

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
«04» июля 2022 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.05.1 Безопасность компьютерных сетей

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2022

Автор программы:

Кандидат педагогических наук, доцент Самохвалов Алексей Владимирович

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «29» июня 2022 г. Протокол № 12

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «04» июля 2022 г. № 6.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	9
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	32
6. Учебно-методическое и информационное обеспечение дисциплины.....	34
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	35

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

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

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

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-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	Администрирует программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей на иностранном языке

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		3	4	5	6	8
1	Адаптационная "Безопасность компьютерных сетей"			+	+	
2	Анализ защищенности компьютерных сетей			+	+	
3	Компьютерные сети	+	+			
4	На иностранном языке "Network security"			+	+	
5	Эксплуатационная практика					+

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Безопасность компьютерных сетей» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Безопасность компьютерных сетей» изучается в 5, 6 семестрах.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 4 з.е.

Очная: 4 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	144
Контактная работа	56
Лекции (Лекции)	28
Лабораторные (Лаб. раб.)	28
Самостоятельная работа (СР)	52
Экзамен	36
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
5 семестр					
1	Куб кибербезопасности	4	4	10	Лабораторна работа; Собеседование; Тестирование
2	Угрозы кибербезопасности , уязвимости и атаки	4	4	10	Лабораторная работа; Лабораторная работа; Собеседование
3	Способы защиты секретной информации	4	4	10	Собеседование; Лабораторная работа; Тестирование
4	Обеспечения целостности данных	4	4	10	Собеседование; Тестирование; Лабораторная работа
6 семестр					
5	Концепция «пять девяток»	4	4	4	Собеседование
6	Защита уровней обеспечения кибербезопасности	4	4	4	Собеседование; Лабораторная работа
7	Как стать специалистом в области кибербезопасности	4	4	4	Собеседование; Лабораторная работа

Тема 1. Куб кибербезопасности (ПК-2)

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 моделей 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 2. Угрозы кибербезопасности, уязвимости и атаки (ПК-2)

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.

Лабораторная работа 1

Обнаружение угроз и уязвимостей.

Лабораторная работа 2

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

Тема 3. Способы защиты секретной информации (ПК-2)

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 4. Обеспечения целостности данных (ПК-2)

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 НМАС? Принцип действия механизма НМАС. Применение механизма НМАС. 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 5. Концепция «пять девяток» (ПК-2)

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 средства 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 6. Защита уровней обеспечения кибербезопасности (ПК-2)

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 **Настройка зональных межсетевых экранов Cisco**
- 3 Часть 1. Основная конфигурация маршрутизаторов
 - Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа.
 - Настройте статические маршруты для организации сквозной связи.

Часть 2. Настройка зонального межсетевого экрана (ZPF)

- Используйте CLI для настройки зонального межсетевого экрана.
- Используйте CLI для проверки конфигурации.

Тема 7. Как стать специалистом в области кибербезопасности (ПК-2)

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:

5 семестр

- посещаемость – 10 баллов
- текущий контроль – 62 балла
- контрольные срезы – 4 среза: 5 баллов, 10 баллов, 5 баллов, 8 баллов
- 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.	Куб кибербезопасности	Лабораторная работа	10	Лабораторные работы выполняются по тематике практических занятий. 10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 6 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы

		Собеседование(контрольный срез)	5	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>2 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		Тестирование	7	<p>Тест состоит из вопросов с выбором ответа.</p> <p>6-7 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>3 балла – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>

2.	Угрозы кибербезопасности, уязвимости и атаки	Лабораторная работа	10	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>6 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Лабораторная работа	10	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>6 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>

		Собеседование	5	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>2 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
--	--	---------------	---	---

3.	Способы защиты секретной информации	Собеседование	5	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>2 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
----	-------------------------------------	---------------	---	---

		Лабораторная работа(контрольный срез)	10	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>6 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестирование	5	<p>Тест состоит из вопросов с выбором ответа.</p> <p>4-5 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>3 балла – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>

