Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

УТВЕРЖДАЮ
Зам. директора
по учебно-методической работе
филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске
_____ В.В. Рожков
«03» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01 Информационная безопасность

Магистерская программа: Безопасность автоматизированных систем

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2024

Смоленск

Программа составлена с учетом ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от «26» ноября 2020 г. № 1455.

Программу составил:

канд. техн. наук, доц. _____ _____В.П. Фомченков_____
подпись ФИО

«18» _____апреля____ 2024 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«24» апреля 2024 г., протокол № 7.

Заведующий кафедрой информационных технологий в экономике и управлении:

_____ __д-р техн. наук, проф. М.И. Дли_____
подпись ФИО

«02» мая 2024 г.

Согласовано:

Заведующий кафедрой вычислительной техники:

_____ __д-р техн. наук, проф. А.С. Федулов_____
подпись ФИО

«02» _____мая____ 2024 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

_____ _____Е.В. Зуева_____
подпись ФИО

«02» _____мая____ 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого типа в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины: изучить понятийный аппарат дисциплины, основные теоретические положения и методы обеспечения безопасности компьютерных сетей; ознакомить обучающихся с принципами построения и функционирования, примерами реализаций современных локальных и глобальных компьютерных сетей и их компонентов; дать представление об уязвимости компьютерных сетей, технических каналах "утечки" информации в компьютерных сетях, основных характеристиках технических средств защиты информации от утечек по техническим каналам в компьютерных сетях, категориях сетевых атак, технологиях обнаружения сетевых вторжений, организационных мерах по защите информации; рассмотреть вопросы информационной безопасности IP-сетей, технологий виртуальных защищенных сетей, защиты беспроводных каналов связи; ознакомить обучающихся с национальными, межгосударственными и международными стандартами в области защиты информации, стандартами по защите сетей промышленных систем автоматизации, видами политик безопасности компьютерных сетей, архитектурой системы управления средствами информационной безопасности сети, основными средствами, способами и принципами построения сетевой инфраструктуры систем защиты информации автоматизированных систем, программно-аппаратными средствами обеспечения защиты информации в компьютерных сетях, особенностями защиты промышленных сетей; сформировать умения и привить навыки применения теоретических знаний для решения профессиональных задач, таких как определение уровня защищенности компьютерных сетей, оценка соответствия механизмов безопасности компьютерной сети требованиям существующих стандартов и нормативных документов, формулировка предложений по устранению выявленных уязвимостей, формирование политики безопасности компьютерных сетей, задание требований к защите информации в компьютерной сети, выбор средств защиты в соответствии с выявленными угрозами по критерию соответствия их стандартам информационной безопасности, разработка моделей сетевой инфраструктуры автоматизированных систем и подсистем безопасности сетевой инфраструктуры автоматизированных систем, проектирование защищенных виртуальных локальных сетей, проектирование защищенных каналов корпоративных сетей, тестирование систем защиты сетевой инфраструктуры автоматизированных систем, документирование технических средств компьютерных сетей с учетом требований по обеспечению защиты информации, настройка средств защиты сетевого трафика активного сетевого оборудования, конфигурирование безопасной сетевой инфраструктуры IoT, конфигурирование и настройка защищенного беспроводного канала связи.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Информационная безопасность компьютерных сетей относится *к части, формируемой участниками образовательных отношений*.

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

Б1.В.01 Организационно-правовые механизмы обеспечения информационной безопасности;
Б1.В.03 Проектирование программного обеспечения автоматизированных систем.

Перечень последующих дисциплин и практик, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной:
Б1.В.05 Интеллектуальный анализ и моделирование информационных систем и процессов;
Б1.В.06 Криптографические методы и средства защиты информации;
Б1.В.07 Технические средства защиты информации;
Б1.В.ДВ.02.01 Комплексная защита корпоративной информации;
Б1.В.ДВ.02.02 Аудит информационной безопасности;
Б1.В.ДВ.03.01 Безопасность веб-приложений;
Б1.В.ДВ.03.02 Технологии и методы защиты информации в сети Интернет;
Б2.В.02 (П) Проектно-технологическая практика;
Б2.В.03 (П) Преддипломная практика;
Б3.01 Подготовка к защите и защита выпускной квалификационной работы.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-1. Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ) организации на основе современных положений СМИБ	ПК-1.2 Способен проектировать аппаратные средства для защиты информации автоматизированных систем.	Знает: принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; эталонную модель взаимодействия открытых систем; технические каналы "утечки" информации в компьютерных сетях; основные средства, способы и принципы построения сетевой инфраструктуры систем защиты информации автоматизированных систем; особенности защиты промышленных сетей; основные характеристики технических средств защиты информации от утечек по техническим каналам в компьютерных сетях; программно-аппаратные средства обеспечения защиты информации в компьютерных сетях; функции и особенности функционирования межсетевых экранов; технологии виртуальных защищенных сетей; технологии безопасности беспроводных сетей; архитектуры защищенных промышленных информационных сетей. Умеет: разрабатывать модели сетевой инфраструктуры автоматизированных систем и подсистем безопасности сетевой инфраструктуры автоматизированных систем; проектировать

