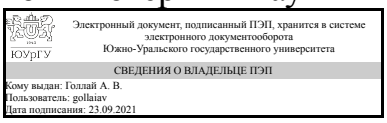
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



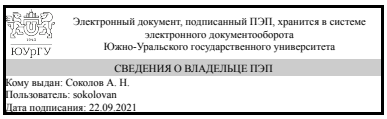
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.27 Безопасность сетей электронных вычислительных машин
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

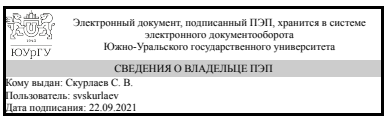
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
старший преподаватель



С. В. Скурлаев

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ. Задачи: - изучение основных элементов теории построения сетей; - изучение основных принципов функционирования сетевых протоколов; - привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей; - изучение основных угроз в сетях ЭВМ и методов противодействия им; - овладение механизмами построения систем безопасности сетей ЭВМ.

Краткое содержание дисциплины

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать:принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей
	Уметь:
	Владеть:
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать:методы проектирования и администрирования компьютерных сетей
	Уметь:проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети
	Владеть:навыками эксплуатации и администрирования локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знать:принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей
	Уметь:
	Владеть:навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Знать:основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; критерии оценки эффективности и надежности средств защиты сетей ЭВМ
	Уметь:эффективно использовать различные методы и средства защиты информации для компьютерных сетей
	Владеть:навыками использования программно-аппаратных средств обеспечения безопасности

	сетей ЭВМ
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать:критерии оценки эффективности и надежности средств защиты сетей ЭВМ
	Уметь:оценивать эффективность и надежность защиты сетей ЭВМ
	Владеть:
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Знать:методы проектирования и администрирования компьютерных сетей
	Уметь:проводить мониторинг угроз безопасности компьютерных сетей
	Владеть:навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.18 Языки программирования, Б.1.08 Информатика	Б.1.37 Комплексное обеспечение защиты информации объектов информатизации, Б.1.29 Безопасность систем баз данных, Б.1.36 Информационная безопасность открытых систем

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.08 Информатика	Студенты должны знать формы представления информации, эталонную модель взаимодействия открытых систем, иметь понятие о стеке протоколов TCP/IP, должны уметь пользоваться поисковыми системами
Б.1.18 Языки программирования	Студенты должны знать о взаимодействии программ со стеком протоколов, установленным в системе, через прикладной программный интерфейс

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 5 з.е., 180 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
Общая трудоёмкость дисциплины	180	180
Аудиторные занятия:	80	80
Лекции (Л)	32	32

Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	16	16
Самостоятельная работа (СРС)	100	100
Изучение материалов по плану СРС	64	64
Подготовка к лабораторным работам, оформление результатов	18	18
Подготовка к практическим занятиям, оформление результатов	18	18
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основы организации и функционирования сетей ЭВМ	6	6	0	0
2	Сети TCP/IP	20	8	8	4
3	Технологии глобальных сетей	6	2	4	0
4	Сетевые сервисы и службы	16	4	8	4
5	Средства и способы построения отказоустойчивых сетей	8	4	4	0
6	Сетевая безопасность	24	8	8	8

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Понятие сети ЭВМ. Этапы развития сетей ЭВМ	2
2	1	Критерии классификации сетей ЭВМ. Характеристики сетей ЭВМ	2
3	1	Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей ЭВМ. Модель ISO OSI. Технологии обеспечения безопасности в сетях ЭВМ	2
4	2	Практические отличия реализации стека TCP/IP от эталонной модели ISO OSI.	2
5	2	Методы коммутации. Методы доступа к разделяемой среде. Угрозы безопасности информации, передаваемой в сетях ЭВМ, на физическом и канальном уровнях.	2
6	2	Сетевой уровень построения сетей ЭВМ. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях	2
7	2	Протоколы разрешения адресов ARP, RARP. Алгоритмы маршрутизации, их характеристика. Протоколы и алгоритмы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, NLSP, EGP, BGP)	2
8	3	Транспортные услуги и технологии глобальных сетей. Технология MPLS	2
9	4	Сетевые службы и средства управления	2
10	4	Средства контроля внешнего периметра сети. Средства контроля доступа к сетевым службам. Средства активного аудита сетей ЭВМ. Протокол SNMP	2
11	5	Технология VLAN. Угрозы безопасности информации, передаваемой в	2

