

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»  
Институт математики, физики и информационных технологий  
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:  
Директор института



Н. Л. Королева  
«05» июля 2021 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.В.ДВ.05.2 Анализ защищенности компьютерных сетей

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

**Автор программы:**

Кандидат педагогических наук, доцент Самохвалов Алексей Владимирович

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «26» ноября 2020 г. № 1461).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	4
3. Объем и содержание дисциплины.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	11
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	22
6. Учебно-методическое и информационное обеспечение дисциплины.....	24
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	24

## 1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-3 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- эксплуатационный

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 12 Обеспечение безопасности (в сфере защиты информации)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-3 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	Проводит инструментальный мониторинг защищенности компьютерных систем и сетей для обеспечения их безопасности

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-3 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		4	6	7	8	9
1	"Networksecurity"	+				
2	Безопасность компьютерных сетей	+				
3	Защита программ и данных					+
4	Ознакомительная практика		+			
5	Системы и сети передачи информации			+	+	

## 2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Анализ защищенности компьютерных сетей» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Анализ защищенности компьютерных сетей» изучается в 4 семестре.

## 3. Объем и содержание дисциплины

## 3.1.Объем дисциплины:

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>108</b>
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Зачет	-

## 3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
4 семестр					
1	Потребность в кибербезопасности	4	4	4	Тестирование
2	Атаки, понятия и техники	2	2	4	Тестирование
3	Защита данных и конфиденциальности	2	2	4	Тестирование
4	Защита организации	4	2	4	Тестирование
5	Образование и карьера в сфере информационной безопасности	2	4	4	Тестирование
6	Кибербезопасность — мир экспертов и преступников	2	2	4	Тестирование
7	Куб кибербезопасности	2	2	2	Тестирование
8	Угрозы кибербезопасности , уязвимости и атаки	2	4	2	Тестирование
9	Способы защиты секретной информации	2	2	2	Тестирование
10	Обеспечения целостности данных	2	2	2	Тестирование
11	Концепция «пять девяток»	2	2	4	Тестирование
12	Защита уровней обеспечения кибербезопасности	2	2	4	Тестирование

13	Как стать специалистом в области кибербезопасности	4	2	4	Тестирование
----	--	---	---	---	--------------

## **Тема 1. Потребность в кибербезопасности (ПК-3)**

### **Лекция.**

Введение. Потребность в кибербезопасности. Персональные данные. Что такое «Персональные данные». Что такое кибербезопасность. Идентификация пользователя онлайн и оффлайн. Вычислительные устройства. Корпоративные данные. Что такое «Корпоративные данные». Последствия нарушения безопасности. Злоумышленники и эксперты по кибербезопасности. Профиль киберпреступника. Юридические и этические проблемы кибербезопасности. Кибервойна. Понятие кибервойны.

### **Лабораторные работы.**

1. Назовите мотивацию белого хакера.
2. Какие элементы являются компонентами тройки CIA?
3. Что такое кибервойна?
4. Кто такие хактивисты?
5. Перечислите основные задачи белых хакеров.

## **Тема 2. Атаки, понятия и техники (ПК-3)**

### **Лекция.**

Кибератаки на объекты критической информационной инфраструктуры Интернет Вещей (IoT) - это эволюция в межмашинной связи, уникальное соединение, позволяющее вычислительным устройствам передавать данные по всей сети без участия хотя бы одного человека. Тревожной ситуацией является растущая взаимосвязь объектов критической информационной инфраструктуры с помощью технологий Интернета Вещей и сопутствующее увеличение числа организованных кибератак по всему миру. Было установлено, что многие кибератаки Stuxnet, Havex, Black Energy 3 и Industroyer, совершенные за последние годы, были направлены на системы управления SCADA, принадлежащие к различным субъектам критической информационной инфраструктуры. Очевиден тот факт, что вредоносное ПО, которое нацелено на водные и газовые станции, электростанции и транспортные системы, является делом рук профессионалов и было специально разработано для совершения подобных действий. Многие устройства, работающие на базе Интернета Вещей, интегрированы в субъекты критической информационной инфраструктуры для достижения максимально эффективного взаимодействия и коммуникации. По прогнозам к 2025 году число устройств, подключенных к интернету, достигнет 75 миллиардов, что может значительно ухудшить ситуацию и привести к увеличению роста кибератак, нацеленных на критическую информационную инфраструктуру, которые разрабатываются с использованием решений на основе Интернета Вещей и соответственно могут быть подвержены кибератакам.

