

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.06.3 International information security

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

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

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

Автор программы:

Кандидат педагогических наук, доцент Самохвалов Алексей Владимирович

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

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

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

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	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).....	20
6. Учебно-методическое и информационное обеспечение дисциплины.....	22
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	22

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-5 Способен организовывать процедуру аттестации объектов вычислительной техники на соответствие требованиям по защите информации

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-5 Способен организовывать процедуру аттестации объектов вычислительной техники на соответствие требованиям по защите информации	Проводит аттестацию объектов вычислительной техники на соответствие требованиям стандартов международной информационной безопасности

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-5 Способен организовывать процедуру аттестации объектов вычислительной техники на соответствие требованиям по защите информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения					
		Очная (семестр)					
		3	4	5	7	8	10
1	Защита информационных процессов в компьютерных системах					+	
2	Защита персональных данных в информационных системах				+		
3	Международная информационная безопасность			+			
4	Микропроцессорная техника	+					

5	Основы электро- и радиоизмерений	+					
6	Преддипломная практика						+
7	Стандарты в области информационной безопасности			+			
8	Техническая защита информации		+	+			
9	Электроника и схемотехника	+					

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «International information security» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «International information security» изучается в 5 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины:

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	144
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Экзамен	36

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лекции	Лаб. раб.	СР	
		О	О	О	
5 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	8	Собеседование; Тестирование
4	Защита организации	4	6	6	Собеседование; Тестирование
5	Кибербезопасность — мир экспертов и преступников	6	6	8	Собеседование; Тестирование
6	Куб кибербезопасности	4	4	8	Собеседование; Тестирование

Тема 1. Потребность в кибербезопасности (ПК-5)

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 киберпреступника, образ злоумышленника.

Тема 2. Атаки, понятия и техники (ПК-5)

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-5)

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.

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-5)

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-5)

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-5)

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 девяток. 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.

Задания для самостоятельной работы.

- 1 Что понимается под термином безопасность информации?
- 2 Что включает в себя защита информации?
- 3 Какие цели преследует защита информации?
- 4 Какое место занимает защита информации в информационной безопасности?

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

5 семестр

- посещаемость – 10 баллов
- текущий контроль – 50 баллов
- контрольные срезы – 2 среза по 5 баллов каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

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

1.	Потребность в кибербезопасности	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 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	5	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>5 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	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 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)	5	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>5 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>

3.	Защита данных и конфиденциальности	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 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	5	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>5 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>

4.	Защита организации	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 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	5	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>5 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>

5.	Кибербезопасность — мир экспертов и преступников	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 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)	5	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>5 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>

6.	Куб кибербезопасности	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 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	5	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>5 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>
7.	Посещаемость		10	<p>10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.</p>
8.	Премиальные баллы		20	<p>Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой 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</p>

9.	Ответ на экзамене	30	25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно»
10.	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

Собеседование

Тема 1. Потребность в кибербезопасности

Какие три типа данных киберпреступники чаще всего пытаются похитить у организаций?

К какой категории, согласно классификации NICE Workforce Framework, относится специализированная оценка поступающей информации о кибербезопасности с целью определения ее пригодности для аналитики?

При какой атаке цель выводится из строя путем отправки ей огромного количества запросов от множества других систем?

Как называют хакера, занимающегося взломами ради продвижения некой идеи?

Как называют хакеров-дилетантов?

Тема 2. Атаки, понятия и техники

Почему важно обеспечить кибербезопасность?

Какие основные понятия?

Что такое Атака и как она происходит?

Какие системы используются для зи?

Приведите пример Кибератаки

Тема 3. Защита данных и конфиденциальности

Какие технологии информационной защиты необходимо использовать чтобы обеспечить надежную защиту ресурсов информационной системы?

Что такое доступность, целостность и конфиденциальность?

Что такое угроза безопасности информации, ущерб безопасности, источник угрозы безопасности, уязвимость, атака?