4.	Обеспечения целостности данных	Собеседование(контрольный срез)	<div data-bbox="496 78 638 2083">5</div> <div data-bbox="638 78 1481 2083"> <p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>2 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p> </div>
----	--------------------------------	---------------------------------	--

	Лабораторная работа	10	Лабораторные работы выполняются по тематике практических занятий. 10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 6 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
5.	Посещаемость	10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % занятий 4-6 баллов – посещаемость студента составляет не менее 50 % занятий 1-3 балла – посещаемость студента составляет не менее 25 % занятий
6.	Премияльные баллы	20	Дополнительные премияльные 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 / журнале из перечня ВАК – 10 / 15 / 20
7.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Провести анализ по одной статье из журналов по рекомендуемой литературы из рабочей программы соответствующей дисциплины с оценкой ее содержания (20 баллов) Прохождение тестирования (90 вопросов) по всему курсу дисциплины (10 баллов)
8.	Итого за семестр	100	

6 семестр

- посещаемость – 10 баллов
- текущий контроль – 35 баллов
- контрольные срезы – 2 среза: 10 баллов, 15 баллов
- премияльные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
--------	------------------------------------	---------------------------------	--------------------	--------------------------------------

1.	Концепция «пять девяток»	Собеседо вание	10	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>10 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>5 баллов – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
----	-----------------------------	-------------------	----	---

2.	Защита уровней обеспечения кибербезопасности	Собеседование(контрольный срез)	10	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>10 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>5 баллов – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
----	--	---------------------------------	----	---

		Лабораторная работа	15	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>15 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>10 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>5 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
--	--	---------------------	----	---

3.	Как стать специалистом в области кибербезопасности	Собеседование	10	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>10 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с испо.</p> <p>5 баллов – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
----	--	---------------	----	---

		Лабораторная работа(контрольный срез)	15	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>15 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>10 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>5 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
4.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
5.	Премияльные баллы		20	<p>Дополнительные премияльные баллы могут быть начислены:</p> <ul style="list-style-type: none"> - 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 дисциплине – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

6.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «достаточно полные и систематизированные знания по дисциплине;» умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.</p> <p>- Оценка «отлично» – систематизированные и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.</p>
7.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	<p>Провести анализ по одной статье из журналов по рекомендуемой литературе из рабочей программы соответствующей дисциплины с оценкой ее содержания (20 баллов)</p> <p>Прохождение тестирования (90 вопросов) по всему курсу дисциплины (10 баллов)</p>
8.	Итого за семестр	100	

Итоговая оценка по экзамену 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
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Лабораторная работа

Тема 1. Куб кибербезопасности

- 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.

Лабораторная работа

Тема 2. Угрозы кибербезопасности, уязвимости и атаки

Лабораторная работа

Изучение основных методов работы вирусов-вымогателей.

Порядок выполнения:

- изучение принципа работы
- изучение банд вымогателей

Лабораторная работа.

Изучение фишинг-атак

Порядок выполнения:

- изучение принципа работы
- изучение способов применения
- изучение способов защиты

Тема 3. Способы защиты секретной информации

Лабораторная работа

Основы компьютерной стеганографии

Приобретение умений исследования свойства стеганографических контейнеров, разработка стegosистемы и их применение для сокрытия данных при передаче с помощью графика изображений.

Тема 4. Обеспечение целостности данных

1. Какие программы называются файловыми менеджерами?
2. Какая информация отражается в области просмотра программы Konqueror?
3. Как создать новое окно с помощью программы Konqueror?
4. Перечислите задачи по управлению файловой системой, которые можно решать с помощью диспетчера файлов?
5. Перечислите стандартные функции KDE.

Тема 6. Защита уровней обеспечения кибербезопасности

Настройка зональных межсетевых экранов Cisco

Часть 1. Основная конфигурация маршрутизаторов

- Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте статические маршруты для организации сквозной связи.

Часть 2. Настройка зонального межсетевого экрана (ZPF)

- Используйте CLI для настройки зонального межсетевого экрана.
- Используйте CLI для проверки конфигурации.

Тема 7. Как стать специалистом в области кибербезопасности

Packet Tracer. Отработка комплексных практических навыков.