		локальных сетях ЭВМ. Методы их нейтрализации	
12	5	Протоколы VRRP/HSRP. Основы кластерных решений. DM VPN (Cisco VPN) как пример динамически организующейся сети	2
13	6	Классификации угроз безопасности телекоммуникационных сетей	2
14	6	Классификация методов защиты. Основные технологии обеспечения безопасности в сети	2
15	6	Межсетевые экраны и средства обнаружения вторжений. Сегментирование. Аутентификация, авторизация, аудит.	2
16	6	Криптографические средства защиты информации в сетях ЭВМ. Виртуальные частные сети. Протокол SSL	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Создание элементов структурированной кабельной системы	4
2	2	Построение сетей с помощью коммутаторов, организация подсетей, настройка маршрутизатора	4
3	3	Настройка протоколов внутренней и междоменной маршрутизации	4
4	4	Развёртывание доменной структуры (на базе Windows Server), DNS, настройка пользователей, настройка доменных политик	4
5	4	Настройка сервера WEB, VPN, почтовых служб, дополнительных сервисов	4
6	5	Построение сети, сегментированной на VLAN, взаимодействие между различными сегментами, аутентификация в целевой VLAN (протокол 802.1X)	2
7	5	Настройка кластера маршрутизаторов с помощью протокола VRRP или HSRP	2
8	6	Настройка межсетевого экрана, средства обнаружения вторжений (snort или suricata). Аудит журналов	4
9	6	Построение модели сети организации (организация сегментов сети, взаимодействующих через VPN, аутентификация пользователей по протоколу 802.1X)	4

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	2	Изучение промышленных коммутаторов и маршрутизаторов. Управление конфигурациями устройств. Построение простейшей сети на базе лаборатории	4
2	4	Организация доверительных отношений между доменами Active Directory, управление полномочиями пользователей, изучение протокола Kerberos	4
3	6	Организация сегмента сети с применением протоколов группы IEEE 802.11, изучение атак на беспроводные сети	4
4	6	Организация защищённой сети с помощью сертифицированных средств криптографической защиты, взаимодействие между узлами сетей разных организаций, нюансы сертифицированных решений	4

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение материалов по темам: Сетевые службы и средства управления. Средства контроля доступа к сетевым службам. Средства активного аудита сетей ЭВМ (nmap, Kali Linux)	Дополнительная литература	19
Подготовка к лабораторным работам, оформление результатов	Основная литература	18
Изучение материалов по темам: Этапы развития сетей ЭВМ. Стандартные стеки коммуникационных протоколов. Методы коммутации.	Основная литература, дополнительная литература	14
Изучение материалов по темам: Методика расчета сетей Ethernet. Протоколы IPv4, IPv6, адресация в IP-сетях. Транспортные протоколы в Internet: TCP и UDP. Протоколы управления SNMP и CMIP. Виртуальные частные сети (OpenVPN).	Основная литература, дополнительная литература	31
Подготовка к практическим занятиям, оформление результатов	Основная литература	18

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Моделирование сетевых процессов в Cisco Packet Tracer	Практические занятия и семинары	Проектирование топологии сети, настройка активного сетевого оборудования, установка основных сетевых служб с помощью построения соответствующих моделей в программной среде Cisco Packet Tracer	8
Моделирование сетевых процессов с применением виртуальных машин	Лабораторные занятия	Построение сети, установка и настройка сетевых средств защиты информации в виртуальных средах VMware Player или Oracle VM VirtualBox	4