### **Лабораторные работы.**

1. Почему внутренние угрозы безопасности могут нанести организации еще больший ущерб, чем внешние?
2. Какие способы можно использовать для обеспечения конфиденциальности информации?
3. Как еще называют конфиденциальность информации?
4. Какой способ используется для проверки целостности данных?

### **Задания для самостоятельной работы.**

1. Задание. Определение термина «уязвимость».

2. Задание. Определение типов вредоносного ПО.
3. Задание. Определение типа DoS-атаки.

### **Тема 3. Защита данных и конфиденциальности (ПК-3)**

#### **Лекция.**

Защита устройств и сети. Защита вычислительных устройств. Соблюдение правила безопасности при использовании беспроводных сетей. Использование уникальных паролей для каждой учетной записи в сети. Ведение данных. Шифрование данных. Резервное копирование данных. Окончательное удаление данных. Защита персональных данных в сети. Надежная аутентификация. Двухфакторная аутентификация. OAuth 2.0. Конфиденциальность электронной почты и веб-браузера.

#### **Лабораторные работы.**

1. Создание и сохранение надежных паролей
2. Резервное копирование данных во внешнее хранилище
3. Лабораторная работа.
4. Насколько рискованно поведение пользователя в Интернете?

### **Тема 4. Защита организации (ПК-3)**

#### **Лекция.**

Межсетевые экраны. Типы межсетевых экранов. Сканирование портов. Устройства безопасности. Обнаружение атак в реальном времени. Обнаружение атак в реальном времени. Лучшие практические методики по информационной безопасности. Подход к кибербезопасности на основе поведения. Ботнет. Убийственная цепочка. Убийственная цепочка в киберзащите. Безопасность на основе поведения. NetFlow и кибератаки. Подход Cisco к кибербезопасности. CSIRT. Сборник сценариев по обеспечению безопасности. Инструменты для предотвращения и обнаружения инцидентов. Системы IDS и IPS.

#### **Лабораторные работы.**

1. Какой тип атаки позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)?
2. В чем заключается основная цель атак типа «отказ в обслуживании» (DoS-атак)?
3. Для чего предназначен руткит?
4. Какие характеристики описывают программу-червь?

#### **Задания для самостоятельной работы.**

1. Задание. Определение ответа программы сканирования портов.
2. Задание. Определение устройства безопасности.
3. Задание. Определение порядка этапов убийственной цепочки.

### **Тема 5. Образование и карьера в сфере информационной безопасности (ПК-3)**

#### **Лекция.**

Образование и карьера в сфере информационной безопасности. Возможности сертификации. Возможности сертификации. Расширенные возможности сертификации. Карьера. Вакансии в области кибербезопасности на сайте Cisco.com. Другие вакансии в сфере кибербезопасности.

#### **Лабораторные работы.**

Поиск вакансий по информационной безопасности за рубежом

Порядок выполнения:

- поиск зарубежных сайтов с вакансиями
- настройка фильтров
- изучение полученного списка
- выбор хорошего предложения на рынке

### **Тема 6. Кибербезопасность — мир экспертов и преступников (ПК-3)**

### **Лекция.**

Кибербезопасность — мир экспертов и преступников. Обзор уровней обеспечения кибербезопасности. Примеры уровней обеспечения кибербезопасности. Рост кибердоменов. Кто такие киберпреступники? Мотивы киберпреступников. Зачем становиться специалистом по кибербезопасности? Противодействие киберпреступникам. Типовые угрозы для конечных пользователей. Типы персональных данных. Угрозы Интернет-сервисам. Угрозы ключевым отраслям промышленности. Угрозы образу жизни людей. Внутренние и внешние угрозы. Уязвимости мобильных устройств. Появление Интернета вещей. Влияние больших данных. Использование передового оружия. Более широкий охват и каскадный эффект. Предпосылки безопасности. Повышенное распознавание угроз кибербезопасности. Решение проблемы нехватки специалистов по кибербезопасности. Национальная концепция профессиональной подготовки сотрудников в сфере кибербезопасности (The National Cybersecurity Workforce Framework). Профессиональные организации. Студенческие организации и конкурсы по кибербезопасности. Отраслевые сертификации. Сертификации, спонсируемые компаниями. Как стать экспертом по кибербезопасности.