		защищенные виртуальные локальные сети; проектировать защищенные каналы корпоративных сетей; тестировать системы защиты сетевой инфраструктуры автоматизированных систем; документировать технические средства компьютерных сетей с учетом требований по обеспечению защиты информации. Владеет: умением анализировать основные характеристики и возможности компьютерных сетей по передаче информации; навыками выбора мер защиты информации, подлежащих реализации в системе защиты сетевой инфраструктуры автоматизированной системы; навыками определения видов и типов средств защиты информации, обеспечивающих реализацию технических мер защиты компьютерных сетей; методами исследования моделей сетевой инфраструктуры автоматизированных систем и подсистем безопасности сетевой инфраструктуры автоматизированных систем; навыками настройки средств защиты сетевого трафика активного сетевого оборудования; навыками конфигурирования безопасной сетевой инфраструктуры IoT; навыками конфигурирования и настройки защищенного беспроводного канала связи; навыками контроля безотказного функционирования технических средств защиты информации в компьютерных сетях.
ПК-3 Способен управлять безопасностью компьютерных систем и сетей.	ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей.	Знает: принципы построения компьютерных сетей; уязвимости компьютерных сетей; проблемы и угрозы информационной безопасности сетевого объекта; категории сетевых атак; технологии обнаружения сетевых вторжений; национальные, межгосударственные и международные стандарты в области защиты информации; стандарты по защите сетей промышленных систем автоматизации. Умеет: определить уровень защищенности компьютерных сетей; оценить соответствие механизмов безопасности компьютерной сети требованиям существующих нормативных документов; формулирует предложения по устранению выявленных уязвимостей. Владеет: умением производить анализ политики безопасности на предмет адекватности; навыками разработки предложений по устранению выявленных уязвимостей; навыками анализа стандартов информационной безопасности.
	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей.	Знает: виды политик безопасности компьютерных сетей; возможности используемых и планируемых к использованию средств защиты информации; архитектуру системы управления средствами информационной безопасности сети; организационные меры по защите информации.

		Умеет: формировать политики безопасности компьютерных сетей; определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной сети; задавать требования к защите информации в компьютерной сети; проводить выбор средств защиты в соответствии с выявленными угрозами по критерию соответствия их стандартам информационной безопасности. Владеет: умением формулирования задания по безопасности компьютерных сетей; навыками выполнения анализа безопасности компьютерных сетей и разработки рекомендаций по эксплуатации систем защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 1										Семестр 2										Итого за курс										Каф.	Семестры
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель		
				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего			
11	Б1.В.04	Информационная безопасность компьютерных сетей											Экз КР	216	104	34	34	18	18	76	36	6		Экз КР	216	104	34	34	18	18	76	36	6		20	2

ОБОЗНАЧЕНИЯ:
Виды промежуточной аттестации (виды контроля):
Экз - экзамен;
ЗаО - зачет с оценкой;
За – зачет;
Виды работ:
Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КРП – курсовая работа (курсовой проект);
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	Лекционные занятия 17 шт. по 2 часа: 1.1. Введение в дисциплину. Основные понятия и определения. 1.2. Проблемы и угрозы информационной безопасности сетей. 1.3. Управление безопасностью компьютерных сетей. 1.4. Отечественные и зарубежные стандарты информационной безопасности компьютерных сетей. 1.5. Введение в сетевой информационный обмен. 1.6. Межсетевые экраны. Схемы сетевой защиты на базе МЭ. 1.7. Категории сетевых атак. 1.8. Технологии обнаружения сетевых вторжений. 1.9. Виртуальные локальные сети. 1.10. Конфигурирование виртуальных локальных сетей. 1.11. Виртуальные защищенные сети VPN. 1.12. Технологии и протоколы VPN. 1.13. Построение VPN на основе маршрутизаторов. 1.14. Понятие и разновидности промышленных информационных сетей. 1.15. Промышленный Ethernet. Интегрированные системы промышленной автоматизации. 1.16. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. 1.17. Защищенные системы беспроводной связи. Беспроводные виртуальные сети.
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа: 2.1. Мониторинг сетевых пакетов в IP-сетях. 2.2. Исследование методов защиты сетевого трафика. 2.3. Проектирование защищенной виртуальной локальной сети. 2.4. Защита канальной инфраструктуры сети. 2.5. Проектирование защищенной корпоративной сети. 2.6. Сетевая защита на базе межсетевых экранов. 2.7. Управление трафиком межсетевого взаимодействия. 2.8. Конфигурирование безопасной сетевой инфраструктуры IoT. 2.9. Конфигурирование и настройка беспроводного канала связи в соответствии с требованиями информационной безопасности.
3	Практические занятия 9 шт. по 2 часа: 3.1. Формирование политики информационной безопасности компании. 3.2. Формирование политики безопасности компьютерных сетей. 3.3. Разработка требований по защите компьютерных сетей на основе стандартов информационной безопасности компьютерных сетей и сетей связи. 3.4. Разработка требований по защите промышленных компьютерных сетей на основе стандартов информационной безопасности промышленных систем и сетей. 3.5. Расчет адресного пространства IP-сети. 3.6. Проектирование конфигурации IP-сети. 3.7. Анализ безопасности трафика на примере протоколов TCP и UDP. 3.8. Анализ безопасности трафика на примере протокола ICMP. 3.9. Безопасность сети на основе технологии сегментации трафика.
4	Консультации по курсовой работе: 9 шт. по 2 часа.

