

**МИНОБРНАУКИ РОССИИ**  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»**  
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ  
Директор института энергетике,  
информационных технологий и  
управляющих систем

Белоусов А.В.

« 20 » \_\_\_\_\_ 2021 г.

**РАБОЧАЯ ПРОГРАММА**  
дисциплины

**Безопасность сетей ЭВМ**

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетике, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и  
автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: \_\_\_\_\_ (Буханов Д.Г.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

« 14 » \_\_\_\_\_ 05 \_\_\_\_\_ 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент \_\_\_\_\_ (Поляков В.М.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем  
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент \_\_\_\_\_ (Поляков В.М.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

« 14 » \_\_\_\_\_ 05 \_\_\_\_\_ 2021 г.

Рабочая программа одобрена методической комиссией института

« 20 » \_\_\_\_\_ 05 \_\_\_\_\_ 2021 г., протокол № 9

Председатель к.т.н., доцент \_\_\_\_\_ (Семернин А.Н.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

## 1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
	ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.3 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные принципы взаимодействия операционных систем с компьютерными сетями;</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать и администрировать компьютерные сети;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности</li> </ul>
	ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1 Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем	<p>Знать:</p> <ul style="list-style-type: none"> <li>– алгоритмы работы основных сетевых протоколов;</li> <li>– принципы построения и функционирования, принципы реализации современных локальных и глобальных компьютерных сетей.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– выявлять архитектурные ошибки в комплексе обеспечения безопасности компьютерных сетей;</li> <li>– эффективно использовать различные методы и средства защиты информации для компьютерных сетей;</li> <li>– проводить мониторинг угроз безопасности компьютерных сетей.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>навыками использования программных средств мониторинга сетевой активности</li> </ul>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

**2.1. Компетенция ОПК-9.** Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Данная компетенция формируется следующими дисциплинами.

№	Наименование дисциплины (модуля)
1.	Безопасность систем баз данных
2.	Безопасность операционных систем
3.	Безопасность сетей ЭВМ
4.	Квантовые вычисления и квантовая криптография
5.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

**2.2 Компетенция ОПК-12.** Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

Данная компетенция формируется следующими дисциплинами.

№	Наименование дисциплины
1.	Сети и системы передачи данных
2.	Базы данных
3.	Архитектура вычислительных систем
4.	Операционные системы
5.	Безопасность систем баз данных
6.	Безопасность операционных систем
7.	Безопасность сетей ЭВМ
8.	Производственная технологическая практика
9.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

### 3. ОБЪЁМ ДИСЦИПЛИНЫ

3.1. Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часа.

Форма промежуточной аттестации дифференцированный зачет.

Вид учебной работы	Всего часов	Семестр № 7
<b>Общая трудоемкость дисциплины, час</b>	<b>144</b>	<b>144</b>
<b>Контактная работа (аудиторные занятия), в т.ч.:</b>	<b>71</b>	<b>71</b>
лекции	34	34
лабораторные	34	34
практические	-	-
групповые консультации в период теоретического обучения и промежуточной аттестации	3	3
<b>Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:</b>	<b>73</b>	<b>73</b>
Курсовой проект		
Курсовая работа		
Расчетно-графическое задание		
Индивидуальное домашнее задание		
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	73	73
Дифференцированный зачёт	-	-

## 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 4.1. Наименование тем, их содержание и объем

№ п/п	Наименование раздела (модуля)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа на подготовку к аудиторным занятиям
1	2	3	4	5	6
семестр № 1					
1.	<b>Введение. Информационные угрозы.</b> Источники и последствия угроз ИБ. Объекты сетевой безопасности. Основы организации и функционирования сетей ЭВМ.	4		4	8
2.	<b>Физический и каналный уровень построения сетей ЭВМ.</b> Сетевые коллизии сетей Ethernet и их влияние на физический уровень.	3		3	7
3.	<b>Технологии построения локальных сетей ЭВМ.</b> Сетевые топологии и их применение. Коммуникационное оборудование и их применение. Виртуальные локальные сети.	4		4	9
4.	<b>Сетевой уровень построения сетей ЭВМ.</b> Проблемы маршрутизации. ИБ сетевого уровня. IPv4, IPv6. Сниффинг и спуфинг в компьютерных сетях. Межсетевые экраны	4		4	9
5.	<b>Безопасность транспортной подсистемы сетей ЭВМ.</b> Туннелирование. Транспортные шлюзы. Виртуальные частные сети. OpenVPN. Проблемы создания безопасного канала передачи данных. Системы трансляции адресов и портов.	6		6	11
6.	<b>Безопасность уровня приложений.</b> Управление сетями ЭВМ. Программные системы обнаружения атак и вторжений. Snort. Уязвимости в сетевых приложениях.	4		4	9
7.	<b>Программно-технические средства защиты сетей ЭВМ.</b> Программно-аппаратные системы обнаружения атак и вторжений. Cisco ASA 5000 серии.	5		5	10
8.	<b>Безопасность беспроводных сетей.</b> WEP, WPA, WPA2.WPS Анализ безопасности Wi-Fi с использованием kali-linux.	4		4	10
	ВСЕГО	34		34	73

## 4.2. Содержание практических (семинарских) занятий.

Не предусмотрено учебным планом.