### **Лабораторные работы.**

- 1 Поиск работы в сфере кибербезопасности.
- 2 Идентификация угроз.
- 3 Задачи профессионалов в сфере кибербезопасности.
- 4 Packet Tracer — создание компьютерного мира.
- 5 Packet Tracer — Общение в кибермире.

## **Тема 7. Куб кибербезопасности (ПК-3)**

### **Лекция.**

Принципы информационной безопасности. Состояния данных. Меры кибербезопасности. Принципы конфиденциальности. Защита конфиденциальных данных. Контроль доступа. Законы и ответственность. Принцип целостности данных. Требования к целостности данных. Проверки целостности. Принцип доступности. Пять девятков. Обеспечение доступности. Варианты хранения данных. Задачи защиты хранящихся данных. Методы передачи данных. Задачи защиты передаваемых данных. Виды обработки данных. Задачи защиты обрабатываемых данных. Технологические программные меры защиты. Технологические аппаратные меры защиты. Технологические сетевые меры защиты. Технологические средства защиты на базе облака. Образовательные и учебные мероприятия по кибербезопасности. Формирование культуры кибербезопасности. Политики. Стандарты. Рекомендации. Процедуры. Обзор модели кибербезопасности. Уровни обеспечения кибербезопасности. Контрольные цели. Средства управления. Модель кибербезопасности ISO и триада «КЦД». Использование модели кибербезопасности ISO и состояния данных. Модель кибербезопасности ISO и меры защиты.

### **Лабораторные работы.**

- 1 Установка виртуальной машины на ПК.
- 2 Аутентификация, авторизация и учет.
- 3 Packet Tracer — изучение шифрования файлов и данных.
- 4 Packet Tracer — проверка целостности файлов и данных.

## **Тема 8. Угрозы кибербезопасности, уязвимости и атаки (ПК-3)**

### **Лекция.**



Угрозы кибербезопасности, уязвимости и атаки. Что такое вредоносная программа? Вирусы, интернет-черви и «троянские кони». Логические бомбы. Программы-вымогатели. Бэкдоры и руткиты. Защита от вредоносных программ. Спам. Шпионское, рекламное ПО и поддельные антивирусные программы. Фишинг. Вишинг, смишинг, фарминг и уэйлинг. Заражение браузера и подключаемых модулей. Защита от атак через браузер и электронную почту. Социальная инженерия. Тактики социальной инженерии. Взгляд через плечо и поиск в мусоре. Имперсонификация и розыгрыш. Несанкционированное проникновение. Мошенничество в Интернете и по электронной почте. Защита от обмана. Отказ в обслуживании. Прослушивание. Подмена. Атака через посредника. Атаки нулевого дня. Клавиатурные шпионы (кейлогеры). Защита от атак. Условно вредоносное ПО и смишинг. Вредоносные точки доступа. Глушение радиочастот. Bluejacking и Bluesnarfing. Атаки на WEP и WPA. Защита от атак на беспроводные сети и мобильные устройства. Межсайтовый скриптинг. Внедрение кода. Переполнение буфера. Удаленный запуск программ. Элементы управления ActiveX и Java. Защита от атак на приложения.

#### **Лабораторные работы.**

- 1 Обнаружение угроз и уязвимостей.
- 2 Packet Tracer — настройка WEP/WPA2 PSK/WPA2 RADIUS.

### **Тема 9. Способы защиты секретной информации (ПК-3)**

#### **Лекция.**

Искусство защиты секретов. Что такое криптография? История криптографии. Создание криптограммы. Два типа шифрования. Процесс симметричного шифрования. Типы криптографических преобразований. Симметричные алгоритмы шифрования. Процесс асимметричного шифрования. Алгоритмы асимметричного шифрования. Управление ключами. Сравнение типов шифрования. Приложения. Системы разграничения физического доступа. Системы разграничения логического доступа. Средства административного контроля доступа. Обязательное разграничение доступа. Дискреционное разграничение доступа. Контроль доступа на основе ролей. Разграничение доступа на основе правил. Что такое идентификация? Средства контроля идентификации. Что-то, что мы знаем (фактор знания). Что-то, что мы имеем (фактор владения). Что-то, что является частью нас (фактор свойства). Многофакторная аутентификация. Что такое авторизация?. Использование авторизации. Что такое отчетность? Внедрение отчетности. Превентивные средства контроля. Сдерживающие средства контроля. Распознавательные средства контроля. Корректирующие средства контроля. Средства восстановления. Компенсирующие средства контроля. Что такое маскирование данных? Методы маскирования данных. Что такое стеганография?. Методы стеганографии. Социальная стеганография. Обнаружение. Обфускация. Приложения.