5	Курсовая работа «Разработка предложений по повышению информационной безопасности ЛВС организации».
6	Самостоятельная работа студентов: 6.1. Подготовка к защите лабораторных работ. 6.2. Подготовка к ответам на контрольные вопросы на практических занятиях. 6.3. Самостоятельное изучение теоретических материалов по следующим вопросам. Лекция 1.3. Управление безопасностью компьютерных сетей. Вопросы: Задачи управления безопасностью компьютерных сетей. Лекция 1.4. Отечественные и зарубежные стандарты информационной безопасности компьютерных сетей. Вопросы: Зарубежные стандарты информационной безопасности. Лекция 1.5. Введение в сетевой информационный обмен. Вопросы: Модель взаимодействия открытых систем (OSI). Лекция 1.7. Категории сетевых атак. Вопросы: Средства анализа защищенности сетевых протоков и сервисов. Лекция 1.9. Виртуальные локальные сети. Вопросы: Идентификация сетей VLAN. Протокол VTP. Лекция 1.11. Виртуальные защищенные сети VPN. Вопросы: Классификация VPN. Основные варианты архитектуры VPN. Лекция 1.12. Технологии и протоколы VPN. Вопросы: Сетевые защищенные протоколы. Лекция 1.13. Построение VPN на основе маршрутизаторов. Вопросы: Принципы маршрутизации. Статическая и динамическая маршрутизация. Лекция 1.14. Понятие и разновидности промышленных информационных сетей. Вопросы: Сетевая информационная структура предприятия. Лекция 1.15. Промышленный Ethernet. Интегрированные системы промышленной автоматизации. Вопросы: Интегрированные системы промышленной автоматизации. Лекция 1.16. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Вопросы: Угрозы безопасности промышленных предприятий. Управление безопасностью на производстве согласно ISA S99. Техническая архитектура безопасности на основе IEC 62443. Лекция 1.17. Защищенные системы беспроводной связи. Беспроводные виртуальные сети. Стандарты безопасности WPA/WPA2.

	Стандарт IEEE 802.1x/EAP. Системы обнаружения вторжений в беспроводных сетях. 6.4. Выполнение курсовой работы «Разработка предложений по повышению информационной безопасности ЛВС организации». 6.5. Подготовка к экзамену по дисциплине (оценочные материалы приведены в разделе 6 настоящей РПД).

Текущий контроль:
- проверка конспектов лекций и дополнительных теоретических материалов;
- проверка отчетов по лабораторным работам;
- защита лабораторных работ;
- проверка выполнения заданий практических занятий;
- проверка выполнения заданий курсовой работы;
- проверка отчета по курсовой работе;
- защита курсовой работы.

Индикаторы достижения компетенции	**Вид текущего контроля**	**Тема**
ПК-1.2	Проверка конспектов лекций и дополнительных теоретических материалов. Проверка отчетов по лабораторным работам. Защита лабораторных работ. Проверка выполнения заданий практических занятий. Проверка выполнения заданий курсовой работы. Проверка отчета по курсовой работе. Защита курсовой работы.	1.1. Введение в дисциплину. Основные понятия и определения. 1.5. Введение в сетевой информационный обмен. 1.6. Межсетевые экраны. Схемы сетевой защиты на базе МЭ. 3.5. Расчет адресного пространства IP-сети. 3.6. Проектирование конфигурации IP-сети. 3.7. Анализ безопасности трафика на примере протоколов TCP и UDP. 3.8. Анализ безопасности трафика на примере протокола ICMP. 3.9. Безопасность сети на основе технологии сегментации трафика. 1.9. Виртуальные локальные сети. 1.10. Конфигурирование виртуальных локальных сетей. 1.11. Виртуальные защищенные сети VPN. 1.12. Технологии и протоколы VPN. 1.13. Построение VPN на основе маршрутизаторов. 2.3. Проектирование защищенной виртуальной локальной сети. 2.4. Защита канальной инфраструктуры сети. 2.5. Проектирование защищенной корпоративной сети. 2.6. Сетевая защита на базе межсетевых экранов. 2.7. Управление трафиком межсетевого взаимодействия. 1.14. Понятие и разновидности промышленных информационных сетей. 1.15. Промышленный Ethernet. Интегрированные системы промышленной автоматизации. 1.16. Защита информационных сетей на

		промышленных предприятиях и объектах критической инфраструктуры. 2.8. Конфигурирование безопасной сетевой инфраструктуры IoT. 1.17. Защищенные системы беспроводной связи. Беспроводные виртуальные сети. 2.9. Конфигурирование и настройка беспроводного канала связи в соответствии с требованиями информационной безопасности. 5. Курсовая работа «Разработка предложений по повышению информационной безопасности ЛВС организации».
ПК-3.1	Проверка конспектов лекций и дополнительных теоретических материалов. Проверка отчетов по лабораторным работам. Защита лабораторных работ. Проверка выполнения заданий практических занятий. Проверка выполнения заданий курсовой работы. Проверка отчета по курсовой работе. Защита курсовой работы.	1.1. Введение в дисциплину. Основные понятия и определения. 1.2. Проблемы и угрозы информационной безопасности сетей. 1.4. Отечественные и зарубежные стандарты информационной безопасности компьютерных сетей. 1.5. Введение в сетевой информационный обмен. 1.7. Категории сетевых атак. 1.8. Технологии обнаружения сетевых вторжений. 2.1. Мониторинг сетевых пакетов в IP-сетях. 3.7. Анализ безопасности трафика на примере протоколов TCP и UDP. 3.8. Анализ безопасности трафика на примере протокола ICMP. 1.16. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. 5. Курсовая работа «Разработка предложений по повышению информационной безопасности ЛВС организации».
ПК-3.2	Проверка конспектов лекций и дополнительных теоретических материалов. Проверка отчетов по лабораторным работам. Защита лабораторных работ. Проверка выполнения заданий практических занятий. Проверка выполнения заданий курсовой работы. Проверка отчета по курсовой работе. Защита курсовой работы.	1.1. Введение в дисциплину. Основные понятия и определения. 1.3. Управление безопасностью компьютерных сетей. 1.6. Межсетевые экраны. Схемы сетевой защиты на базе МЭ. 1.9. Виртуальные локальные сети. 1.13. Построение VPN на основе маршрутизаторов. 1.16. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. 1.17. Защищенные системы беспроводной связи. Беспроводные виртуальные сети. 3.1. Формирование политики информационной безопасности компании. 3.2. Формирование политики безопасности компьютерных сетей. 3.3. Разработка требований по защите компьютерных сетей на основе стандартов

