САМАРСКИЙ ПОЛИТЕХ
Самарский университет

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Директор филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
_____ / Г.И. Заболотни
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.1.01.12 «Защита информации»

Код и направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Информатика и вычислительная техника в нефтехимическом производстве
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2024
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Кафедра-разработчик	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Объем дисциплины, ч. / з.е.	180 / 5
Форма контроля (промежуточная аттестация)	Экзамен

Самара 2024

Б1.В.1.01.12 «Защита информации»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **09.03.01 Информатика и вычислительная техника**, утвержденного приказом Министерства образования и науки РФ от № 929 от 19.09.2017 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат педагогических наук, доцент	Е.Н Горбачевская
(должность, степень, ученое звание)	(ФИО)
Заведующий кафедрой	
	(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	А.А Малафеев, кандидат экономических наук, доцент
	(ФИО, степень, ученое звание)
Руководитель образовательной программы	С.В. Краснов, доктор технических наук, профессор
	(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способен обслуживать сетевые устройства информационно-коммуникационной системы	ПК-1.1 Планирует архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	Владеть навыками защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем
			Знать методы защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем
			Уметь планировать архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем с учетом защиты информации
		ПК-1.6 Применяет инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы	Владеть навыками применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы
			Знать методы применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы
			Уметь применять инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно□коммуникационной системы
	ПК-2 Способен выполнять работы и управление работами по созданию(модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы на предприятиях нефтехимического производства	ПК-2.1 Анализирует современные методики, методы и инструменты проектирования ИС на предприятиях нефтехимического производства	Владеть навыками анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства
			Знать методы анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства
			Уметь анализировать современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства

		ПК-2.2 Анализирует современные методики управление ИС на предприятиях нефтехимического производства	Владеть навыками анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства
			Знать методы анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства
			Уметь анализировать современные методик защиты информации при управлении ИС на предприятиях нефтехимического производства

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ПК-1	WEB технологии; Базовые технологии и процессы; Базы данных; Интегрированные системы автоматизации для управления бизнес-процессами в нефтехимическом производстве; Информационные системы электронного документооборота нефтехимического производства; Информационные технологии и программирование; Корпоративные информационные сети нефтехимического производства; Корпоративные информационные системы нефтехимического производства; Организация и планирование автоматизированных производств; Проектирование вычислительных систем и комплексов в нефтехимическом производстве; Системное программное обеспечение	Анализ информационных проектов нефтехимического производства; Выполнение и защита выпускной квалификационной работы; Надежность систем; Производственная практика:технологическая (проектно-технологическая) практика	

ПК-2	WEB технологии; Базовые технологии и процессы; Базы данных; Интегрированные системы автоматизации для управления бизнес-процессами в нефтехимическом производстве; Интеллектуальные системы и технологии; Информационное обеспечение экономики предприятия нефтехимического производства; Информационные системы электронного документооборота нефтехимического производства; Информационные технологии и программирование; Корпоративные информационные сети нефтехимического производства; Корпоративные информационные системы нефтехимического производства; Моделирование; Организация и планирование автоматизированных производств; Пакеты прикладных программ; Проектирование вычислительных систем и комплексов в нефтехимическом производстве; Системное программное обеспечение; Системы искусственного интеллекта	Анализ информационных проектов нефтехимического производства; Выполнение и защита выпускной квалификационной работы; Надежность систем; Производственная практика:технологическая (проектно-технологическая) практика	

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	8 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	64	64
Лекции	32	32
Практические занятия	32	32
Самостоятельная работа (всего), в том числе:	80	80
подготовка к лекциям	10	10
подготовка к практическим занятиям	40	40
подготовка к экзамену	30	30
Контроль	36	36
Итого: час	180	180
Итого: з.е.	5	5

4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	32	0	0	25	57
2	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	0	0	32	55	87
	Контроль	0	0	0	0	36
	Итого	32	0	32	80	180

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
8 семестр				
1	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Основные понятия и определения предмета защиты информации	Основные понятия и определения предмета защиты информации	2
2	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Разграничение доступа к ресурсам	Разграничение доступа к ресурсам.	2
3	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Идентификация и аутентификация субъектов	Идентификация и аутентификация субъектов	2
4	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Методы и средства криптографической защиты	Методы и средства криптографической защиты	2

5	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Контроль целостности информации	Контроль целостности информации. Электронно-цифровая подпись.	2
6	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Контроль целостности информации.	Контроль целостности информации. Электронно-цифровая подпись.	2
7	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Хранение и распределение ключевой информации.	Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей.	2
8	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Хранение и распределение ключевой информации.	Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей.	2
9	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Защита программного обеспечения от несанкционированного использования	Защита программного обеспечения от несанкционированного использования.	2
10	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Защита программного обеспечения от несанкционированного использования	Защита программного обеспечения от несанкционированного использования.	2
11	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Защита от разрушающих программных воздействий	Защита от разрушающих программных воздействий.	2
12	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Защита от разрушающих программных воздействий	Защита от разрушающих программных воздействий.	2
13	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Защита информации в компьютерных сетях	Защита информации в компьютерных сетях.	2

14	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Инженерно-техническая защита информации	Инженерно-техническая защита информации.	2
15	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Инженерно-техническая защита информации	Инженерно-техническая защита информации.	2
16	Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	Правовое обеспечение информационной безопасности и противодействию терроризму	Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	2
			Итого за семестр:	**32**
			Итого:	**32**