#### **Лабораторные работы.**

- 1 Применение стеганографии.
- 2 Packet Tracer. Настройка транспортного режима VPN.
- 3 Packet Tracer. Настройка туннельного режима VPN.

### **Тема 10. Обеспечения целостности данных (ПК-3)**

#### **Лекция.**

Что понимается под хешированием? Свойства хеш-функций. Алгоритмы хеширования. Современные алгоритмы хеширования. Хеширование файлов и цифровых носителей. Хеширование паролей. Приложения. Взлом хешей. Что понимается под добавлением соли? Предотвращение атак. Реализация механизма добавления соли. Для чего применяется механизм HMAC? Принцип действия механизма HMAC. Применение механизма HMAC. Что собой представляет цифровая подпись? Невозможность отказа. Процессы, применяемые при создании цифровой подписи. Использование цифровых подписей. Сравнение алгоритмов цифровой подписи. Что собой представляет цифровой сертификат? Использование цифровых сертификатов. Что собой представляет источник сертификатов? Что содержит в себе цифровой сертификат? Процесс проверки. Путь сертификата. Целостность данных. Средства контроля ввода данных. Правило проверки. Проверка типа данных. Проверка входных данных. Проверка аномалий. Целостность объекта. Ссылочная целостность. Целостность домена.

#### **Лабораторные работы.**

- 1 Взлом пароля.
- 2 Использование цифровых подписей.
- 3 Удаленный доступ.

### **Тема 11. Концепция «пять девяток» (ПК-3)**

#### **Лекция.**

Что означает термин «пять девяток»? Сферы, в которых реализация концепции «пять девяток» обязательна. Угрозы доступности. Проектирование систем высокой доступности. Идентификация ресурсов. Классификация ресурсов. Стандартизация ресурсов. Идентификация угроз. Анализ рисков. Устранение. Многоуровневый подход. Ограничение. Разнообразие. Соккрытие информации. Простота. Единая точка отказа. Резервирование по схеме "N+1". RAID. STP. Резервирование маршрутизаторов. Способы резервирования маршрутизаторов. Размещение резервных копий данных на удаленном объекте. Проектирование с учетом требований к способности системы к восстановлению. Отказоустойчивость приложений. Отказоустойчивость IOS. Подготовка. Обнаружение и анализ. Изоляция, ликвидация и восстановление. Подведение итогов по инцидентам информационной безопасности. Сетевой модуль Cisco NAC. Системы обнаружения вторжений. Система предотвращения вторжений. NetFlow и IPFIX. Продвинутое средство анализа угроз. Виды аварий. План аварийного восстановления. Внедрение мер аварийного восстановления. Необходимость в непрерывности бизнес-процессов. Аспекты непрерывности бизнес-процессов. Лучшие практики обеспечения непрерывности бизнес-процессов.

#### **Лабораторные работы.**

- 1 Cisco Packet Tracer. Резервирование маршрутизаторов и коммутаторов.
- 2 Cisco Packet Tracer. Отказоустойчивость маршрутизаторов и коммутаторов.

### **Тема 12. Защита уровней обеспечения кибербезопасности (ПК-3)**

#### **Лекция.**

Безопасность операционной системы. Защита от вредоносных программ. Управление исправлениями. Межсетевые экраны (брандмауэры) и системы обнаружения вторжений на основе хоста. Защита коммуникаций. WEP, WPA/WPA2. Взаимная аутентификация. Разграничение доступа к файлам. Шифрование файлов. Резервное копирование данных и систем. Фильтрация и блокирование содержимого. Клонирование жесткого диска и утилита Deep Freeze. Защитные кабели и замки. Блокировка компьютера после бездействия. GPS-мониторинг. Реестр устройств и радиометки. Управление удаленным доступом. Telnet, SSH и SCP. Защита портов и сервисов. Привилегированные учетные записи. Групповые политики. Включение журналов и оповещений. Питание. Отопление, вентиляция и кондиционирование воздуха (ОВК, HVAC). Контроль аппаратных средств. Оперативные центры. Коммутаторы, маршрутизаторы и сетевые устройства. Беспроводные и мобильные устройства. Сетевые сервисы и сервисы маршрутизации. Оборудование VoIP. Камеры. Оборудование для видео-конференц-связи. Сетевые датчики и датчики Интернета вещей. Технологии биометрической идентификации. Пропуска и журналы доступа. Охрана и сопровождение. Видеонаблюдение и наблюдение с использованием электронных средств. RFID и беспроводное наблюдение.

