

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.05.3 "Networksecurity"

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

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 «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 бакалавра.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	8
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	18
6. Учебно-методическое и информационное обеспечение дисциплины.....	19
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	20

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
- эксплуатационный

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	8
1	International information security			+	
2	Анализ защищенности компьютерных сетей		+		
3	Безопасность компьютерных сетей		+		
4	Компьютерные сети	+	+		
5	Международная информационная безопасность			+	
6	Стандарты в области информационной безопасности			+	
7	Эксплуатационная практика				+

2. Место дисциплины в структуре ОП бакалавриата:

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

Дисциплина «"Networksecurity"» изучается в 4 семестре.

3.Объем и содержание дисциплины

3.1.Объем дисциплины:

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	108
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	6	4	6	Собеседование; Тестирование
2	Атаки, понятия и техники	6	6	8	Собеседование; Тестирование
3	Защита данных и конфиденциальности	6	6	10	Собеседование; Тестирование
4	Защита организации	4	6	10	Собеседование; Тестирование
5	Кибербезопасность — мир экспертов и преступников	6	6	10	Собеседование; Тестирование
6	Куб кибербезопасности	4	4	-	Собеседование; Тестирование

Тема 1. Потребность в кибербезопасности (ПК-2)

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. Кибервойна - изучите ход событий, которые уже были и предположите вероятность кибервойны в наше время
2. Изучите деятельность злоумышленников и экспертов по кибербезопасности
3. Какие программы и средства помогают реализовать структуру кибербезопасности?

Задания для самостоятельной работы.

1. Что такое «Корпоративные данные»
2. Последствия нарушения безопасности
3. Объясните, как используется инфраструктура открытых ключей для обеспечения конфиденциальности данных и аутентификации.
4. Создайте ход действия киберприступника, образ злоумышленника.

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

Лекция.

Анализ кибератаки. Уязвимости системы безопасности и эксплойты. Типы уязвимостей системы безопасности. Типы и симптомы вредоносного ПО. Способы проникновения. Отказ в обслуживании. Ландшафт кибербезопасности. Смешанная атака. Уменьшение последствий.

Лабораторные работы.

1. Найти киберугрозы для персонального компьютера работающего как рабочая станция в организации. Изучить, найти методы реализации
2. Провести анализ своего ПК и результат представить в отчете с подробным описанием каждого процесса
3. Используя полученные навыки работы с поисковой системой, определить наиболее актуальные методы фишинг атак и представить их в отчете.

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-2)

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. Насколько рискованно поведение пользователя в Интернете?

Задания для самостоятельной работы.

1. Объясните, каким образом процессы и процедуры защищают систему.
2. Опишите методы, используемые для предотвращения распространенных сетевых атак. Опишите защиту периметра сети.
3. Дайте определение понятию защита информации.
4. Что понимается под термином безопасность информации?
5. Что включает в себя защита информации?
6. Какие цели преследует защита информации?
7. Какое место занимает защита информации в информационной безопасности?

Тема 4. Защита организации (ПК-2)

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. Настройка межсетевого экрана "Произвести настройку межсетевого экрана на основе зон"

Цель: В этой лабораторной работе вы создадите сеть с несколькими маршрутизаторами, настроите маршрутизаторы и хосты ПК, а также настроите межсетевой экран на основе зон с помощью интерфейса командной строки Cisco IOS (CLI).

2. Настройка базовой конфигурации ASA "На сетевых устройствах должны быть настроены базовые параметры"

Цель: Цель этой лабораторной работы - настроить ASA как базовый межсетевой экран. Другие устройства получают минимальную конфигурацию для поддержки части этой лабораторной работы, посвященной ASA. В этой лабораторной работе используется интерфейс командной строки ASA, аналогичный интерфейсу командной строки IOS, для настройки основных параметров устройства и безопасности.

3. Настройка VPN "На сетевых устройствах должны быть настроены VPN"

Цель: В этой лабораторной работе вы создадите и настроите сеть с несколькими маршрутизаторами, воспользуетесь Cisco IOS для настройки IPsec VPN типа "сеть-сеть", а затем протестируете VPN.