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование	Контролируемая компетенция ЗУНы	Вид контроля (включая	№№ заданий

разделов дисциплины		текущий)	
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Экзамен	8-14
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Экзамен	36-42
Все разделы	ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Экзамен	29-35
Все разделы	ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Экзамен	15-21
Все разделы	ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Экзамен	22-28
Все разделы	ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Экзамен	1-7
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Защита отчёта по практической работе	Практическая 1-4
Все разделы	ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Защита отчёта по лабораторной работе	Лабораторная 1-4
Сетевая безопасность	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Задание на допуск	Практическое задание
Сетевые сервисы и службы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Доклад по теме на выбор из списка	Доклад
Сети TCP/IP	ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Бонусные баллы за выполнение практических 1-3	Практическая 1-3
Все разделы	ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Бонусные баллы за участие в мероприятиях по информационной безопасности	—

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Защита отчёта по практической работе	Защита практической работы осуществляется индивидуально. Студент представляет результат выполнения практического задания из методических указаний и отвечает на вопрос преподавателя. Оценивается качество оформления, своевременность выполнения работы и ответы на вопросы (задаётся 1 вопрос). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей: - правильность выполнения работы, если есть недочёты, то из оценки вычитается 1 балл; - своевременность сдачи работы и ответа на вопрос, за каждую неделю просрочки отчета из оценки вычитается 1балл. Максимальное количество баллов за одну работу – 6. Всего в течение семестра предусмотрено 4 рейтинговых практических работы. Весовой коэффициент каждой практической – 1. Общее количество за практические работы – 24.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 % Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %
Бонусные баллы за участие в мероприятиях по информационной безопасности	Студент представляет копии документов, подтверждающие победу или участие в предметных олимпиадах, конференциях или иных мероприятиях по темам дисциплины При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %	Зачтено: +15 % за призовое место в мероприятии международного уровня +10 % за призовое место в мероприятии российского уровня +5 % за призовое место в мероприятии университетского уровня +1 % за участие в мероприятии Не зачтено: —
Бонусные баллы за выполнение практических 1-3	Студент выполняет практическую работу в виртуальных машинах на базе ОС Linux. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +12	Зачтено: +4 за каждую работу Не зачтено: —
Доклад по теме на выбор из списка	Доклад осуществляется в течение семестра по теме из списка. Подготовка и выступление происходит индивидуально или в группе, в зависимости от темы. Студент(ы) представляет результат подготовки в виде презентации и доклада, отвечает (-ют) на вопрос преподавателя и других студентов. Оценивается качество выступления и ответы на вопросы. При	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 % Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %

	оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей: - ответы на вопрос, за каждый не отвеченный вопрос из оценки вычитается 1балл. Максимальное количество баллов за работу – 5. Весовой коэффициент мероприятия – 1.	
Защита отчёта по лабораторной работе	Защита лабораторной работы осуществляется индивидуально. Студент представляет результат выполнения лабораторной работы из методических указаний по выбору преподавателя и представляет отчёт. Оценивается качество оформления, своевременность выполнения работы. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей: - правильность выполнения работы, если есть недочёты, то из оценки вычитается 1 балл; - своевременность сдачи и качество выполнения отчёта, за каждую неделю просрочки или недочёт в отчёте из оценки вычитается 1балл. Максимальное количество баллов за одну работу – 6. Всего в течение семестра предусмотрено 4 рейтинговых лабораторных работы. Весовой коэффициент каждого мероприятия (за каждую лабораторную работу) – 1. Общее количество за лабораторные работы – 24.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 % Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %
Экзамен	На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Отлично: Величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: Величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 % Если рейтинг обучающегося по дисциплине ниже 60%, то он сдает экзамен с целью возможного повышения рейтинга. По результатам сдачи экзамена	Отлично: Общий рейтинг обучающегося >85% Хорошо: Общий рейтинг обучающегося между 75% и 84% Удовлетворительно: Общий рейтинг обучающегося между 60% и 74% Неудовлетворительно: Не выполнен план по дисциплине