#### **Лабораторные работы.**

- 1 Повышение надежности системы Linux.
- 2 Cisco Packet Tracer. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе.

### **Тема 13. Как стать специалистом в области кибербезопасности (ПК-3)**

#### **Лекция.**

Общие угрозы и уязвимости, связанные с пользователями. Управление угрозами, связанными с пользователями. Распространенные угрозы для устройств. Управление угрозами, связанными с устройствами. Распространенные угрозы для локальной сети. Управление угрозами для локальной сети. Распространенные угрозы для частного облака. Управление угрозами для частного облака. Распространенные угрозы для общедоступного облака. Управление угрозами для общедоступного облака. Распространенные угрозы для физических средств. Управление угрозами для физических средств. Распространенные угрозы для приложений. Управление угрозами для приложений. Этические ценности специалиста по обеспечению кибербезопасности. Институт компьютерной этики. Киберпреступность. Гражданское и уголовное законодательство и нормативные требования информационного и телекоммуникационного права. Отраслевые законы. Законы об уведомлении в случае нарушения безопасности. Защита конфиденциальности. Международные законы. Национальная база данных уязвимостей. CERT. Internet Storm Center. Передовой центр кибербезопасности (Advanced Cyber Security Center, ACSC). Сканеры уязвимостей. Тестирование на возможность проникновения. Анализаторы пакетов. Инструментальные средства безопасности. Определение ролей специалистов по кибербезопасности. Средства поиска вакансий.

#### **Лабораторные работы.**

- 1 Packet Tracer. Отработка комплексных практических навыков.
- 2 В этом задании два маршрутизатора настроены на обмен данными.
- 3 Вы отвечаете за настройку подынтерфейсов для взаимодействия с коммутаторами.
- 4 Вам предстоит настроить сети VLAN, транковую связь и EtherChannel с протоколом PVST.
- 5 Все интернет-устройства настроены заранее

### **4. Контроль знаний обучающихся и типовые оценочные средства**

#### **4.1. Распределение баллов:**

#### **4 семестр**

- посещаемость – 20 баллов
- текущий контроль – 72 балла
- контрольные срезы – 2 среза по 4 балла каждый
- премиальные баллы – 20 баллов

## Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Потребность в кибербезопасности	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
2.	Атаки, понятия и техники	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
3.	Защита данных и конфиденциальности	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
4.	Защита организации	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
5.	Образование и карьера в сфере информационной безопасности	<b>Тестирование(контрольный срез)</b>	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
6.	Кибербезопасность — мир экспертов и преступников	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
7.	Куб кибербезопасности	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
8.	Угрозы кибербезопасности, уязвимости и атаки	<b>Тестирование(контрольный срез)</b>	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.

9.	Способы защиты секретной информации	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
10.	Обеспечения целостности данных	Тестирование	4	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 4 балла; - 65 % - 3 балла; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
11.	Концепция «пять девяток»	Тестирование	12	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 12 баллов; - 65 % - 6 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
12.	Защита уровней обеспечения кибербезопасности	Тестирование	14	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 14 баллов; - 65 % - 6 баллов; - 50 % - 3 балла; - менее 50 % - балл не начисляется.
13.	Как стать специалистом в области кибербезопасности	Тестирование	14	Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы: - 90 % - 14 баллов; - 65 % - 6 баллов; - 50 % - 3 балла; - менее 50 % - балл не начисляется.
14.	Посещаемость		20	20 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 10 баллов – студент посетил не менее 50% занятий 5 баллов – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.
15.	Премиальные баллы		20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции
16.	Итого за семестр		100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

#### 4.2 Типовые оценочные средства текущего контроля

## Тестирование

### Тема 1. Потребность в кибербезопасности

Вопрос 1:

Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

- а) Руководитель среднего звена
- б) Высшее руководство
- в) Владелец
- г) Пользователь

Вопрос 2:

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

- а) Сотрудники
- б) Хакеры
- в) Атакующие
- г) Контрагенты (лица, работающие по договору)

Вопрос 3:

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

- а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- в) Улучшить контроль за безопасностью этой информации
- г) Снизить уровень классификации этой информации

Вопрос 4:

Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

- а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- б) Необходимый уровень доступности, целостности и конфиденциальности
- в) Оценить уровень риска и отменить контрмеры
- г) Управление доступом, которое должно защищать данные

Вопрос 5:

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

- а) Владельцы данных
- б) Пользователи
- в) Администраторы
- г) Руководство

Вопрос 6:

Что такое процедура?