Что такое санкционированный и несанкционированный доступ к информации, права доступа?

Что такое защита информации, объект защиты, эффективность защиты информации, цель защиты информации, защита информации от утечки?

Тема 4. Защита организации

1 Дайте определение понятий «информационная безопасность», «защита информации».

- 2 Определите составляющие характеристики защищенности информации.
- 3 Дайте определение понятия «политика безопасности».
- 4 Назовите этапы выработки политики безопасности.
- 5 Назовите нормативные документы федерального уровня, определяющие политику информационной безопасности ЯО.

Тема 5. Кибербезопасность — мир экспертов и преступников

- 1 Назовите нормативные документы федерального уровня, определяющие политику информационной безопасности ЯО.
- 2 Назовите характерные свойства функционирования АС СФЗ ЯО с точки зрения информации и информационной безопасности.
- 3 Чем определяются основные требования по защите информации, составляющей государственную и служебные тайны.
- 4 Какие сведения необходимо защищать на ЯО.
- 5 Какие информационные объекты необходимо защищать на ЯО.

Тема 6. Куб кибербезопасности

- 1 Какие угрозы связаны с умышленной деятельностью человека.
- 2 Определите возможные способы нарушения информационной безопасности СФЗ ЯО.
- 3 Перечислите информационные способы нарушения информационной безопасности СФЗ ЯО.
- 4 Перечислите программно-математические способы нарушения информационной безопасности СФЗ ЯО.
- 5 Перечислите физические способы нарушения информационной безопасности СФЗ ЯО.
- 6 Перечислите радиоэлектронные способы нарушения информационной безопасности СФЗ ЯО.

Тестирование

Тема 1. Потребность в кибербезопасности

Как называется защищенная виртуальная сеть, существующая внутри общедоступной сети?

Как называют устройство хранения данных, подключенное к сети?

Назовите три метода идентификации, применяемые в процессе аутентификации.

Назовите два метода проверки целостности данных.

Какой из принципов подразумевает исключение доступа неавторизованных лиц, ресурсов и процессов к информации?

Тема 2. Атаки, понятия и техники

1. В 2016 году были украдены данные 412 миллионов аккаунтов сайта для «взрослых» знакомств AdultFriendFinder (AFF). Злоумышленники воспользовались LFI — local file inclusion — на одном из серверов. А что это такое?

Возможность изменения и выполнения локальных файлов на серверной стороне.

Уязвимость в процессе копирования при записи, из-за которой пользователь мог повысить свои привилегии.

Аппаратная ошибка процессора, позволяющая получить доступ к виртуальной памяти сервера.

2. В 2018 году стало известно об утечке данных клиентов отелей Marriott: данные 383 млн гостей, 8,6 млн номеров кредитных карт, 5 млн незашифрованных паролей. Как вы думаете, сколько времени длилась данная атака?

6 месяцев

1 год

2 года

4 года

3. В этом году было несколько примеров атак на цепь поставок (Supply chain attack), когда злоумышленники действовали не напрямую, а через доверенных партнёров. Свежий пример — атака на индийского аутсорс-гиганта Wipro, чьи сотрудники имеют доступ во внутренние сети европейских и американских компаний. Через Wipro преступники внедрились к его клиентам и установили на компьютерах программу для удалённого доступа. А вы догадаетесь, какую именно?

TeamViewer

Ammyy Admin

ScreenConnect

RDP

4. Еще одной головной болью специалистов по безопасности являются облачные сервисы. В 2017 году в облачном хранилище Amazon была обнаружена открытая база данных 200 млн американских избирателей. Информация была бережно подготовлена и систематизирована для аналитической работы и принадлежала компании Deep Root Analytics, которая обрабатывала их по заказу Республиканской партии. Для доступа к ней было достаточно...