	выставляется оценка, которая учитывается при определении рейтинга. Формат экзамена -- ответы на вопросы из билетов. Каждый вопрос добавляет 10% в общий рейтинг	
Задание на допуск	Защита и выполнение этой практической работы осуществляется индивидуально. Студент представляет результат выполнения одного варианта практического задания из указанного списка и отвечает на вопрос преподавателя. Оценивается качество оформления, своевременность выполнения работы и ответы на вопросы (задаётся 1 вопрос). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей: - правильность выполнения работы, если есть недочёты, то из оценки вычитается 1 балл. Максимальное количество баллов за эту работу – 15. Весовой коэффициент мероприятия – 1.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 % Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %
Экзамен	Тест	Отлично: от 36 до 42 правильных ответов Хорошо: от 29 до 35 правильных ответов Удовлетворительно: от 22 до 28 правильных ответов Неудовлетворительно: до 21 правильного ответа

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Защита отчёта по практической работе	
Бонусные баллы за участие в мероприятиях по информационной безопасности	
Бонусные баллы за выполнение практических 1-3	
Доклад по теме на выбор из списка	
Защита отчёта по лабораторной работе	
Экзамен	15 Межсетевые экраны и средства обнаружения вторжений. Сегментирование. Аутентификация, авторизация, аудит. 7 Протоколы разрешения адресов ARP, RARP. Алгоритмы маршрутизации, их характеристика. Протоколы и алгоритмы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, NLSP, EGP, BGP) 2 Критерии классификации сетей ЭВМ. Характеристики сетей ЭВМ 5 Методы коммутации. Методы доступа к разделяемой среде.

	Угрозы безопасности информации, передаваемой в сетях ЭВМ, на физическом и канальном уровнях. 6 Сетевой уровень построения сетей ЭВМ. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях 1 Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Понятие сети ЭВМ. Этапы развития сетей ЭВМ 8 Транспортные услуги и технологии глобальных сетей. Технология MPLS 11 Технология VLAN. Угрозы безопасности информации, передаваемой в локальных сетях ЭВМ. Методы их нейтрализации 13 Классификации угроз безопасности телекоммуникационных сетей 9 Сетевые службы и средства управления 14 Классификация методов защиты. Основные технологии обеспечения безопасности в сети 10 Средства контроля внешнего периметра сети. Средства контроля доступа к сетевым службам. Средства активного аудита сетей ЭВМ. Протокол SNMP 3 Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей ЭВМ. Модель ISO OSI. Технологии обеспечения безопасности в сетях ЭВМ 4 Практические отличия реализации стека TCP/IP от эталонной модели ISO OSI. 12 Протоколы VRRP/HSRP. Основы кластерных решений. DM VPN (Cisco VPN) как пример динамически организующейся сети 16 Криптографические средства защиты информации в сетях ЭВМ. Виртуальные частные сети. Протокол SSL
Задание на допуск	1. Настройка взаимодействия (межсетевого экранирования) между тремя виртуальными машинами с заранее настроенными сервисами 2. Настройка защищённой сети ViPNet 3. Настройка средства обнаружения вторжений, создание и демонстрация работы тестовых правил
Экзамен	Итоговые тесты.docx

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы Текст учеб. для вузов по направлению 552800 "Информатика и вычисл. техника" и по специальностям 220100 "Вычисл. машины, комплексы, системы и сети", 220200 "Автоматизир. системы обработки информ. и упр.", 220400 "Програм. обеспечение вычисл. техники и автоматизир. систем" В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. и др.: Питер, 2007. - 957 с. ил.
2. Олифер, В. Г. Компьютерные сети: Принципы, технологии, протоколы [Текст] Учеб. пособие по направлению "Информатика и вычисл. техника" и специальностям... В. Г. Олифер, Н. А. Олифер. - СПб. и др.: Питер, 2001. - 668 с. ил.