Варианты ответа:

- а) Правила использования программного и аппаратного обеспечения в компании
- б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

Вопрос 7:

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Варианты ответа:

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

Вопрос 8:

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Варианты ответа:

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

б) Когда риски не могут быть приняты во внимание по политическим соображениям

в) Когда необходимые защитные меры слишком сложны

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

Вопрос 9:

Что такое политики безопасности?

Варианты ответа:

а) Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) Широкие, высокоуровневые заявления руководства

г) Детализированные документы по обработке инцидентов безопасности

## Тема 2. Атаки, понятия и техники

**1. Хакер заблокировал пользователей и зашифровал хранящиеся на их персональных компьютерах файлы и данные, и предлагает восстановить доступ к ним если ему заплатят выкуп. Как называется такой тип кибератаки?**

-Browser hijacker

-Ransomware(программа-вымогатель)

-Brute-force

**2. В вечерних новостях репортер рассказывал о Интернет-угрозе под названием 'Botnet'. Что такое Botnet?**

-Вредоносная программа, которая маскирует себя среди других файлов или данных, хранящихся на компьютере.

-Группа компьютеров, на которых работают вредоносные программы, удаленно управляемые киберпреступниками.

-Новый тип китайского вируса, создающий хаос по всему миру.

**3. Какие типы атак приводят к нарушению нормальной работы web-сайта или другого сетевого ресурса?**

-Атака DoS

-Атака POS

-Фишинг

**4. Что из перечисленного является примером фишинга?**

-К вам пришло письмо по электронной почте от человека, с которым вы редко контактируете, и оно содержит только ссылку на адрес в web.-К вам пришло письмо по электронной почте из вашего банка с просьбой ввести номер вашего счета в этом банке и пароль, но адрес отправителя не похож на адрес вашего банка.

-Вы получили сообщение о том, что вы выиграли в конкурсе, и для получения приза нужно щелкнуть по ссылке.

-Все вышеперечисленное

**5. Вы поехали в командировку в другой город и зашли в кафе чтобы отправить письма своим коллегам относительно текущих проектов.**

Для обеспечения безопасности при использовании этих общедоступных сетей нужно всегда:

-Найти поблизости самый сильный сигнал WiFi.

-Отключить сервис обмена файлами

-Использовать виртуальную частную сеть Virtual Private Network (VPN)

**6. Вам предстоит участвовать в совещании, посвященном новому европейскому закону о защите персональных данных General Data Protection Regulation (GDPR), который начнет действовать в мае этого года. Какое из следующих утверждений относительно GDPR является правильным?**

-GDPR касается защиты персональных данных граждан Европейского Союза и поэтому его требования должны выполнять только европейские компании.

-GDPR тесно связан с Информационной Безопасностью.

-Хотя невыполнение требований GDPR наносит ущерб репутации компании, никакие финансовые штрафы за нарушение этого закона не предусмотрены.

### Тема 3. Защита данных и конфиденциальности

1. Конфиденциальность — это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

2. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

3. Конфиденциальную информацию можно разделить:

А) предметную

Б) служебную

В) глобальную

4. Основными источниками внутренних отказов являются:

А) ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации



## Тема 4. Защита организации

### **Защита информации от утечки это деятельность по предотвращению:**

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

### **Защита информации это:**

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

## Тема 5. Образование и карьера в сфере информационной безопасности

### Поиск вакансий по информационной безопасности за рубежом

#### Порядок выполнения:

- поиск зарубежных сайтов с вакансиями
- настройка фильтров
- изучение полученного списка
- выбор хорошего предложения на рынке

## Тема 6. Кибербезопасность — мир экспертов и преступников

### Тестирование

1. Почему устройства IoT представляют больше риска, чем другие вычислительные устройства в сети?
2. Какая конфигурация беспроводного маршрутизатора считается неадекватной защитой для беспроводной сети?
3. Как пользователю обезопасить себя от «подслушивания» сетевого трафика, когда он пользуется публичной точкой доступа Wi-Fi на своем ПК?
4. Туннелирование трафика.