		информационной безопасности компьютерных сетей и сетей связи. 3.4. Разработка требований по защите промышленных компьютерных сетей на основе стандартов информационной безопасности промышленных систем и сетей. 2.2. Исследование методов защиты сетевого трафика. 5. Курсовая работа «Разработка предложений по повышению информационной безопасности ЛВС организации».

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица - Образовательные технологии, используемые при реализации различных видов учебных занятий по дисциплине

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Классическая (традиционная, информационная) лекция в формате мультимедийных презентаций. Индивидуальные и групповые консультации по дисциплине
2	Практические занятия	Технология обучения на основе решения задач и выполнения упражнений. Метод контрольных вопросов.
3	Лабораторные работы	Технология выполнения лабораторных заданий индивидуально. Технология проблемного обучения на основе анализа результатов лабораторной работы: индивидуальный опрос, представление студентом результатов лабораторной работы в форме отчета.
4	Консультации по курсовой работе	Индивидуальные и групповые консультации. Информационно-коммуникационные технологии: технология взаимодействия со студентами в режиме связи «offline»; технология взаимодействия со студентами в режиме связи «online».
5	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
6	Контроль (промежуточная аттестация: экзамен)	Технология устного опроса.

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ – ДЛЯ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает как текущий контроль успеваемости, так и промежуточную аттестацию.

Оценочные средства текущего контроля успеваемости:

Вопросы для защиты лабораторной работы «Мониторинг сетевых пакетов в IP-сетях»

1. Назначение и принцип работы протокола ICMP.
2. Какова структура заголовка ICMP сообщения?
3. Назначение и принцип работы протокола UDP.
4. Как используется протокол UDP при определении IP-адреса хоста по его доменному имени?
5. Каким образом в списке пакетов UDP можно найти запись стандартного запроса к какому-либо хосту? Какие сведения содержаться в этой строке.
6. Каким образом по сведениям о стандартном запросе можно определить IP и MAC-адреса компьютера-источника запроса, основного шлюза?
7. Какие сведения о стандартном DNS-запросе содержатся в окне User Datagram Protocol? В окне Domain Name System (query)?
8. Как изменяются роли источника и назначения в DNS-запросе и DNS-ответе?
9. Назначение и принцип работы протокола TCP.
10. Как называется процесс установления сеанса TCP между клиентом и сервером? Из каких этапов он состоит?
11. Каким образом в списке пакетов найти сегмент первого этапа трехэтапного квитирования? Как перейти на следующий сегмент трехэтапного квитирования?
12. Какие сведения о сегменте TCP содержатся в окне Transmission Control Protocol?
13. Каково назначение номера ISN (Initial Sequence Number - начальный номер последовательности) и как можно узнать его значение в просматриваемом сегменте TCP?
14. На основании какой информации из заголовка сегмента TCP можно сделать вывод о том, что соединение TCP настроено?
15. Каким образом можно отфильтровать пакеты соединения между двумя сокетами?
16. Как найти заключительный пакет TCP-сеанса?

Вопросы для защиты лабораторной работы «Исследование методов защиты сетевого трафика»

1. В чем состоят различия возможностей локального и сетевого входа в систему?
2. Настройка общего доступа к дискам и папкам компьютера.
3. Настройка удаленного доступа к рабочему столу.
4. Для каких целей проводится мониторинг трафика сети?
5. Основные возможности анализатора сетевого трафика.
6. Как выполнить захват сетевого трафика рабочей станции?
7. Как можно определить принадлежность пакета узлу сети и протоколу?
8. Как получить общую статистику по захвату?
9. Как получить информацию о распределении трафика по протоколам?
10. Какой трафик потенциально опасен?
11. Использование протокола IPSec для блокирования ICMP-трафика.

Вопросы для защиты лабораторной работы «Проектирование защищенной виртуальной локальной сети»

1. Дайте определение виртуальной локальной сети (VLAN).
2. Что нужно сделать, чтобы заработала используемая по умолчанию виртуальная локальная сеть vlan1?
3. Что собой представляет магистральная связь (Trunk link), каково ее назначение?
4. Как создать магистральную связь trunk между коммутаторами?
5. Для каких целей используется режим связи доступа (Access link)?
6. Из каких этапов состоит процесс конфигурирования виртуальных локальных сетей?
7. Как сконфигурировать виртуальную сеть для компьютеров, входящих в эту виртуальную сеть?