## 4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторной работы	К-во часов	Самостоятельная работа на подготовку к аудиторным занятиям
1.	<b>Введение. Информационные угрозы.</b> Источники и последствия угроз ИБ. Объекты сетевой безопасности. Основы организации и функционирования сетей ЭВМ.	Сетевая настройка рабочей станции на базе Linux систем.	3	5
2.	<b>Физический и канальный уровень построения сетей ЭВМ.</b> Сетевые коллизии сетей Ethernet и их влияние на физический уровень.	Аудит безопасности протокола SNMP.	3	6
3.	<b>Технологии построения локальных сетей ЭВМ.</b> Сетевые топологии и их применение. Коммуникационное оборудование и их применение. Виртуальные локальные сети.	Виртуальные локальные сети и IEEE 802.1.	4	7
4.	<b>Сетевой уровень построения сетей ЭВМ.</b> Проблемы маршрутизации. ИБ сетевого уровня. IPv4, IPv6. Сниффинг и спуфинг в компьютерных сетях. Межсетевые экраны.	Протокол SSH.	4	7
5.	<b>Безопасность транспортной подсистемы сетей ЭВМ.</b> Туннелирование. Транспортные шлюзы. Виртуальные частные сети. OpenVPN. Проблемы создания безопасного канала передачи данных. Системы трансляции адресов и портов.	Базовые механизмы безопасности коммутаторов.	5	7
6.	<b>Безопасность уровня приложений.</b> Управление сетями ЭВМ. Программные системы обнаружения атак и вторжений. Snort. Уязвимости в сетевых приложениях.	Списки контроля доступа ACL.	5	8
7.	<b>Программно-технические средства защиты сетей ЭВМ.</b> Программно-аппаратные системы обнаружения атак и вторжений. Cisco ASA 5000 серии.	Знакомство с локальным брандмауэром iptables.	4	6
8.	<b>Безопасность беспроводных сетей.</b> WEP, WPA, WPA2, WPS. Анализ безопасности Wi-Fi с использованием kali-linux.	Безопасность сетей WiFi.	4	6
9.	Разделы 1-8	Технология Network Address Translation.	2	4
ИТОГО:			34	56

#### 4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

#### 4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом

### 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

#### 5.1. Реализация компетенций

**Компетенция ОПК-9.** Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-9.3 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Устный опрос, работа на лабораторных занятиях, зачет

**Компетенция ОПК-12.** Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-12.1 Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем	Устный опрос, работа на лабораторных занятиях, зачет

#### 5.2. Типовые контрольные задания для промежуточной аттестации

##### 5.2.1. Перечень контрольных вопросов (типовых заданий)

для дифференцированного зачета



№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Введение. Информационные угрозы (ОПК-9.3)	<p>Виды компьютерных сетей и их назначение</p> <p>Последствия и угрозы информационное безопасности</p> <p>Объекты информационной безопасности</p> <p>Основные компоненты информационной безопасности</p> <p>Многоаспектная классификация ЛВС и классификационные группы</p> <p>Особенности построения, достоинства и недостатки одноранговых ЛВС и серверных ЛВС</p> <p>Классификация компьютерных сетей по типу</p> <p>Сетевая модель OSI. Задачи и функции по уровням модели. Понятие стека протоколов. Основные стеки. Соответствие протоколов модели OSI</p>
2	Физический и канальный уровень построения сетей ЭВМ (ОПК-9.3)	<p>Методы доступа к каналам связи сети и их отличительные особенности</p> <p>Характеристика сетевой технологии IEEE 802.1/Ethernet и её разновидностей</p> <p>Характеристика сетевой технологии IEEE 802.1/TokenRing</p> <p>Краткая характеристика сетевой технологии ARCNET</p> <p>Краткая характеристика сетевой технологии FDDI</p> <p>Физический уровень: функции, протоколы</p> <p>Канальный уровень: функции, протоколы</p> <p>Протоколы разрешения адресов ARP, RARP</p> <p>Назначение протокола STP и его разновидностей</p>
3	Технологии построения локальных сетей ЭВМ (ОПК-9.3)	<p>Устройства межсетевого интерфейса</p> <p>Основные рейтинговые параметры ЛВС</p> <p>Интернет. Основные принципы работы и протоколы</p> <p>Общие проблемы информационной безопасности</p> <p>VLAN, тегированный трафик</p> <p>Протокол 802.1q</p> <p>Аспекты безопасности при сегментации трафика</p>
4	Сетевой уровень построения сетей ЭВМ (ОПК-9.3)	<p>Основные протоколы, используемые в Интернет на сетевом уровне.</p> <p>Проблемы использования этих протоколов</p> <p>Системы адресации, используемые в сети Интернет</p> <p>Сетевая модель OSI. Сетевой уровень: функции, протоколы</p> <p>Стек протоколов TCP/IP</p> <p>Алгоритмы маршрутизации, их характеристика</p> <p>Спуфинг и снифинг. Механизмы их реализаций</p> <p>WinPCap, WinDivert. Wireshark</p> <p>Пояснить типовой сценарий использования LibPcap и WinPCap для работы с портами сетевого адаптера</p> <p>Указать порядок действий при захвате пакетов с LibPcap</p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
5	Безопасность транспортной подсистемы сетей ЭВМ (ОПК-12.1)	<p>Основные протоколы, используемые в Интернет на транспортном уровне</p> <p>Задачи транспортного уровня</p> <p>Проблемы использования протоколов транспортного уровня</p> <p>Сетевая модель OSI. Транспортный уровень: функции, протоколы</p> <p>Туннелирование, виртуальные частные сети</p> <p>Провести сравнительный анализ различных вариантов построения виртуальных сетей</p> <p>Ассиметричные и симметричные алгоритмы шифрования в компьютерных сетях</p> <p>Указать надежные и скомпрометированные алгоритмы шифрования, применяемые в компьютерных сетях</p>
6	Безопасность уровня приложений (ОПК-12.1)	<p>Основные протоколы, используемые в Интернет на прикладном уровне</p> <p>Проблемы использования протоколов прикладного уровня</p> <p>Характеристика базовых пользовательских технологий: HTTP, FTP, SSH</p> <p>Утилиты для создания SSH-канала на основе разных ОС</p> <p>Порядок применения PUTTy для установления SSH-соединения</p> <p>Сеансовый уровень: функции, протоколы. Сетевая модель OSI</p> <p>Представительский уровень: функции, протоколы. Сетевая модель OSI</p> <p>Прикладной уровень: функции, протоколы</p> <p>Протоколы управления SNMP и CMIP. Проксирование трафика</p>
7	Программно-технические средства защиты сетей ЭВМ (ОПК-12.1)	<p>Классификации СОАВ. Существующие методы классификации данных в современных СОВ</p> <p>Методы обнаружения ошибок</p> <p>Методы коррекции ошибок</p> <p>Угрозы безопасности информации, передаваемой в локальных сетях ЭВМ</p> <p>Средства контроля внешнего периметра сети</p> <p>Отличия между СОВ и СПВ. Примеры распространенных СОВ и СПВ</p> <p>Системы трансляции адресов и портов(NAT). Виды. Общая характеристика. Назначение</p> <p>Элементы повешения безопасности систем Dallas Lock</p>
8	Безопасность беспроводных сетей (ОПК-12.1)	<p>Беспроводные технологии передачи данных (Bluetooth, WiFi и т.д.)</p> <p>Алгоритмы обеспечения безопасности беспроводных технологий передачи данных</p> <p>Алгоритмы шифрования WiFi. Их достоинства и недостатки</p> <p>Основные классы угроз для беспроводных сегментов сетей</p> <p>Анализ безопасности существующих протоколов криптографической защиты передачи данных</p> <p>Ad-hoc. Manet</p> <p>Алгоритмы безопасной маршрутизации</p>