## 5. VPN как средство защиты.

### Тема 7. Куб кибербезопасности

Вопрос 1: Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

- а) Руководитель среднего звена
- б) Высшее руководство
- в) Владелец
- г) Пользователь

Вопрос 2: Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

- а) Сотрудники
- б) Хакеры
- в) Атакующие
- г) Контрагенты (лица, работающие по договору)

Вопрос 3: Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

- а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- в) Улучшить контроль за безопасностью этой информации
- г) Снизить уровень классификации этой информации

Вопрос 4: Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

- а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- б) Необходимый уровень доступности, целостности и конфиденциальности
- в) Оценить уровень риска и отменить контрмеры
- г) Управление доступом, которое должно защищать данные

Вопрос 5: Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

- а) Владельцы данных
- б) Пользователи
- в) Администраторы
- г) Руководство

Вопрос 6: Что такое процедура?

Варианты ответа:

- а) Правила использования программного и аппаратного обеспечения в компании
- б) Пошаговая инструкция по выполнению задачи
- в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- г) Обязательные действия

### Тема 8. Угрозы кибербезопасности, уязвимости и атаки

Лабораторная работа 1

Обнаружение угроз и уязвимостей.

## Лабораторная работа 2

Packet Tracer — настройка WEP/WPA2 PSK/WPA2 RADIUS.

## Лабораторная работа 3

Packet Tracer - настройка доступа к беспроводной LAN

## Тема 9. Способы защиты секретной информации

- 1 Применение стеганографии.
- 2 Packet Tracer. Капсулирование трафика.
- 3 Packet Tracer. Туннели GRE.
- 4 Packet Tracer. Настройка транспортного режима VPN.
- 5 Packet Tracer. Настройка туннельного режима VPN.

## Тема 10. Обеспечения целостности данных

## Задание

- 1 Взлом пароля.
- 2 Использование цифровых подписей.
- 3 Удаленный доступ.
- 4 Фишинговые атаки.
- 5 Социальная инженерия.

## Тема 11. Концепция «пять девяток»

## Задание 1

Cisco Packet Tracer. Резервирование маршрутизаторов и коммутаторов.

## Задание 2

Cisco Packet Tracer. Отказоустойчивость маршрутизаторов и коммутаторов.

## Задание 3

Cisco Packet Tracer. Настройка списков доступа.

## Задание 4

Cisco Packet Tracer. Пароли для удаленных линий доступа.

## Тема 12. Защита уровней обеспечения кибербезопасности

## Задание 1

Повышение надежности системы Linux.

## Задание 2

Cisco Packet Tracer. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе.

## Задание 3

Cisco Packet Tracer. Настройка VLAN

## Тема 13. Как стать специалистом в области кибербезопасности

- 1 Packet Tracer. Отработка комплексных практических навыков.
- 2 В этом задании два маршрутизатора настроены на обмен данными.
- 3 Вы отвечаете за настройку подынтерфейсов для взаимодействия с коммутаторами.
- 4 Вам предстоит настроить сети VLAN, транковую связь и EtherChannel с протоколом PVST.
- 5 Все интернет-устройства настроены заранее

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

**Типовые вопросы зачета (ПК-3)**

Элементы управления доступом к учетной записи пользователя и криптографию, которые могут защищать системные файлы и данные.

Брандмауэры, которые на сегодняшний день являются наиболее распространенными системами профилактики с точки зрения безопасности компьютерных сетей. Это связано с тем, что они способны (в том случае, если их правильно настроить) защищать доступ к внутренним сетевым службам и блокировать определенные виды атак посредством фильтрации пакетов.

Системы обнаружения вторжений (IDS), которые предназначены для обнаружения сетевых атак в процессе их осуществления, а также для оказания помощи после атаки, в то время как контрольные журналы и каталоги выполняют аналогичную функцию для отдельных систем.