Вопросы для защиты лабораторной работы «Защита канальной инфраструктуры сети»

1. Каковы цели и механизм атаки канального уровня типа MAC-flooding?
2. Каковы цели и механизм атаки канального уровня типа MAC-spoofing?
3. Какую защиту позволяет реализовать механизм port security?
4. Какие методы построения списков разрешенных MAC-адресов вы знаете?
5. В чем состоят настройки механизма port security на коммутаторе?
6. Описать назначение и принцип работы механизма port security sticky для статического метода формирования MAC-адресов.
7. Возможно ли применение механизма port security для защиты от атак типа ARP spoofing и DHCP spoofing?

Вопросы для защиты лабораторной работы «Проектирование защищенной корпоративной сети»

1. Дайте определение маршрутизации, маршрута, таблицы маршрутов, маршрутизатора.
2. Как соединить маршрутизаторы по последовательному интерфейсу?
3. Как настраивается интерфейс маршрутизатора, подключенный к внешней сети?
4. Как настраивается интерфейс маршрутизатора, подключенный к внутренней сети?
5. Каким способы задания маршрутов вы знаете?
6. Как задать статический маршрут к определенной сети?
7. К каким интерфейсам маршрутизатора можно подключить конечное оборудование?
8. Дайте определение статической и динамической маршрутизации.
9. Какое оборудование Cisco поддерживает технологию организации VPN-туннеля?

Вопросы для защиты лабораторной работы «Сетевая защита на базе межсетевых экранов»

1. Дайте определение межсетевого экрана (МЭ). Какие функции он выполняет?
2. Какие типы МЭ можно выделить по признаку охвата контролируемых потоков данных?
3. Какие типы МЭ можно выделить в зависимости от уровня, на котором происходит управление доступом?
4. Какие типы МЭ можно выделить в зависимости от реализации возможности отслеживания активных соединений?
5. Назовите дополнительные механизмы защиты и управления информационными потоками, реализуемые в МЭ?
6. Что собой представляет первичная фильтрация пакетов, и каким образом её можно реализовать на маршрутизаторе?
7. В чем состоит основная идея технологии CBAC?

Вопросы для защиты лабораторной работы «Управление трафиком межсетевого взаимодействия»

1. Дайте определение маршрутизатора. Что такое шлюз?
2. Какова топология соединения подсетей с помощью маршрутизатора?
3. Какие настройки необходимо выполнить, чтобы хосты двух подсетей, соединенных через маршрутизатор, стали видеть друг друга?
4. Дайте определение списка управления доступом (ACL). Для каких целей он используется?
5. Какие существуют типы и способы создания ACL-списков?
6. Из каких этапов состоит создание ACL-списка?
7. Каков синтаксис именованного расширенного списка?
8. Каким образом созданный список прикрепляется к интерфейсу маршрутизатора?
9. Как просмотреть списки доступа маршрутизатора? Как удалить список доступа?
10. Что собой представляет шаблон маски правила списка? Для каких целей он используется? В чем его отличие от маски сети?
11. Что такое обратная маска? Каким образом её можно использовать для формирования шаблона маски правила списка?
12. Каково действие шаблонов `host` и `any` в правиле списка доступа?

Вопросы для защиты лабораторной работы «Конфигурирование безопасной сетевой инфраструктуры IoT»

1. Дайте определение таким понятиям как «Индустрия 4.0», «Промышленный Интернет», «Интернет вещей», «Умное предприятие», «Умный дом».
2. Какие функциональные уровни имеет архитектура IoT?
3. Что вы отнесете к сетевой инфраструктуре IoT?
4. Из каких устройств состоит интеллектуальная домашняя сеть?
5. Что необходимо сделать, чтобы подключить новое сетевое устройство в интеллектуальную домашнюю сеть? Какие способы подключения вы знаете?
6. Каким образом добавляется проводное устройство ввода-вывода?
7. Как добавить беспроводное устройство ввода-вывода?
8. Каким образом настаивается интеллектуальное сетевое устройство?
9. Какие механизмы обеспечивают защиту сетевой инфраструктуры IoT от несанкционированного доступа?

Вопросы для защиты лабораторной работы «Конфигурирование и настройка беспроводного канала связи в соответствии с требованиями информационной безопасности»

1. Сравните беспроводные локальные сети с локальными сетями.
2. Дайте определение точки доступа.
3. Какой состав оборудования необходим для создания полностью беспроводной защищенной сети?
4. Каким образом настроить прохождение VLAN-трафика в беспроводном маршрутизаторе?
5. С какими угрозами информационной безопасности приходится сталкиваться в беспроводных сетях связи?
6. Из каких этапов состоит процесс аутентификации клиента беспроводной локальной сети IEEE 802.11?
7. Назовите особенности VPN в виртуальных средах.

Контрольные вопросы для обсуждения на практическом занятии по теме «Формирование политики информационной безопасности компании»

1. Дайте определение политики информационной безопасности.

2. Какие вы можете назвать принципы формирования политики информационной безопасности?
3. Назовите виды политики информационной безопасности?
4. Структура документа «Политика информационной безопасности».
5. Каково содержание раздела «Объекты защиты» документа «Политика информационной безопасности»?
6. Каково содержание раздела «Основные угрозы безопасности информации» документа «Политика информационной безопасности»?
7. Сформулируйте предложения по формированию политики информационной безопасности организации (по вариантам)?