### 5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

*Текущий контроль* осуществляется в течение семестра в форме выполнения и защиты лабораторных работ.

Защита лабораторных работ проводится в форме устного опроса студента по выполненной работе и направлена на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы.

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Введение. Информационные угрозы (ОПК-9.3)	Виды компьютерных сетей и их назначение Последствия и угрозы информационное безопасности Объекты информационной безопасности Многоаспектная классификация ЛВС и классификационные группы Особенности построения, достоинства и недостатки одноранговых ЛВС и серверных ЛВС Классификация компьютерных сетей по типу Сетевая модель OSI. Задачи и функции по уровням модели. Понятие стека протоколов. Основные стеки. Соответствие протоколов модели OSI
2.	Физический и канальный уровень построения сетей ЭВМ (ОПК-9.3)	Методы доступа к каналам связи сети и их отличительные особенности Характеристика сетевой технологии IEEE 802.1/Ethernet и её разновидностей Характеристика сетевой технологии IEEE 802.1/TokenRing Краткая характеристика сетевой технологии ARCNET Краткая характеристика сетевой технологии FDDI Физический уровень: функции, протоколы Канальный уровень: функции, протоколы Протоколы разрешения адресов ARP, RARP Назначение протокола STP и его разновидностей
3.	Технологии построения локальных сетей ЭВМ (ОПК-9.3)	Устройства межсетевого интерфейса Основные рейтинговые параметры ЛВС Интернет. Основные принципы работы и протоколы Общие проблемы информационной безопасности VLAN, тегированный трафик Протокол 802.1q Аспекты безопасности при сегментации трафика
4.	Сетевой уровень построения сетей ЭВМ (ОПК-9.3)	Основные протоколы, используемые в Интернет на сетевом уровне. Проблемы использования этих протоколов Системы адресации, используемые в сети Интернет Сетевая модель OSI. Сетевой уровень: функции, протоколы Стек протоколов TCP/IP Алгоритмы маршрутизации, их характеристика Спуфинг и снифинг. Механизмы их реализаций WinPCap, WinDivert. Wireshark
5.	Безопасность транспортной подсистемы сетей ЭВМ (ОПК-12.1)	Основные протоколы, используемые в Интернет на транспортном уровне Проблемы использования протоколов транспортного уровня Сетевая модель OSI. Транспортный уровень: функции, протоколы Туннелирование, виртуальные частные сети Ассиметричные и симметричные алгоритмы шифрования в компьютерных сетях

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
6.	Безопасность уровня приложений (ОПК-12.1)	Основные протоколы, используемые в Интернет на прикладном уровне Проблемы использования протоколов прикладного уровня Характеристика базовых пользовательских технологий: HTTP, FTP, SSH Сеансовый уровень: функции, протоколы. Сетевая модель OSI Представительский уровень: функции, протоколы. Сетевая модель OSI Прикладной уровень: функции, протоколы Протоколы управления SNMP и CMIP. Проксирование трафика
7.	Программно-технические средства защиты сетей ЭВМ (ОПК-12.1)	Классификации СОАВ. Существующие методы классификации данных в современных СОВ Методы обнаружения ошибок Методы коррекции ошибок Угрозы безопасности информации, передаваемой в локальных сетях ЭВМ Средства контроля внешнего периметра сети Системы трансляции адресов и портов(NAT). Виды. Общая характеристика. Назначение Элементы повешения безопасности систем Dallas Lock
8.	Безопасность беспроводных сетей (ОПК-12.1)	Беспроводные технологии передачи данных (Bluetooth, WiFi и т.д.) Алгоритмы обеспечения безопасности беспроводных технологий передачи данных Анализ безопасности существующих протоколов криптографической защиты передачи данных Ad-hoc. Manet Алгоритмы безопасной маршрутизации

После изучения каждой темы раздела для закрепления изученного материала проводится **тестирование**. Тестирование проходит с использованием системы MyTest. Задание теста включает 10 вопросов. Время выполнения заданий теста составляет 10 минут.

### Тестовые задание по темам

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Введение. Информационные угрозы (ОПК-9.3)	<b>Задание 1</b> Основные объекты защиты при обеспечении информационной безопасности <i>Выберите один из 3 вариантов ответа:</i> 1) информация, ресурсные, физические и пользовательские объекты 2) информация, физические и пользовательские объекты 3) процессы информационного обмена, информационные ресурсы <b>Задание 2</b> Укажите недостатки одноранговых ЛВС