В этом задании два маршрутизатора настроены на обмен данными.

Вы отвечаете за настройку подынтерфейсов для взаимодействия с коммутаторами.

Вам предстоит настроить сети VLAN, транковую связь и EtherChannel с протоколом PVST.

Все интернет-устройства настроены заранее

Собеседование

Тема 1. Куб кибербезопасности

1. Назовите последний этап структуры убийственной цепочки.
2. Какой инструмент может выполнять анализ трафика и портов в реальном времени, а также выявлять атаки сканирования портов, создания цифровых отпечатков и переполнения буфера?
3. Какой инструмент может выявлять вредоносный трафик, сравнивая содержимое пакета с известными сигнатурами атак?

Тема 2. Угрозы кибербезопасности, уязвимости и атаки

1. Что является примером домена данных в Интернете?
2. К какой категории, согласно классификации NICE Workforce Framework, относится специализированная оценка поступающей информации о кибербезопасности с целью определения ее пригодности для аналитики?
3. При какой атаке цель выводится из строя путем отправки ей огромного количества запросов от множества других систем?

Тема 3. Способы защиты секретной информации

1. Какие меры эффективны в борьбе с киберпреступниками?
2. Что означает термин «уязвимость»?
3. Современные методы защиты конфиденциальной информации делятся на две группы. Назовите их.
4. Как регламентировать порядок защиты конфиденциальной информации?
5. Права субъекта и обязанности оператора ПД в политике безопасности.

Тема 4. Обеспечения целостности данных

1. Назвать методы идентификации, применяемые в процессе аутентификации
2. К какой категории относятся законы в сфере кибербезопасности, регулирующие раскрытие организациями конфиденциальной информации о пользователе?
3. Какой механизм можно применить в организации в качестве средства защиты от непреднамеренного изменения информации авторизованными пользователями?
4. Для чего используются хеш-функции в криптографии?
5. Что такое целостность данных?

Тема 5. Концепция «пять девяток»

1. Какой криптографический алгоритм применяется в АНБ и подразумевает использование эллиптических кривых для формирования цифровых подписей и обмена ключами?
2. Назвать процессы, которые относятся к категории логических средств контроля доступа.
3. Назвать примеры административных средств контроля доступа.
4. От чего зависит доступность и недоступность сервиса?
5. Для гарантированной доступности выше 99,8%, чем необходимо заниматься?

Тема 6. Защита уровней обеспечения кибербезопасности

1. При каком алгоритме шифрования применяется один и тот же общий PSK-ключ, чтобы зашифровать и расшифровать данные?

2. Какие термины применяются для описания ключей шифрования?
3. Какой из асимметричных алгоритмов определяет схему электронной передачи общего секретного ключа?
4. Какие виды уровней ИБ существуют?
5. Что включает в себя каждый уровень ИБ?

Тема 7. Как стать специалистом в области кибербезопасности

1. Какой метод подразумевает поиск пароля путем перебора всех возможных комбинаций?
2. Для чего применяется криптографически стойкий генератор псевдослучайных чисел?
3. По каким принципам происходят кибератаки и какие есть способы защиты от них?
4. что такое модели TCP/IP либо OSI?
5. назовите названия уровней одной из моделей?
6. что такое криптография?
7. какие виды криптографии бывают и для чего применяются?

Тестирование

Тема 1. 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 3. Способы защиты секретной информации

Процесс, в ходе которого зашифрованный текст преобразуется в исходный, называется ...

- шифрование
- дешифрование
- преобразование
- искажение

4. Процесс, в ходе которого зашифрованный текст преобразуется в исходный, называется ...

- шифрование
- дешифрование
- преобразование
- искажение

5. Информация, необходимая для беспрепятственного шифрования и дешифрования текстов, называется ...

- ключ
- шифр
- код
- пароль

6. Характеристика шифра, определяющая его стойкость к шифрованию без знания ключа, называется ...

- криптостойкостью
- пароль
- аудентификатор
- шифратор

7. Асимметричное шифрование для шифрования и расшифровки использует ...