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. Кибербезопасность — мир экспертов и преступников (ПК-2)

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. Packet Tracer — создание компьютерного мира.
2. Packet Tracer — Общение в кибермире
3. Изучить существующие алгоритмы вычисления дайджестов сообщений и написать программу, реализующую хэширование при помощи MD5.
4. Опишите и изучите хэширование при помощи алгоритма MD5, SHA-512, SHA-256

Задания для самостоятельной работы.

1. Поиск работы в сфере кибербезопасности.

2. Идентификация угроз.
3. Задачи профессионалов в сфере кибербезопасности.

Тема 6. 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.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

4 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов 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	Собеседование	6	<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>6 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</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	8	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>8 баллов – студент правильно отвечает на 80-100% вопросов в тесте.</p> <p>4 балла - студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>3 балла – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 1-25% вопросов в тесте.</p>

2.	Атаки, понятия и техники	Собеседование	6	<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>6 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</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(контрольный срез)	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>10 баллов – студент правильно отвечает на 80-100% вопросов в тесте.</p> <p>7 баллов - студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>5 баллов – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 1-25% вопросов в тесте.</p>

3.	Защита данных и конфиденциальности	Собеседование	6	<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>6 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</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	6	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>6 баллов – студент правильно отвечает на 80-100% вопросов в тесте.</p> <p>5 баллов - студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>4 балла – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 1-25% вопросов в тесте.</p>

4.	Защита организации	Собеседование	6	<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>6 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</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	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>10 баллов – студент правильно отвечает на 80-100% вопросов в тесте.</p> <p>7 баллов - студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>5 баллов – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 1-25% вопросов в тесте.</p>

5.	Кибербезопасность — мир экспертов и преступников	Собеседование	6	<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>6 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</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(контрольный срез)	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>10 баллов – студент правильно отвечает на 80-100% вопросов в тесте.</p> <p>7 баллов - студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>5 баллов – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 1-25% вопросов в тесте.</p>

6.	Куб кибербезопасности	Собеседование	6	<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>6 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</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	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>10 баллов – студент правильно отвечает на 80-100% вопросов в тесте.</p> <p>7 баллов - студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>5 баллов – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 1-25% вопросов в тесте.</p>
7.	Посещаемость		10	<p>10 баллов – студент посетил все 100% занятий</p> <p>7-9 баллов – студент посетил не менее 80% занятий</p> <p>4-6 баллов – студент посетил не менее 50% занятий</p> <p>1-3 балла – студент посетил не менее 25% занятий</p> <p>Если студент посетил менее 25% занятий, баллы не начисляются</p>

8.	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
9.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
10.	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

Собеседование

Тема 1. Потребность в кибербезопасности

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.

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

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ПК-2)

1. Что такое SQL-инъекция и чем она отличается от XXE?
2. Что такое: IDS, IPS и EDR. Чем они отличаются?
3. Чем CSRF отличается от XSS?
4. Что такое DLP, как оно работает?
5. Что такое ACL? Как их использовать?
6. Что такое VLAN и когда его использовать? Как работает переключение VLAN?
7. Что такое DoS и DDoS? Какая разница?

Типовые задания для зачета (ПК-2)

1. Настройка SSH "Сетевые устройства должны быть настроены для поддержки SSH."
2. Настройка автоконфигурации безопасности. "На сетевых устройствах должны быть настроены автоматические функции безопасности"
3. Настройка межсетевого экрана "Произвести настройку межсетевого экрана на основе зон"
4. Настройка параметров защиты STP "На сетевых устройствах должны быть настроены параметры для защиты STP"
5. Настройка базовой конфигурации ASA "На сетевых устройствах должны быть настроены базовые параметры"
6. Настройка базовой конфигурации ASA "На сетевых устройствах должны быть настроены базовые параметры"

4.4. Шкала оценивания промежуточной аттестации

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	<p>Не способен продемонстрировать знания в области обеспечения безопасности компьютерных сетей.</p> <p>Не способен администрировать программно-аппаратные средства защиты информации для обеспечения безопасности компьютерных сетей.</p> <p>Не умеет проводить работы связанные с разработкой требований по защите и формированию политики безопасности компьютерных сетей.</p>
---------------------------------	------	--

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.prlib.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.