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p><i>Выберите несколько из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) необходимость помнить столько паролей, сколько имеется разделенных ресурсов</li> <li>2) необходимость производить резервное копирование отдельно на каждом компьютере, чтобы защитить все совместные данные</li> <li>3) трудоемкость конфигурирования</li> <li>4) невозможность пользователям полностью контролировать свои собственные ресурсы</li> </ol> <p><b><u>Задание 3</u></b> Классификация компьютерных сетей по типу <i>Выберите один из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) LAN, кампусные, MAN и WAN</li> <li>2) LAN, MAN и WAN</li> <li>3) LAN и WAN</li> <li>4) LAN, MAN и WAN. Кампусные сети – частный случай, занимают промежуточное положение между LAN и MAN</li> </ol> <p><b><u>Задание 4</u></b> Признаки серверной ЛВС <i>Выберите несколько из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) централизованное управления учетными записями пользователей, безопасностью и доступом</li> <li>2) недостаточная скорость выполнения прикладных задач в сети</li> <li>3) возможность для пользователей получить доступ ко всем ресурсам, к которым имеют праваЮ имея только один пароль</li> <li>4) разделение серверных и клиентских ресурсов</li> </ol> <p><b><u>Задание 5</u></b> Последствия реализованной информационной угрозы <i>Выберите несколько из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) подмена, хищение и уничтожение информации</li> <li>2) прямые и косвенные убытки</li> <li>3) получение доступа к ресурсам целевой сетевой инфраструктуры</li> <li>4) компрометация защитных механизмов и протоколов</li> </ol> <p><b><u>Задание 6</u></b> Периметр сети определяется <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) пограничными коммутационными устройствами</li> <li>2) физическими кондициями сети</li> <li>3) логической структурой сети</li> </ol> <p><b><u>Задание 7</u></b> Реализация и планирование АРТ осуществляется <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) с учетом известных уязвимостей алгоритмов и средств защиты</li> <li>2) на основе предварительного изучения особенностей целевой сети</li> <li>3) с использованием средств социальной инженерии</li> </ol> <p><b><u>Задание 8</u></b> Укажите недостатки серверной ЛВС <i>Выберите один из 3 вариантов ответа:</i></p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>1) выход из строя сервера может привести к неработоспособности сети (невозможности решать прикладные задачи)</p> <p>2) выход из строя сервера может привести к неработоспособности сети (прекращению взаимодействия между узлами клиентов)</p> <p>3) необходимость постоянного мониторинга распределения ресурсов</p> <p><b><u>Задание 9</u></b> Необходимость перехода ЛВС к серверному типу возникает по мере _____ <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) увеличения количества клиентских узлов</li> <li>2) роста количества пользователей при фиксированном количестве узлов</li> <li>3) усложнения топологии сети</li> </ol> <p><b><u>Задание 10</u></b> Для кампусных сетей характерно <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) наличие как вертикальных, так и горизонтальных высокоскоростных подсистем</li> <li>2) наличие горизонтальных высокоскоростных подсистем</li> <li>3) отсутствие четкой иерархии как в плане разделения на подсистемы вертикального и горизонтального ориентирования, так и в плане скоростей</li> </ol>
2	Физический и канальный уровень построения сетей ЭВМ (ОПК-9.3)	<p><b><u>Задание 1</u></b> Маркерный метод доступа к среде передачи предполагает <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) прослушивание несущей частоты (carrier-sense)</li> <li>2) захват и удержание специализированного пакета, передаваемого в сети</li> <li>3) получение права начать передачу с учетом приоритетности запроса</li> </ol> <p><b><u>Задание 2</u></b> Возникновение коллизий в сетях Ethernet вызвано <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) попыткой одновременной передачи пакета несколькими станциями</li> <li>2) переполнением буфера коммутационного устройства</li> <li>3) достижением интенсивностью трафика верхнего предела пропускной способности сети</li> </ol> <p><b><u>Задание 3</u></b> Расстояние между устройствами сети Ethernet не должно превышать <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) 128 м</li> <li>2) 100 м</li> <li>3) 200 м</li> </ol> <p><b><u>Задание 4</u></b> Укажите, какие протоколы относятся к канальному уровню <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) Ethernet, Token Ring, FDDI</li> <li>2) Ethernet, FDDI, ICMP</li> </ol>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>3) Token Ring, FDDI</p> <p><b><u>Задание 5</u></b> FDDI работает в режиме <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) двойного кольца</li> <li>2) одиночного кольца с дублирующим кольцом</li> <li>3) переключения колец</li> </ol> <p><b><u>Задание 6</u></b> Сети Token Ring работают по принципу <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) общей шины, несмотря на иную топологию (ненаправленное кольцо)</li> <li>2) направленного кольца</li> <li>3) кольца с возможностью смены направления обмена данными</li> </ol> <p><b><u>Задание 7</u></b> На физическом уровне модели OSI определяются <i>Выберите несколько из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) характеристики электрических сигналов, передающих дискретную информацию</li> <li>2) доступность среды передачи</li> <li>3) скорость передачи сигналов</li> </ol> <p><b><u>Задание 8</u></b> Протокол STP обеспечивает <i>Выберите несколько из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) передачу данных между устройствами в режиме точка-точка или точка-многоточка</li> <li>2) устранение петель в топологии произвольной сети Ethernet</li> <li>3) передачу последовательности пакетов через физический канал, искажения в котором вызывают ошибки в передаваемых данных</li> </ol> <p><b><u>Задание 9</u></b> ARCNET использует для доступа к среде передачи <i>Выберите несколько из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) маркерный метод доступа</li> <li>2) произвольный метод доступа</li> <li>3) доступ по приоритетному требованию</li> </ol> <p><b><u>Задание 10</u></b> Активные и пассивные повторители характерны для сетей <i>Выберите несколько из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) TokenRing</li> <li>2) ARCNET</li> <li>3) Ethernet</li> </ol>
3	Технологии построения локальных сетей ЭВМ (ОПК-9.3)	<p><b><u>Задание 1</u></b> Какие из перечисленных устройств работают на канальном уровне модели ЭМВОС <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) повторители</li> <li>2) мосты</li> </ol>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>3) шлюзы</p> <p><b><u>Задание 2</u></b>          Главное назначение устройства межсетевого интерфейса  <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) объединение сетей</li> <li>2) физическая сегментация единой сети</li> <li>3) создание физической иерархии сети</li> </ol> <p><b><u>Задание 3</u></b>          Общие проблемы информационной безопасности сводятся к необходимости обеспечения  <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) целостности, конфиденциальности и доступности информации для легитимных пользователей</li> <li>2) целостности, конфиденциальности и доступности информации</li> <li>3) достоверности, конфиденциальности и доступности информации для легитимных пользователей</li> </ol> <p><b><u>Задание 4</u></b>          К основным рейтинговым параметрам ЛВС относятся  <i>Выберите несколько из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) ранговый тип сети</li> <li>2) уровень защищенности сети</li> <li>3) надежность сети</li> <li>4) используемый тип физической среды</li> </ol> <p><b><u>Задание 5</u></b>          Для построения VLAN не используются подходы на основе  <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) тегированного трафика</li> <li>2) использования MAC-адресов</li> <li>3) группировки узлов в виртуальную сеть по параметру hostname</li> </ol> <p><b><u>Задание 6</u></b>          Какое количество VLAN позволяет построить создать стандарт 802.1Q в одной сети  <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) 4094</li> <li>2) 4096</li> <li>3) 1024</li> </ol> <p><b><u>Задание 7</u></b>          Тегированный кадр содержит  <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) поле в заголовке с указанием номера сети</li> <li>2) поле в конце с указанием номера сети</li> <li>3) дополнительное поле в заголовке для указания номера сети</li> </ol> <p><b><u>Задание 8</u></b>          Какой из протоколов при обмене информацией использует TCP/IP  <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) HTTP</li> <li>2) FTP</li> <li>3) UDP</li> </ol> <p><b><u>Задание 9</u></b>          Безопасность сети путей сегментации обеспечивается за счет  <i>Выберите один из 3 вариантов ответа:</i></p>