- один открытый ключ и один закрытый ключ
- один открытый ключ
- один закрытый ключ
- один и тот же ключ
- два открытых ключа
- два закрытых ключа

8. Асимметричное шифрование для шифрования использует ... ключ.

- открытый
- закрытый

Тема 4. Обеспечения целостности данных

Целостность информации – это

- а) Состояние информации, при котором отсутствует любое ее изменение;
- б) Состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- в) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Безопасность персональных данных – это

- а) Состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;
- б) Состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных;
- в) Состояние защищенности персональных данных, характеризующееся способностью технических средств обеспечить конфиденциальность персональных данных.

Блокирование персональных данных – это

- а) Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- б) Временное прекращение обработки персональных данных;
- в) Временное прекращение обработки персональных данных для уточнения персональных данных.

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ПК-2)

- 1 Что называется компьютерной сетью?
- 2 Какова основная задача компьютерной сети?
- 3 Для чего создаются локальные сети ЭВМ?
- 4 Что такое сервер? Рабочая станция?
- 5 Какие сетевые технологии называются клиент-серверными?
- 6 Что такое сетевой адаптер? Какие типы сетевых адаптеров существуют?
- 7 Какие виды линий (каналов) используются для связи компьютеров в локальных сетях?
- 8 Какие методы доступа от компьютеру используются в локальных сетях?
- 9 Что означает значок Сетевое окружение на Рабочем столе Windows?

Типовые задания для зачета (ПК-2)

- 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 папке «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

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- + Аудит, анализ уязвимостей, риск-ситуаций

Типовые вопросы экзамена (ПК-2)

- 1 Какие сетевые технологии называются клиент-серверными?
- 2 Что такое сетевой адаптер? Какие типы сетевых адаптеров существуют?
- 3 Какие виды линий (каналов) используются для связи компьютеров в локальных сетях?
- 4 Какие методы доступа от компьютеру используются в локальных сетях?
- 5 Что означает значок Сетевое окружение на Рабочем столе Windows?

Типовые задания для экзамена (ПК-2)

1) 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

2) Принцип Кирхгофа:

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

3) ЭЦП – это:

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

4) Наиболее распространены угрозы информационной безопасности корпоративной системы:

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

5) Наиболее распространены угрозы информационной безопасности сети:

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

6) 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

7) Утечкой информации в системе называется ситуация, характеризуемая:

- + Потерей данных в системе
- Изменением формы информации

- Изменением содержания информации

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

- + Целостность
- Доступность
- Актуальность

9) Угроза информационной системе (компьютерной сети) – это:

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

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

- Регламентированной
- Правовой
- + Защищаемой

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

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

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

- + Владелец сети
- Администратор сети
- Пользователь сети

13) 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

14) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- + Аудит, анализ уязвимостей, риск-ситуаций

4.4. Шкала оценивания промежуточной аттестации

Зачет

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-2	Демонстрирует высокий уровень теоретических знаний в области обеспечения безопасности компьютерных сетей.. Способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей. Умеет проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.

«не зачтено» (0 - 49 баллов)	ПК-2	Не способен продемонстрировать знания в области обеспечения безопасности компьютерных сетей. Не способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей. Не умеет проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.
---------------------------------	------	---

Экзамен

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-2	Демонстрирует высокий уровень теоретических знаний в области обеспечения безопасности компьютерных сетей.. Способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей. Умеет проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.
«хорошо» (70 - 84 баллов)	ПК-2	Демонстрирует хороший уровень теоретических знаний в области обеспечения безопасности компьютерных сетей.. Способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей. Может проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.
«удовлетворительно» (50 - 69 баллов)	ПК-2	Демонстрирует достаточный уровень теоретических знаний в области обеспечения безопасности компьютерных сетей.. Способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей. Плохо умеет проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.
«неудовлетворительно» (менее 50 баллов)	ПК-2	Не способен продемонстрировать знания в области обеспечения безопасности компьютерных сетей. Не способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей. Не умеет проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.

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. Лапонина 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

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