Знать URL или перейти на внутренний субдомен dra-dw (Deep Root Analytics Data Warehouse)

Использовать стандартную связку логин/пароль: administrator/qwerty

Быть клиентом Deep Root Analytics и зайти под своей учетной записью.

Скачать по ссылке с официального сайта Deep Root Analytics в разделе техническая поддержка

5. Даже небольшая ошибка с правами доступа может привести к неприятным последствиям. В этом году с этим столкнулась Почтовая служба США. Любой желающий мог получить доступ к данным 60 млн пользователей и информации о движении коммерческих грузов. Для этого было достаточно:

Использовать SQL-инъекции на сайте при поиске почтового отправления.

Знать URL или внутренний субдомен dra-dw облачного сервера Почтовой службы

Используя свои учетные данные, подключиться к сервисам USPS по API.

Тема 3. Защита данных и конфиденциальности

Что самое главное должно продумать руководство при классификации данных? Варианты ответа:

Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

Необходимый уровень доступности, целостности и конфиденциальности

Оценить уровень риска и отменить контрмеры

Управление доступом, которое должно защищать данные

Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

служебная информация

коммерческая тайна

банковская тайна

конфиденциальная информация

Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

конфиденциальность

целостность

доступность

аутентичность

апшелеруемость

Автоматизированная система должна обеспечивать

надежность

доступность

целостность

контролируемость

Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...

Защита информации

Компьютерная безопасность

Защищенность информации

Безопасность данных

Тема 4. Защита организации

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

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

Виды информационной безопасности:

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

Цели информационной безопасности – своевременное обнаружение, предупреждение:

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

Основные объекты информационной безопасности:

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

Тема 5. Кибербезопасность — мир экспертов и преступников

- 1 Сформулируйте требования и рекомендации по защите речевой информации.
- 2 Сформулируйте требования и рекомендации по защите информации от утечки за счет побочных электромагнитных излучений и наводок..
- 3 Сформулируйте требования и рекомендации по защите информации от несанкционированного доступа.
- 4 Сформулируйте требования и рекомендации по защите информации от фотографических и оптикоэлектронных средств разведки.
- 5 Сформулируйте требования и персоналу СФЗ ЯО.

Тема 6. Куб кибербезопасности

- 1 Сформулируйте принципы обеспечения информационной безопасности СТРС при их использовании на ЯО.
- 2 Перечислите основные этапы классификации СТРС.
- 3 Перечислите основные данные необходимые для классификации СТРС.
- 4 Перечислите классы защищенности СТРС и дайте их краткую характеристику.
- 5 Перечислите подсистемы системы защиты информации СТРС.

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ПК-5)

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 экзамена (ПК-5)

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)
«отлично» (85 - 100 баллов)	ПК-5	Способен проводить аттестацию объектов вычислительной техники на соответствие требованиям международных стандартов информационной безопасности. Демонстрирует знания в области международной информационной безопасности.
«хорошо» (70 - 84 баллов)	ПК-5	Частично способен проводить аттестацию объектов вычислительной техники на соответствие требованиям международных стандартов информационной безопасности. Демонстрирует знания в области международной информационной безопасности.

«удовлетворительно» (50 - 69 баллов)	ПК-5	Недостаточно способен проводить аттестацию объектов вычислительной техники на соответствие требованиям международных стандартов информационной безопасности. Демонстрирует знания в области международной информационной безопасности.
«неудовлетворительно» (менее 50 баллов)	ПК-5	Не способен проводить аттестацию объектов вычислительной техники на соответствие требованиям международных стандартов информационной безопасности. Не обладает знаниями в области международной информационной безопасности.

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

5.1 Методические указания по организации самостоятельной работы обучающихся:

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

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

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

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

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

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

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

5.3 Рекомендации по работе с научной и учебной литературой

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

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

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

В процессе работы с основной и дополнительной литературой студент может:

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

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

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

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

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

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

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Ковган Н. М. Компьютерные сети : учебное пособие. - Минск: РИПО, 2014. - 180 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=463304>
2. 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.