Контрольные вопросы для обсуждения на практическом занятии по теме «Формирование политики безопасности компьютерных сетей»

1. Какие составляющие политики информационной безопасности компании следует отнести к безопасности компьютерных сетей?
2. Какова структура и содержание разделов документа «Политика межсетевого взаимодействия»?
3. Какова структура и содержание разделов документа «Политика использования VPN»?
4. Какова структура и содержание разделов документа «Правила работы в локальной вычислительной сети»?
5. Сформулируйте предложения по формированию политики безопасности компьютерной сети организации (по вариантам)?

Контрольные вопросы для обсуждения на практическом занятии по теме «Разработка требований по защите компьютерных сетей на основе стандартов информационной безопасности компьютерных сетей и сетей связи»

1. Что собой представляет система сертификации ГОСТ Р?
2. Что означают аббревиатуры ГОСТ Р ИСО и ГОСТ Р МЭК?
3. Является ли система сертификации ГОСТ Р обязательной?
4. В каких стандартах сформулированы требования, предъявляемые к информационной безопасности компьютерных сетей и сетей связи?
5. Что из себя представляет система сертификации ГОСТ Р?
6. В каких стандартах сформулированы требования, предъявляемые к информационной безопасности компьютерных сетей?
7. Каковы основные положения стандарта ГОСТ Р ИСО/МЭК 27033-1-2011?
8. Какие вопросы в области защиты компьютерных сетей регулирует стандарт ГОСТ Р ИСО/МЭК 27033-3-2014?
9. Нормативное регулирование обеспечения безопасности функционирования российского сегмента сети Интернет.
10. Сформулируйте требования по защите компьютерной сети организации (по вариантам)? Какими стандартами вы при этом руководствовались?

Контрольные вопросы для обсуждения на практическом занятии по теме «Разработка требований по защите промышленных компьютерных сетей на основе стандартов информационной безопасности промышленных систем и сетей»

1. Какими правовыми актами и нормативными документами регулируются вопросы обеспечения безопасности объектов критической инфраструктуры?

2. В каких стандартах сформулированы требования, предъявляемые к информационной безопасности промышленных систем автоматизации и промышленных сетей?
3. Какой российский стандарт описывает безопасность оборудования с ограниченными возможностями с точки зрения применения информационных технологий в домашних сетях?
4. Какие методы защиты каналов связи применяются на промышленных предприятиях?
5. Назовите основные положения стандарта ISA-99.
6. Назовите основные положения семейства стандартов IEC 62443.
7. В каких национальных стандартах РФ рассматриваются вопросы защиты промышленных систем и сетей?
8. Какие требования к составлению программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики предъявляет стандарт ГОСТ Р МЭК 62443-2-1-2015?
9. Каковы основные требования к системной безопасности ГОСТ Р МЭК 62443-3-3-2016?
10. Сформулируйте требования по защите промышленной сети организации (по вариантам)? Какими стандартами вы при этом руководствовались?

Контрольные вопросы для обсуждения на практических занятиях по темам «Расчет адресного пространства IP-сети» и «Проектирование конфигурации IP-сети»

1. Какова структура IP-адреса версии IPv4.
2. Какие существуют классы IP-адресов?
3. Каким образом по IP-адресу сети можно определить класс сети?
4. Что такое широковещательный IP-адрес?
5. Что собой представляет маска сети, каково ее назначение?
6. Каковы стандартные маски подсетей для IP- адресов классов A, B, C как в десятичной нотации, так и в виде двоичных чисел?
7. Каким образом по IP-адресу и маске можно определить адрес сети? Первый и последний доступный IP-адреса сети? Широковещательный адрес сети?
8. Какие условия должны быть выполнены, чтобы компьютеры сети «видели» друг друга?
9. Какие существуют способы подключения к сетевому оборудованию для его конфигурирования? Какой способ предпочтительнее и почему? Что означает аббревиатура CLI?
10. Каким образом можно просмотреть текущую конфигурацию коммутатора?
11. Какие существуют виды конфигураций коммутатора? Где они хранятся?
12. Каким образом можно обезопасить себя от потери конфигурационной информации?
13. Какие способы изменения конфигурации коммутатора вы можете назвать?
14. Каким образом можно изменить имя коммутатора как хоста сети?
15. Как задаются IP-адреса и маски сети коммутаторам?
16. В какой секции конфигурационного файла хранится информация о IP-адресе и маске сети коммутатора?

Контрольные вопросы для обсуждения на практических занятиях по темам «Анализ безопасности трафика на примере протоколов TCP и UDP» и «Анализ безопасности трафика на примере протокола ICMP»

1. Дайте определение DoS-атаки, что является её целью?
2. Назовите причины возникновения DoS-условия.
3. В чем состоит отличие DDoS-атаки?
4. Какие типы DoS-атак вы знаете?
5. Каковы особенности DoS-атаки типа TCP SYN Flood?
6. Каким образом можно смоделировать атаку TCP SYN Flood? Как её идентифицировать?

7. Каковы особенности DoS-атаки типа UDP Flood?
8. Каким образом можно смоделировать атаку UDP Flood? Как её идентифицировать?
9. Каковы особенности DoS-атаки типа ICMP Flood?
10. Каким образом можно смоделировать атаку ICMP Flood? Как её идентифицировать?
11. Какие выводы вы сделали по итогам практического занятия?

Контрольные вопросы для обсуждения на практическом занятии по теме «Безопасность сети на основе технологии сегментации трафика»

1. Что такое сегмент сети, подсеть?
2. По каким причинам целесообразно производить разбиение сети на подсети?
3. Какие методы сегментации сети вы знаете?
4. Каким образом осуществляется разбиение сети на подсети с помощью маски?
5. Как определить необходимое число разрядов на адрес подсети? На адрес хоста?
6. Какие меры необходимо предпринять, чтобы предотвратить несанкционированный доступ к ресурсам одной подсети из другой?
7. Как в сегментированной сети обеспечить прохождение трафика между подсетями?