### **Типовые задания для зачета (ПК-3)**

#### **1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

#### **2) Основными источниками угроз информационной безопасности являются все указанное в списке:**

- Хищение жестких дисков, подключение к сети, инсайдерство
- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

#### **3) Виды информационной безопасности:**

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

#### **4) Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

#### **5) Основные объекты информационной безопасности:**

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

#### **6) Основными рисками информационной безопасности являются:**

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

#### **7) К основным принципам обеспечения информационной безопасности относится:**

- + Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

#### **8) Основными субъектами информационной безопасности являются:**

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

#### **9) К основным функциям системы безопасности можно отнести все перечисленное:**

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компаний
- Внедрение аутентификации, проверки контактных данных пользователей

#### **тест 10) Принципом информационной безопасности является принцип недопущения:**

- + Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы
- Презумпции секретности

**11) Принципом политики информационной безопасности является принцип:**

- + Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

**12) Принципом политики информационной безопасности является принцип:**

- + Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

**13) Принципом политики информационной безопасности является принцип:**

- + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

**14) К основным типам средств воздействия на компьютерную сеть относится:**

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

**15) Когда получен спам по e-mail с приложенным файлом, следует:**

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- + Удалить письмо с приложением, не раскрывая (не читая) его

**16) Принцип Кирхгофа:**

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- + Секретность закрытого сообщения определяется секретностью ключа

**17) ЭЦП – это:**

- Электронно-цифровой преобразователь
- + Электронно-цифровая подпись
- Электронно-цифровой процессор

**18) Наиболее распространены угрозы информационной безопасности корпоративной системы:**

- Покупка нелегального ПО
- + Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

**19) Наиболее распространены угрозы информационной безопасности сети:**

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- + Сбой (отказ) оборудования, нелегальное копирование данных

**тест\_20) Наиболее распространены средства воздействия на сеть офиса:**

- Слабый трафик, информационный обман, вирусы в интернет
- + Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

**21) Утечкой информации в системе называется ситуация, характеризующаяся:**

- + Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

**22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

- + Целостность

- Доступность
- Актуальность

**23) Угроза информационной системе (компьютерной сети) – это:**

- + Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

**24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

- Регламентированной
- Правовой
- + Защищаемой

**25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:**

- + Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

**26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

- + Владелец сети
- Администратор сети
- Пользователь сети

**27) Политика безопасности в системе (сети) – это комплекс:**

- + Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

**4.4. Шкала оценивания промежуточной аттестации**

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-3	Владеет методами защиты компьютерных систем и сетей от постороннего воздействия.¶Способен администрировать средства защиты компьютерных систем и сетей прикладного и системного программного обеспечения для обеспечения их безопасности.¶
«не зачтено» (0 - 49 баллов)	ПК-3	Не владеет методами защиты компьютерных систем и сетей от постороннего воздействия.¶Не способен администрировать средства защиты компьютерных систем и сетей прикладного и системного программного обеспечения для обеспечения их безопасности.¶

**5. Методические указания для обучающихся по освоению дисциплины (модуля)**

**5.1 Методические указания по организации самостоятельной работы обучающихся:**

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

## 5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

## 5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

## 5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Основная литература:**

1. Ковган Н. М. Компьютерные сети : учебное пособие. - Минск: РИПО, 2014. - 180 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=463304>
2. Лапони́на О. Р. Криптографические основы безопасности. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=429092>

### **6.2 Дополнительная литература:**

1. Фомин Д. В. Компьютерные сети : учебно-методическое пособие. - Москва|Берлин: Директ-Медиа, 2015. - 66 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=349050>
2. Карташевский, В. Г., Лихтциндер, Б. Я., Киреева, Н. В., Буранова, М. А. Компьютерные сети : учебник. - Весь срок охраны авторского права; Компьютерные сети. - Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. - 267 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/71846.html>
3. Ковган, Н. М. Компьютерные сети : учебное пособие. - 2025-03-10; Компьютерные сети. - Минск: Республиканский институт профессионального образования (РИПО), 2019. - 179 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/93384.html>

### **6.3 Иные источники:**

1. Вопросы образования - <http://www.ecsocman.edu.ru/vo>
2. Федеральная служба по надзору в сфере образования и науки - <http://obrnadzor.gov.ru>
3. Портал "Гуманитарное образование" - <http://www.humanities.edu.ru/>
4. Федеральный портал «Российское образование» - <http://www.edu.ru/>

## **7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы**



Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Microsoft Office Профессиональный плюс 2007

Adobe acrobat

LibreOffice

Операционная система "Альт Образование"

Cisco Packet Tracer

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

### **Электронная информационно-образовательная среда**

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz)

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.