты от атак типа отказ – в – обслуживании на примере веб-сервера apache2.

Указания к выполнению лабораторной работы.

1) На компьютере под управлением операционной системы Windows Server 2003 настроить терминальный доступ и проверить его работоспособность с компьютеров-клиентов под управлением Windows и Ubuntu.
2) С помощью программы Torshammer, установленной на компьютере под

управлением Kali Linux 2.0 произвести эмуляцию DoS-атаки на Windows Server 2003 до отказа-в-обслуживании сервера терминального доступа.
3) На компьютере под управлением Ubuntu установить и настроить веб-сервер apache2.
4) Провести тесты DoS-атак типа SYN и HTTP флуд программами Torshammer, PyLoris, Slowhttptest, установленные на компьютере под управлением Kali Linux 2.0.
5) Обнаружить данные атаки, реализовать меры по защиты от будущих подобных атак и проверить работоспособность реализованных мер
6) Сделать отчет по проделанной работе.
7) Ответить на контрольные вопросы.

Самостоятельная работа (57ч.)

4. Подготовка к лекциям. {использование общественных ресурсов} (8ч.)[5,6,7,8,9,10,12]

5. Подготовка к защите лабораторных работ {использование общественных ресурсов} (13ч.)[1,2,3,4,13,14,15,16,17,18,19]

6. Подготовка к промежуточной аттестации (экзамен). {использование общественных ресурсов} (36ч.)[5,6,7,8,9,10,11,12]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Чугунов Г.А., Методические указания по выполнению лабораторных работ по дисциплине «Сети и телекоммуникации». – Барнаул: Изд-во АлтГТУ, 2012. – 17с.; Источник: электронная библиотека образовательных ресурсов АлтГТУ. Реж.доступа http://elib.altstu.ru/eum/download/vsib/tugunov-sit.pdf

2. Шарлаев Е.В. Вычислительные сети. Учебно-методическое пособие/ Е.В. Шарлаев; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2015. - 86 с.;Источник: электронная библиотека образовательных ресурсов АлтГТУ. Реж. доступа http://elib.altstu.ru/eum/download/ivtib/uploads/sharlaev-e-v-ivtiib-569e03fec1d87.pdf

3. Шарлаев Е.В. Администрирование глобальных вычислительных сетей: Учебно-методическое пособие.- Барнаул, АлтГТУ, 2010. -122с. Источник: электронная библиотека образовательных ресурсов АлтГТУ. Режим доступа http://new.elib.altstu.ru/eum/download/vsib/sharlaev_gvs.pdf (Методические указания к выполнению лабораторных работ)

4. Рыбин В.В., Шарлаев Е.В. Безопасность вычислительных сетей.

Лабораторный практикум: учебно-методическое пособие; Алт. гос. техн. ун–т им. И.И. Ползунова, - Барнаул: 2017. - 71 с.; Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/RybinSharlaev_BezopVSLP_ump.pdf

6. Перечень учебной литературы

6.1. Основная литература

5. Зензин, А.С. Информационные и телекоммуникационные сети: учебное пособие / А.С. Зензин; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск: НГТУ, 2011. - 80 с.: табл., схем. - ISBN 978-5-7782-1601-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228912 (15.05.2019).

6. Телекоммуникационные системы и сети: В 3 томах. Том 3. - Мультисервисные сети [Электронный ресурс]: учебное пособие / В.В. Величко [и др.]; под ред. В.П. Шувалова. — Электрон. дан. — Москва: Горячая линия-Телеком, 2015. — 592 с. — Режим доступа: https://e.lanbook.com/book/64092. — Загл. с экрана.

7. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. —Электрон. дан. — Москва: ДМК Пресс, 2012. —592с. —Режим доступа: https://e.lanbook.com/book/3032. —Загл. с экрана.

8. Ачилов, Р.Н. Построение защищенных корпоративных сетей [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. — Электрон. дан. — Москва: ДМК Пресс, 2013. — 250 с. — Режим доступа: https://e.lanbook.com/book/66472. — Загл. с экрана.

9. Беленькая, М.Н. Администрирование в информационных системах [Электронный ресурс]: учебное пособие / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. —Электрон. дан. — Москва: Горячая линия-Телеком, 2011. —400 с. —Режим доступа: https://e.lanbook.com/book/5117. —Загл. с экрана.

6.2. Дополнительная литература

10. Запечников, С.В. Основы построения виртуальных частных сетей [Электронный ресурс]: учебное пособие/ С.В. Запечников, Н.Г. Милославская, А.И. Толстой. — Электрон. дан. —Москва: Горячая линия-Телеком, 2011. — 248 с. — Режим доступа: https://e.lanbook.com/book/11834. — Загл. с экрана.

11. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под общ. ред. Н.И. Синадского; Министерство образования и науки Российской Федерации, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. - Екатеринбург: Издательство Уральского университета, 2014. -179с.: ил. -Библиогр. в кн. - ISBN 978-5-7996-1201-6; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=275694

12. Гурчикова, А.С. Состав и функции сетевого оборудования ККС/ А.С.

Гурчикова. -Москва: Лаборатория книги, 2012. -134 с.: табл., схем. - ISBN 978-5-504-00259-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=142472

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

13. Интернет-сайт открытого программного обеспечения OpenNET (http://opennet.ru/)
14. Интернет-сайт компании Cisco-Россия (http://www.cisco.ru/)
15. Операционная система Linux Ubuntu (http://www.ubuntu.com)
16. Программный продукт виртуализации для операционных систем http://www.virtualbox.org)
17. Сетевой сканер Nmap (http://nmap.org)
18. Анализатор сетевого трафика Wireshark (http://www.wireshark.org)
19. Графический симулятор сети GNS3 (http://www.gns3.net)

8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
1	Cisco Packet Tracer
2	Debian
3	Dia
4	FreeBSD
5	LibreOffice
6	VirtualBox
7	Mozilla Firefox
8	Windows
9	Windows Server

№пп	Используемое программное обеспечение
10	ViPNet client (демо-версия)
11	Kaspersky Endpoint Security для бизнеса Расширенный
12	Squid
13	ViPNet Coordinator (демо-версия)
14	ViPNet CSP
15	Wireshark
16	Xen
17	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
2	Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения занятий лекционного типа
лаборатории и специализированные кабинеты (классы, аудитории)
помещения для самостоятельной работы
учебные аудитории для проведения групповых и индивидуальных консультаций
лаборатории в области сетей и систем передачи информации

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».