б) дополнительная литература:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] учеб. пособие для вузов по направлению "Информатика и вычисл. техника" и по специальности "Вычисл. машины, комплексы, системы и сети" и др. В. Г. Олифер, Н. А. Олифер. - 5-е изд. - СПб. и др.: Питер, 2018. - 991 с. ил.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

г) методические указания для студентов по освоению дисциплины:

1. Скурлаев С.В. Безопасность сетей ЭВМ: методические рекомендации к практическим занятиям.

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с. — Режим доступа: http://e.lanbook.com/book/3032 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	ГОСТ Р ИСО/МЭК 7498-1-99	Консультант плюс	Интернет / Свободный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. -Oracle VirtualBox(бессрочно)

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	904 (3б)	Компьютеры, включая системный блок, монитор, клавиатуру, мышь, проводные и беспроводные сетевые адаптеры. Шкаф с сетевым оборудованием Cisco. Коммутаторы Cisco Catalyst 2950. Маршрутизаторы

		Cisco Router 2600. Беспроводные маршрутизаторы D-Link DIR-620, DIR-615, DIR-300. Межсетевые экраны Cisco PIX 501 Firewall, IPTables (программный, в составе ОС). Системы обнаружения вторжений Cisco IPS 4255, Snort и Surricata (программные, в составе ОС). Анализаторы сетевого трафика (снифферы) tcpdump и Wireshark (программные, в составе ОС). Анализаторы сети nmap/zenmap (программный, в составе ОС). Средства шифрования трафика openssl и OpenVPN (программные, в составе ОС). ПО: ОС Fedora, эмулятор сетевых устройств Cisco Packet Tracer, браузер Mozilla Firefox, IPTables, Snort, Surricata, tcpdump, Wireshark, nmap/zenmap, openssl, OpenVPN, Oracle VM VirtualBox
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Экзамен	904 (3б)	Компьютеры, включая системный блок, монитор, клавиатуру, мышь, проводные и беспроводные сетевые адаптеры. Шкаф с сетевым оборудованием Cisco. Коммутаторы Cisco Catalyst 2950. Маршрутизаторы Cisco Router 2600. Беспроводные маршрутизаторы D-Link DIR-620, DIR-615, DIR-300. Межсетевые экраны Cisco PIX 501 Firewall, IPTables (программный, в составе ОС). Системы обнаружения вторжений Cisco IPS 4255, Snort и Surricata (программные, в составе ОС). Анализаторы сетевого трафика (снифферы) tcpdump и Wireshark (программные, в составе ОС). Анализаторы сети nmap/zenmap (программный, в составе ОС). Средства шифрования трафика openssl и OpenVPN (программные, в составе ОС). ПО: ОС Fedora, эмулятор сетевых устройств Cisco Packet Tracer, браузер Mozilla Firefox, IPTables, Snort, Surricata, tcpdump, Wireshark, nmap/zenmap, openssl, OpenVPN, Oracle VM VirtualBox
Лабораторные занятия	904 (3б)	Компьютеры, включая системный блок, монитор, клавиатуру, мышь, проводные и беспроводные сетевые адаптеры. Шкаф с сетевым оборудованием Cisco. Коммутаторы Cisco Catalyst 2950. Маршрутизаторы Cisco Router 2600. Беспроводные маршрутизаторы D-Link DIR-620, DIR-615, DIR-300. Межсетевые экраны Cisco PIX 501 Firewall, IPTables (программный, в составе ОС). Системы обнаружения вторжений Cisco IPS 4255, Snort и Surricata (программные, в составе ОС). Анализаторы сетевого трафика (снифферы) tcpdump и Wireshark (программные, в составе ОС). Анализаторы сети nmap/zenmap (программный, в составе ОС). Средства шифрования трафика openssl и OpenVPN (программные, в составе ОС). ПО: ОС Fedora, эмулятор сетевых устройств Cisco Packet Tracer, браузер Mozilla Firefox, IPTables, Snort, Surricata, tcpdump, Wireshark, nmap/zenmap, openssl, OpenVPN, Oracle VM VirtualBox