№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>1) изоляции трафика различных групп  2) ограничения пространства, в котором могут возникать инциденты, связанные со снижением безопасности  3) ограничения пространства, в котором могут возникать технические инциденты, а также инциденты, связанные со снижением безопасности</p> <p><b><u>Задание 10</u></b>  Минимальный идентификатор созданной виртуальной сети будет равен  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) 0  2) 1  3) 2</p>
4	Сетевой уровень построения сетей ЭВМ (ОПК-9.3)	<p><b><u>Задание 1</u></b>  Укажите системы адресации, используемые в сети Интернет  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) IP, система доменных имен DNS  2) IP и MAC-адресация  3) система DNS с указанием домена первого уровня</p> <p><b><u>Задание 2</u></b>  Что из перечисленного справедливо для алгоритма Дейкстры  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) не гарантирует выбор оптимального маршрута, но достаточно эффективен и отличается продуктивностью  2) гарантирует выбор оптимального маршрута, отличается продуктивностью  3) гарантирует выбор оптимального маршрута, недостатком является органичное быстрое действие</p> <p><b><u>Задание 3</u></b>  Укажите особенность работы протокола OSPF  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) функционирует в рамках TCP/IP  2) функционирует в рамках IPX/SPX  3) работает с каждым из указанных стеков</p> <p><b><u>Задание 4</u></b>  Какие недостатки свойственны протоколу RIP  <i>Выберите несколько из 4 вариантов ответа:</i></p> <p>1) возникновение петель  2) использует неэффективные механизмы адаптации  3) эффективен только для небольших сетей  3) не подходит для обработки неоднородного трафика</p> <p><b><u>Задание 5</u></b>  Эффективным механизмом защиты от спуфинга является  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) использование инструментов для аутентификации источника или назначения сообщения  2) применение межсетевых экранов  3) применение технологий глубокого анализа пакетов</p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p><b><u>Задание 6</u></b> Работа сниффера пакетов основана на <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) использовании сетевой карты, работающей в неразборчивом режиме</li> <li>2) использовании порта коммутатора, работающего в неразборчивом режиме</li> <li>3) атаке МИМ</li> </ol> <p><b><u>Задание 7</u></b> Библиотека PCap содержит <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) набор функции для управления сетевым адаптером</li> <li>2) драйвер устройства захвата пакетов, низкоуровневую динамическую библиотеку и статическую библиотека высокого уровня</li> <li>3) пакет программных модулей для приема трафика с порта ближайшего коммутатора</li> </ol> <p><b><u>Задание 8</u></b> PCap взаимодействует с данными <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) через стек протоколов ОС</li> <li>2) напрямую, минуя стек протоколов ОС</li> <li>3) любым из указанных способов</li> </ol> <p><b><u>Задание 9</u></b> Укажите, какие протоколы относятся к сетевому уровню <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) ARP, ICMP, IPSec, IPX</li> <li>2) IPv4/IPv6, ARP, ICMP, NCP</li> <li>3) ARP, ICMP, IPSec, DNS, IPv4/IPv6</li> </ol> <p><b><u>Задание 10</u></b> Ограничения Wireshark по захвату пакетов обусловлены <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) версией библиотеки PCap</li> <li>2) особенностями аппаратного обеспечения</li> <li>3) правами пользователя в системе</li> </ol>
5	Безопасность транспортной подсистемы сетей ЭВМ (ОПК-12.1)	<p><b><u>Задание 1</u></b> Какой из указанных протоколов транспортного уровня является неосновным (подпротоколом) <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) UDP</li> <li>2) RUDP</li> <li>3) TCP</li> </ol> <p><b><u>Задание 2</u></b> Защищенные VPN строятся с использованием <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) IPSec, OpenVPN, PPTP</li> <li>2) MPLS и L2TP</li> <li>3) IPSec, MPLS, L2TP</li> </ol>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p><b><u>Задание 3</u></b> Какие виды соединений обеспечивает VPN <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) узел-узел, узел-сеть, сеть-сеть</li> <li>2) узел-сеть, сеть-сеть</li> <li>3) узел-узел, сеть-сеть</li> </ol> <p><b><u>Задание 4</u></b> Для защиты данных протокол IPSec использует <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) стандартизованные алгоритмы шифрования и хеширования</li> <li>2) стандартизованные алгоритмы шифрования и хеширования, а также алгоритмы, добавленные производителями продуктов</li> <li>3) стандартизованные алгоритмы шифрования, а также алгоритмы, добавленные производителями продуктов; хеширование выполняется на основе стандартизованных алгоритмов</li> </ol> <p><b><u>Задание 5</u></b> Укажите основные функции транспортного уровня OSI <i>Выберите несколько из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) обеспечивает приложениям или верхним уровням стека передачу данных с той степенью надежности, которая им требуется</li> <li>2) обеспечивает адресацию программных портов данных приложений</li> <li>3) контролирует работу сетевого уровня</li> <li>3) существенно расширяет функционал сетевого уровня</li> </ol> <p><b><u>Задание 6</u></b> Шифрование туннелированного трафика осуществляется в основном <i>Выберите один из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) симметричными алгоритмами</li> <li>2) асимметричными алгоритмами</li> <li>3) с использованием комбинации алгоритмов любой архитектуры совместно с хешированием</li> <li>3) симметричными алгоритмами с применением хеширования</li> </ol> <p><b><u>Задание 7</u></b> К недостаткам безопасности UDP относятся <i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) возможность замены/удаления пакетов злоумышленником</li> <li>2) отсутствие стандартных механизмов шифрования</li> <li>3) невозможность проверки подлинности пакета</li> </ol> <p><b><u>Задание 8</u></b> Что из указанного может использоваться для защиты TCP/IP от перехвата? <i>Выберите несколько из 3 вариантов ответа:</i></p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>1) выявление устройств, чьи порты работают в неразборчивом режиме  2) туннелирование  3) шифрование всего TCP/IP трафика</p> <p><b><u>Задание 9</u></b>  На транспортном уровне осуществляются взаимодействия вида  <i>Выберите один из 3 вариантов ответа:</i>  1) точка-многоточка  2) точка-точка  3) оба вида</p> <p><b><u>Задание 10</u></b>  Разница между UDP и UDP lite состоит в том, что  <i>Выберите один из 3 вариантов ответа:</i>  1) UDP обеспечивает доставку частично поврежденных пакетов  2) UDP lite обеспечивает доставку частично поврежденных пакетов  3) UDP lite обеспечивает доставку частично поврежденных пакетов в зависимости от категории трафика</p>
6	Безопасность уровня приложений (ОПК-12.1)	<p><b><u>Задание 1</u></b>  Укажите основные протоколы, используемые в сети Интернет на прикладном уровне  <i>Выберите один из 3 вариантов ответа:</i>  1) Kerberos, telnet, HTTP, DHCP  2) Kerberos, HTTP, SMTP, XDR  3) HTTP, SMTP, telnet, DTLS</p> <p><b><u>Задание 2</u></b>  По умолчанию за SSH закреплен порт  <i>Выберите один из 3 вариантов ответа:</i>  1) 880  2) 22  3) 220</p> <p><b><u>Задание 3</u></b>  Укажите недостатки протокола FTP  <i>Выберите один из 3 вариантов ответа:</i>  1) с данными на FTP-сервере нельзя работать напрямую, требуется их полностью переписать на локальный компьютер  2) FTP-сервер не гарантирует защиту данных  3) протокол является низкопроизводительным</p> <p><b><u>Задание 4</u></b>  Главная задача протоколов представительского уровня состоит в  <i>Выберите несколько из 4 вариантов ответа:</i>  1) изменении формы представления передаваемой по сети информации, не меняя при этом ее содержания  2) кодировании и шифровании данных</p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>3) преодоление синтаксических различий в представлении данных</p> <p>4) сопряжение сеансового и прикладного уровней</p> <p><b><u>Задание 5</u></b></p> <p>Проксирование трафика является эффективным инструментом защиты от</p> <p><i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) DDoS-атак</li> <li>2) brut force-атак</li> <li>3) атаки «человек посередине»</li> </ol> <p><b><u>Задание 6</u></b></p> <p>Укажите основные типы прокси-серверов</p> <p><i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) публичные, частные публичные, частные приватные</li> <li>2) публичные, частные публичные, приватные, частные приватные</li> <li>3) публичные, приватные, специализированные</li> </ol> <p><b><u>Задание 7</u></b></p> <p>Какие из протоколов сеансового уровня решают задачи обеспечения безопасности</p> <p><i>Выберите несколько из 4 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) RPC</li> <li>2) PAP</li> <li>3) PPTP</li> <li>4) ISNS</li> </ol> <p><b><u>Задание 8</u></b></p> <p>Категории ПО для работы с протоколом HTTP</p> <p><i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) серверы и клиенты</li> <li>2) серверы, клиенты и прокси</li> <li>3) серверы, клиенты и sms</li> </ol> <p><b><u>Задание 9</u></b></p> <p>Проблемы безопасности DNS заключается в том, что</p> <p><i>Выберите несколько из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) некоторые доменные имена могут использоваться для достижения эффектов спуфинга</li> <li>2) DNS-сервер является, по сути, базой данных имен доверенных хост-компьютеров, которую трудно скрыть</li> <li>3) некоторые DNS-ответы не имеют криптографической подписи</li> </ol> <p><b><u>Задание 10</u></b></p> <p>MIB в рамках SNMP является собой</p> <p><i>Выберите один из 3 вариантов ответа:</i></p> <ol style="list-style-type: none"> <li>1) иерархическую базу данных со сведениями об устройстве</li> <li>2) базу данных управляемых устройств</li> <li>3) базу данных доступных методов управления</li> </ol>
7	Программно-технические	<p><b><u>Задание 1</u></b></p> <p>Укажите отличия между IDS и IPS системами</p> <p><i>Выберите один из 3 вариантов ответа:</i></p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
	<p>средства защиты сетей ЭВМ (ОПК-12.1)</p>	<p>1) отличия отсутствуют  2) IDS системы выявляют признаки вторжений, тогда как IPS им препятствуют  3) IPS системы выявляют признаки вторжений, тогда как IDS им препятствуют</p> <p><b><u>Задание 2</u></b>  Типовая СОВ функционирует на уровне  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) периметра сети  2) внутри периметра  3) возможны оба сценария</p> <p><b><u>Задание 3</u></b>  СОВ, основанная на протоколе, осуществляет  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) контроль и анализ коммуникационных протоколов связанными системами или пользователями  2) наблюдение и анализ данных, передаваемых с использованием специфичных для определённых приложений протоколов  3) анализ системных вызовов, логов приложений, модификаций файлов</p> <p><b><u>Задание 4</u></b>  Укажите основные концепции реализации NAT  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) статическая, динамическая, совмещенная  2) статическая, динамическая, перегруженная  3) статическая, динамическая, селективная</p> <p><b><u>Задание 5</u></b>  Какая роль не принадлежит NAT в обеспечении сетевой безопасности  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам  2) Обеспечивает скрытость ряда внутренних сервисов внутренних хостов/серверов  3) Блокирует вторжения вида DDoS</p> <p><b><u>Задание 6</u></b>  Какая роль не принадлежит NAT в обеспечении сетевой безопасности  <i>Выберите один из 3 вариантов ответа:</i></p> <p>1) Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам  2) Обеспечивает скрытость ряда внутренних сервисов внутренних хостов/серверов  3) Блокирует вторжения вида DDoS</p> <p><b><u>Задание 7</u></b>  Функционал NGFW расширен за счет  <i>Выберите несколько из 4 вариантов ответа:</i></p> <p>1) поддержки VPN  2) включения механизмов DPI и песочницы</p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>3) объединения возможностей экрана и COB 4) выявления аномалий входящего трафика</p> <p><b><u>Задание 8</u></b> Сигнатурами атак являются <i>Выберите несколько из 4 вариантов ответа:</i> 1) характерные участки кода вредоносных объектов 2) сетевые узлы, задействованные в ходе атаки 3) перечень действий, выполняемых вредоносными объектами 4) объекты атаки и их параметры</p> <p><b><u>Задание 9</u></b> Системы Dallas Lock предоставляют <i>Выберите один из 3 вариантов ответа:</i> 1) защиту персональных данных и конфиденциальной информации 2) защиту файловых хранилищ и периметра сети 3) комплексную защиту</p> <p><b><u>Задание 10</u></b> NAT выполняет <i>Выберите один из 3 вариантов ответа:</i> 1) преобразование IP-адресов транзитных пакетов 2) построение правил доступа к внешней распределенной среде 3) изоляцию сегментов сетей</p>
8	Безопасность беспроводных сетей (ОПК-12.1)	<p><b><u>Задание 1</u></b> Укажите строку, в которой стандарты шифрования WiFi указаны в порядке возрастания надежности <i>Выберите один из 3 вариантов ответа:</i> 1) WPA, WPA2, WEP 2) WEP, WPA, WPA2 3) WEP, WPA, WPA2 PSK</p> <p><b><u>Задание 2</u></b> Какие типы атак применимы к серверу WPA2 <i>Выберите один из 3 вариантов ответа:</i> 1) атака по словарю, атака переустановки ключа 2) PTW-атака, атака переустановки ключа 3) FMS-атака, PTW-атака</p> <p><b><u>Задание 3</u></b> Недостатки технологии WiFi <i>Выберите один из 3 вариантов ответа:</i> 1) проблемы ЭМС, вызванные заполненностью диапазона 2,4 ГГц, существуют алгоритмы шифрования с низкой стойкостью, несоответствие заявленной и реальной скоростей 2) возможность взлома точки через проводную сеть 3) все заявленное выше</p> <p><b><u>Задание 4</u></b> В режиме ad-hoc WiFi для шифрования использует <i>Выберите один из 3 вариантов ответа:</i> 1) WPA2</p>