Вопросы для защиты курсовой работы

1. Охарактеризуйте сетевую инфраструктуру организации.
2. Какие вы выявили недостатки в обеспечении информационной безопасности локальной сети?
3. Какие угрозы информационной безопасности в компьютерной сети актуальны для компании?
4. Требования каких стандартов информационной безопасности компьютерных сетей и сетей связи не выполняются или выполняются не в полной мере?
5. Какие объекты защиты информации в сети вы выделили?
6. Какие предложения по повышению информационной безопасности сети вы разработали?
7. Что из предлагаемого относится к организационному уровню защиты?
8. Какие нормативные документы вы разработали?
9. Назовите основные положения политики информационной безопасности локальной сети компании.
10. Какие методы защиты информации вы выбрали? Обоснуйте свой выбор.
11. Каким образом вы обеспечиваете сегментацию сетевого трафика?
12. Каким образом вы обеспечиваете защиту от сетевых атак?
13. Какие аппаратные средства понадобятся для реализации ваших предложений?
14. Была ли вами выполнена проверка работоспособности предлагаемых решений?

Примерный перечень тем курсовой работы:

1. Разработка предложений по повышению информационной безопасности ЛВС промышленного предприятия.
2. Разработка предложений по повышению информационной безопасности ЛВС финансовой организации.
3. Разработка предложений по повышению информационной безопасности ЛВС электрогенерирующей компании.
4. Разработка предложений по повышению информационной безопасности ЛВС органа государственного управления.
5. Разработка предложений по повышению информационной безопасности ЛВС образовательной организации.

6. Разработка предложений по повышению информационной безопасности ЛВС страховой компании.
7. Разработка предложений по повышению информационной безопасности ЛВС гостиницы.
8. Разработка предложений по повышению информационной безопасности ЛВС организации здравоохранения.
9. Разработка предложений по повышению информационной безопасности ЛВС предприятия оптовой торговли.
10. Разработка предложений по повышению информационной безопасности ЛВС организации культуры.

По согласованию с преподавателем обучающийся может выбрать индивидуальную тему курсовой работы, соответствующую цели и задачам дисциплины, по уровню сложности не ниже стандартного задания.

Результаты текущего контроля по вышеуказанным в разделе 4 видам фиксируются с использованием трехбалльной системы (0, 1, 2) в виде контрольных недель - при принятой в филиале системе на 6-й и 12-й учебной неделе семестра, а также учитываются преподавателем при осуществлении промежуточной аттестации по настоящей дисциплине.

Форма промежуточной аттестации по настоящей дисциплине – *экзамен во 2-м семестре.*

Оценочные средства для промежуточной аттестации:
Вопросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к экзамену)

1. Основные понятия и составляющие информационной безопасности компьютерных сетей.
2. Актуальность проблемы обеспечения информационной безопасности современных сетей.
3. Проблемы информационной безопасности сетей.
4. Угрозы информационной безопасности сетей.
5. Классификация методов защиты информации.
6. Общие вопросы формирования политики безопасности.
7. Задачи управления безопасностью компьютерных сетей.
8. Политика безопасности компьютерных сетей.
9. Архитектура системы управления средствами информационной безопасности сети.
10. Отечественные стандарты информационной безопасности компьютерных сетей.
11. Зарубежные стандарты информационной безопасности.
12. Сетевые стандарты и технологии.
13. Модель взаимодействия открытых систем (OSI).
14. Набор протоколов TCP/IP. Межсетевой протокол IP.
15. Функции и особенности функционирования МЭ на различных уровнях модели OSI.
16. Схемы сетевой защиты на базе МЭ.
17. Категории сетевых атак.
18. Средства анализа защищенности сетевых протоков и сервисов.
19. Системы обнаружения атак IDS. Компоненты и архитектура.
20. Методы реагирования на сетевые атаки.
21. Виртуальные локальные сети. Типы виртуальных сетей.
22. Идентификация сетей VLAN. Протокол VTP.

23. Конфигурирование виртуальных локальных сетей.
24. Основные понятия и функции сети VPN.
25. Варианты построения виртуальных защищенных каналов.
26. Средства обеспечения безопасности VPN.
27. Классификация VPN.
28. Основные варианты архитектуры VPN.
29. Сетевые защищенные протоколы.
30. Маршрутизация и автономные системы.
31. Принципы маршрутизации.
32. Статическая и динамическая маршрутизация.
33. Технология организации VPN-туннеля.
34. Промышленные информационные сети: понятие, особенности, разновидности.
35. Сетевая информационная структура предприятия.
36. Информационные сети технологического и полевого уровней.
37. Промышленный Ethernet.
38. Интегрированные системы промышленной автоматизации.
39. Особенности защиты информации на промышленных предприятиях и критически важных объектах.
40. Угрозы безопасности промышленных предприятий.
41. Вопросы безопасности сетевой инфраструктуры в концепции ИБ предприятия.
42. Защита промышленных систем автоматизации от вредоносного ПО.
43. Управление безопасностью на производстве согласно ISA S99.
44. Техническая архитектура безопасности на основе IEC 62443.
45. Методы защиты промышленных сетей.
46. Интегрированные системы безопасности.
47. Механизмы аутентификации беспроводных клиентов по стандарту IEEE 802.11.
48. Комплексная система обеспечения безопасности беспроводных сетей по стандарту IEEE 802.11i.
49. Стандарты безопасности WPA/WPA2.
50. Стандарт IEEE 802.1x/EAP.
51. Развертывание беспроводных виртуальных сетей.
52. Системы обнаружения вторжений в беспроводных сетях.

Примеры практических заданий, выносимых на экзамен, для проверки практических умений и навыков студентов по дисциплине

Задача 1.

По заданному IP адресу устройства и маске подсети определить:

- адрес широковещательной рассылки;
- первый и последний доступные IP адреса для этой сети.

IP-адрес устройства: 113.83.34.54. Маска подсети: 255.254.0.0

Построить модель сети из двух компьютеров, соединенных через коммутатор. Задать компьютерам первый и последний доступные IP адреса рассчитанной сети. Проверить работоспособность сети.

Задача 2.

В сети заданной конфигурации настроить сеть vlan.

Задача 3.

В сети заданной конфигурации настроить защищенный маршрут из сети 172.16.10.0 к серверу.

В филиале используется система с традиционной шкалой оценок – "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", "зачтено", "не зачтено".

Применяемые критерии оценивания по дисциплинам (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23):

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявившему творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «эталонный».
«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, обнаружившему полное знание материала изученной дисциплины, успешно выполняющему предусмотренные задания, усвоившему основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнивший практическое задание, но допустивший при этом непринципиальные ошибки. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «продвинутый».
«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившему другие практические задания из того же раздела дисциплины.. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «пороговый».
«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции на уровне «пороговый», закреплённые за дисциплиной, не сформированы.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебное и учебно-лабораторное оборудование

Для проведения лекционных занятий используется учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для проведения практических занятий используется учебная аудитория для практических занятий, выполняемых в компьютерном классе, оснащенная специализированной мебелью; доской аудиторной; персональными компьютерами, связанными локальной вычислительной сетью с подключением к сети Интернет.

Для проведения занятий лабораторного типа используется учебная аудитория для лабораторных работ, выполняемых в компьютерном классе, оснащенная специализированной мебелью; доской аудиторной; персональными компьютерами, связанными локальной вычислительной сетью с подключением к сети Интернет.

Для проведения консультаций по курсовой работе используется учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная специализированной мебелью; доской аудиторной.

Для самостоятельной работы обучающихся по дисциплине используется помещение для самостоятельной работы обучающихся, оснащенное специализированной мебелью; доской аудиторной; персональным компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

8. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере;
- используется специальная учебная аудитория для лиц с ЛОВЗ – ауд. 106 главного учебного корпуса по адресу 214013, г. Смоленск, Энергетический пр-д, д.1, здание энергетического института (основной корпус).

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены филиалом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается **доступ к информационным и библиографическим ресурсам в сети Интернет** для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1. Костин В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей [Электронный ресурс]: учебное пособие / В. Н. Костин. – Москва: МИСИС, 2018. – 31 с. – Режим доступа: https://e.lanbook.com/book/116743.

2. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург: Лань, 2020. – 124 с. Режим доступа: https://e.lanbook.com/book/133924.

3. Основы информационной безопасности [Электронный ресурс]: учебник / В.Ю. Рогозин, И.Б. Галушкин, В. Новиков, С.Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=562348.

Дополнительная литература.

1. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов.– 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428820.

2. Голиков А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: учебное пособие – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=480637.

3. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс]: учебное пособие. – Москва: Издательский дом Высшей школы экономики, 2015. – 574 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=440285.

4. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=480636.

5. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс]: учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». – Ставрополь: СКФУ, 2017. – 86 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=467139.

6. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. – 3-е изд., стереотип. - Москва: Флинта, 2016 Режим доступа: Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245.

7. Лапонина О.Р. Межсетевые экраны [Электронный ресурс]: учебное пособие / О.Р. Лапонина. – 2-е изд., исправ. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 466 с.: Режим доступа: https://biblioclub.ru/index.php?page=book&id=429093.

Список авторских методических разработок.

1. Методические указания к лабораторным работам и практическим занятиям по дисциплине «Информационная безопасность цифровой экономики» размещены на кафедральных ресурсах.

3. Методические указания к курсовой работе по дисциплине «Информационная безопасность цифровой экономики» размещены на кафедральных ресурсах

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины.

1. Справочная правовая система Консультант плюс [электронный ресурс] – Режим доступа: http://www.consultant.ru/online/.

2. Интернет-портал SecurityLab.ru компании Positive Technologies [электронный ресурс] – Режим доступа: https://www.securitylab.ru.

3. Галатенко В. Стандарты информационной безопасности [Электронный ресурс]: курс лекций // INTUIT.RU: официальный сайт Национального Открытого Университета «ИНТУИТ». – Режим доступа: https://www.intuit.ru/studies/courses/30/30/info.

4. Вопросы кибербезопасности / официальный сайт научного, периодического, информационно-методического журнала с базовой специализацией в области информационной безопасности [электронный ресурс] – Режим доступа: http://cyberrus.com.

5. Архив изданий по информационной безопасности / журнал «Information Security» [электронный ресурс] – Режим доступа: http://www.itsec.ru/articles2/allpubliks.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера страниц				Всего страниц в документе	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					
1	2	3	4	5	6	7	8	9	10