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		<p>2) WEP 3) WEP и WPA</p> <p><b><u>Задание 5</u></b> К протоколам маршрутизации сетей Manet относятся <i>Выберите один из 3 вариантов ответа:</i> 1) DSR, OLSR 2) DSR, OLSR, AODV 3) DSR, DLNA</p> <p><b><u>Задание 6</u></b> В каком из режимов работы Bluetooth используется исключительно аутентификация <i>Выберите один из 3 вариантов ответа:</i> 1) незащищенный 2) защищенный на уровне приложения/службы 3) защищенный на уровне канала связи</p> <p><b><u>Задание 7</u></b> Основу WEP составляет <i>Выберите один из 3 вариантов ответа:</i> 1) RC4 2) AES 3) DES</p> <p><b><u>Задание 8</u></b> Укажите длину ключа безопасности Bluetooth <i>Выберите один из 3 вариантов ответа:</i> 1) 128 бит 2) 8-128 бит 3) 192 бита</p> <p><b><u>Задание 9</u></b> Существует ли ограничение на скорость обмена данными для WiFi в ad-hoc режиме <i>Выберите один из 3 вариантов ответа:</i> 1) не существует, зависит от конкретного стандарта 2) 11 Мбит/с 3) 23 Мбит/с</p> <p><b><u>Задание 10</u></b> Инициализацией Bluetooth-соединения включает в себя <i>Выберите один из 3 вариантов ответа:</i> 1) генерацию ключа и ключа связи, аутентификацию 2) аутентификацию, обмен ключами с последующим шифрованием трафика 3) аутентификацию</p>

#### 5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме дифференцированного зачета и экзаменов используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично<sup>1</sup>.

<sup>1</sup> В ходе текущей аттестации могут быть использованы балльно-рейтинговые шкалы.



Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умения	Умение решать стандартные профессиональные задачи с применением средств и систем диагностики и защиты информации автоматизированных систем
	Умение использовать теоретические знания для выбора методики решения профессиональных задач
Навыки	Владение навыками теоретического и экспериментального исследования состояния безопасности автоматизированных систем
	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последователь-	Излагает знания в логической последовательности, самостоятельно их

Критерий	Уровень освоения и оценка			
	2	3	4	5
знаний			ности	интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

### Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Умение решать стандартные профессиональные задачи с применением средств и систем диагностики и защиты информации автоматизированных систем	Не умеет решать стандартные профессиональные задачи с применением средств и систем диагностики и защиты информации автоматизированных систем.	Допускает неточности в решении стандартных профессиональных задач с применением средств и систем диагностики и защиты информации автоматизированных систем	Умеет решать стандартные профессиональные задачи с применением средств и систем диагностики и защиты информации автоматизированных систем	Безошибочно решает стандартные профессиональные задачи с применением средств и систем диагностики и защиты информации автоматизированных систем
Умение использовать теоретические знания для выбора методики решения профессиональных задач	Не умеет использовать теоретические знания для выбора методики решения профессиональных задач	Использование теоретических знаний для выбора методики решения профессиональных задач вызывает затруднения	Умеет использовать теоретические знания для выбора методики решения профессиональных задач	Умело использует теоретические знания для выбора методики решения профессиональных задач

### Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Профессионально владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности

Критерий	Уровень освоения и оценка			
	2	3	4	5
Качество выполнения исследований объектов профессиональной деятельности	Не качественно выполняет исследования объектов профессиональной деятельности, допускает грубые ошибки	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки с посторонней помощью	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки самостоятельно	Качественно выполняет исследования объектов профессиональной деятельности
Самостоятельность в выполнении исследований объектов профессиональной деятельности	Не может самостоятельно выполнять исследования объектов профессиональной деятельности	Выполняет исследования объектов профессиональной деятельности с посторонней помощью	При выполнении исследования объектов профессиональной деятельности иногда требуется посторонняя помощь	Самостоятельно выполняет исследования объектов профессиональной деятельности

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

### 6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения лабораторных занятий	Специализированная мебель. Компьютерная техника, аппаратный брандмауэр Cisco ASA5505; управляемый коммутатор третьего уровня CiscoCatalyst 3560; управляемый коммутатор второго уровня CiscoCatalyst 2960; беспроводной маршрутизатор CiscoRV 120W; неуправляемый коммутатор CiscoSF 100D-05; модуль «Низкоуровневый контроллер Ethernet». Стенд «Глобальные компьютерные сети» в составе: аппаратный маршрутизатор Cisco1921; управляемый коммутатор третьего уровня CiscoCatalyst 3560; управляемый коммутатор второго уровня CiscoCatalyst 2960; беспроводной маршрутизатор CiscoRV 120W; модуль «Низкоуровневый контроллер Ethernet»
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду

### 6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа

1	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Пакет IPTABLES в составе Linux или другой МСЭ	Свободно распространяемое ПО согласно условиям лицензионного соглашения
5	Kali Linux	Свободно распространяемое ПО согласно условиям лицензионного соглашения

### 6.3. Перечень учебных изданий и учебно-методических материалов

- Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие, – 4-е изд. – СПб. : Питер, 2010. – 943 с.
- Э. Таненбаум Компьютерные сети: учеб. пособие, – СПб.: Питер, 2008.
- Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб. пособие / П. Н. Девянин. - Москва : Горячая линия - Телеком, 2011. - 319 с
- Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации: учебное пособие, – Москва: Евразийский открытый институт, 2012.
- Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 230100 (654600) / П. Б. Хорев. - 4-е изд., стер. - Москва : Академия, 2008. - 256 с.
- Лапони́на, О. Р. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапони́на. - 2-е изд., испр. . - Москва : Интернет-Университет Информационных Технологий ; Москва : БИНОМ. Лаборатория знаний, 2007. - 531 с.
- Буханов, Д.Г. Безопасность сетей ЭВМ: методические указания к выполнению лабораторных работ для студентов специальности 10.05.03 – Информационная безопасность автоматизированных систем / сост.: Д.Г. Буханов, М. В. Панченко. – Белгород: Изд-во БГТУ, 2016 – 36с.
- Буханов, Д.Г. Безопасность сетей ЭВМ : методические указания к выполнению лабораторных работ для студентов направления 10.05.03 / БГТУ им. В. Г. Шухова, каф. программного обеспечения вычисл. техники и

автоматизир. систем; сост. Буханов Д. Г., Панченко М. В. – Белгород : Изд-во БГТУ им. В. Г. Шухова, 2015.

9. Фороузан Б.А. Криптография и безопасность сетей : учеб. пособие для студентов вузов / Б. А. Фороузан; ред. А. Н. Берлин. - Москва : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2010. - 784 с.
10. Мэйволд Э. Безопасность сетей : практ. пособие : самоучитель : пер. с англ. / Э. Мэйволд. - Москва : ЭКОМ : Бином. Лаборатория знаний, 2005. - 528 с.
11. Столлингс, В. Криптография и защита сетей : принципы и практика / В. Столлингс. - 2-е изд. - Москва : Вильямс, 2001. - 669 с.
12. Соколов, А. В. Методы информационной защиты объектов и компьютерных сетей / А. В. Соколов, О. М. Степанюк. - Москва : АСТ, 2000. - 272 с.
13. Роберт Л. Зингер Брандмауэры в Linux – М.: Вильямс, 2001 – 384с.
14. Грир Т. Сети и Интранет, Серия «Стратегические технологии», – ЧеннелТрейдинг Лимитед, 2000.
15. Норткрат С. Защита сетевого периметра – М.: ТИД «ДС», 2004 – 672с.
16. Норткрат С. и др. Анализ типовых нарушений безопасности в сетях. Пер. с англ. - М.: Издательский дом «Вильямс», 2001.
17. Золотов С. Протоколы Интернет – СПб.; ВHV, 1998 – 304с.
18. Internet standard RFC 791, Standart IP protocol, 1981 – 41с.
19. Internet standard RFC 792, Standart ICMP protocol, 1981 – 21с.
20. Internet standard RFC 793, Standart TCP protocol, 1981 – 85с.

#### **6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем**

1. Проблемы защиты информации в сетях ЭВМ[Электронный ресурс]. – Режим доступа: [http://all-ib.ru/content/node6/part\\_1.html](http://all-ib.ru/content/node6/part_1.html)
2. Backtrack[Электронный ресурс]. – Режим доступа: <http://www.backtrack-linux.org/>
3. Сетевые атаки. Виды. Способы борьбы[Электронный ресурс]. – Режим доступа: <http://moluch.ru/conf/tech/archive/5/1115/>

## 7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 202\_\_\_ /202\_\_\_ учебный год  
без изменений / с изменениями, дополнениями

Протокол № \_\_\_\_\_ заседания кафедры от « \_\_\_\_ » \_\_\_\_\_ 202\_\_ г.

Заведующий кафедрой \_\_\_\_\_  
подпись, ФИО

Директор института \_\_\_\_\_  
подпись, ФИО