4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

4.3 Содержание практических занятий

№ занятия	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
8 семестр				
1	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	Базовые механизмы безопасности коммутаторов	Базовые механизмы безопасности коммутаторов.	2
2	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	Базовые механизмы безопасности коммутаторов	Базовые механизмы безопасности коммутаторов.	2
3	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	Безопасность на основе сегментации трафика	Безопасность на основе сегментации трафика.	2
4	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	Безопасность на основе сегментации трафика	Безопасность на основе сегментации трафика.	2
5	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	Безопасность на основе протокола IEEE 802.1x	Безопасность на основе протокола IEEE 802.1x	2
6	Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	Безопасность на основе протокола IEEE 802.1x	Безопасность на основе протокола IEEE 802.1x	2

7	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Списки контроля доступа	Списки контроля доступа ACL.	2
8	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Списки контроля доступа	Списки контроля доступа ACL.	2
9	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Инструменты управления сетью	Утилита iptables	2
10	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Инструменты управления сетью	Утилита iptables	2
11	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	SSL-туннелирование	Туннелирование соединений с использованием протокола SSL.	2
12	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	SSL-туннелирование	Туннелирование соединений с использованием протокола SSL.	2
13	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Удалённое управление с шифрованием данных	Удаленное управление по защищенному протоколу SSH.	2
14	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Удалённое управление с шифрованием данных	Удаленное управление по защищенному протоколу SSH.	2
15	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Установление и управление соединениями между двумя сетевыми узлами Ethernet	PPPoE: особенности настройки, преимущества и отличия от других протоколов соединения.	2
16	Методы защиты сетевых устройств информационно‑коммуникационных систем в том числе и нефтехимических предприятий	Установление и управление соединениями между двумя сетевыми узлами Ethernet	PPPoE: особенности настройки, преимущества и отличия от других протоколов соединения.	2
			Итого за семестр:	**32**
			Итого:	**32**

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
8 семестр			

Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	подготовка к лекциям	Основные понятия и определения предмета защиты информации. Разграничение доступа к ресурсам. Идентификация и аутентификация субъектов. Методы и средства криптографической защиты. Контроль целостности информации. Электронно-цифровая подпись. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Защита программного обеспечения от несанкционированного использования. Защита от разрушающих программных воздействий. Защита информации в компьютерных сетях. Инженерно-техническая защита информации. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	10
Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства	подготовка к экзамену	Основные понятия и определения предмета защиты информации. Разграничение доступа к ресурсам. Идентификация и аутентификация субъектов. Методы и средства криптографической защиты. Контроль целостности информации. Электронно-цифровая подпись. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Защита программного обеспечения от несанкционированного использования. Защита от разрушающих программных воздействий. Защита информации в компьютерных сетях. Инженерно-техническая защита информации. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	15
Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	подготовка к практическим занятиям	Базовые механизмы безопасности коммутаторов. Безопасность на основе сегментации трафика. Безопасность на основе протокола IEEE 802.1x Списки контроля доступа ACL. Утилита iptables. Туннелирование соединений с использованием протокола SSL. Удаленное управление по защищенному протоколу SSH. Протокол PPPoE.	40
Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий	подготовка к экзамену	Базовые механизмы безопасности коммутаторов. Безопасность на основе сегментации трафика. Безопасность на основе протокола IEEE 802.1x Списки контроля доступа ACL. Утилита iptables. Туннелирование соединений с использованием протокола SSL. Удаленное управление по защищенному протоколу SSH. Протокол PPPoE.	15
		Итого за семестр:	**80**
		Итого:	**80**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	**Ресурс НТБ СамГТУ** (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Инженерно-техническая защита информации и технические средства охраны на критически важных объектах; Ай Пи Ар Медиа, 2022.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||122647	Электронный ресурс
2	Методы и средства комплексной защиты информации в технических системах; Российский федеральный ядерный центр – ВНИИЭФ, 2019.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||101925	Электронный ресурс
3	Основы информационной безопасности; Интернет-Университет **Информационных** Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||97562	Электронный ресурс
4	Технологии защиты информации в компьютерных сетях; Профобразование, **2021**.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||102207	Электронный ресурс
5	Учебно-методическое пособие по выполнению курсового проекта по дисциплине Методы и средства защиты информации; Московский технический университет связи и информатики, 2016.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||61496	Электронный ресурс
Дополнительная литература		
6	Защита компьютерной информации. Эффективные методы и средства; Профобразование, 2019.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||87992	Электронный ресурс
7	Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации; **Издательский Дом МИСиС**, 2018.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||98199	Электронный ресурс
8	Основы информационной безопасности и защита информации; Липецкий государственный технический университет, ЭБС АСВ, 2022.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||128718	Электронный ресурс
9	Программно-аппаратные средства защиты информации. В 3 частях. Ч.1; Тамбовский государственный **технический** университет, ЭБС АСВ, 2022.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||133346	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Microsoft Office 2013	Microsoft (Зарубежный)	Лицензионное
2	Microsoft Windows 8.1 Professional операционная система	Microsoft (Зарубежный)	Лицензионное
3	Ubuntu Linux	Canonical Ltd (Зарубежный)	Свободно распространяемое
4	Браузер Google Chrome	Google (Отечественный)	Свободно распространяемое
5	Справочная правовая система (СПС) КонсультантПлюс	АО «Консультант Плюс» (Отечественный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа
2	Электронная библиотека изданий СамГТУ	http://irbis.samgtu.local/cgi-bin/irbis64r_01/cgiirbis_64.exe	Российские базы данных ограниченного доступа
3	eLIBRARY.ru	http://www.eLIBRARY.ru/	Российские базы данных ограниченного доступа
4	КонсультантПлюс (правовые документы) - доступ с ПК в Медиацентре (ауд. 42)	http://www.consultant.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Аудитория № 302
Учебная аудитория для проведения занятий лекционного типа.
Помещение оснащено:
проектор, моноблок, экран;
имеется выход в сеть Интернет; с доступом в электронную информационно□образовательную среду СамГТУ;
учебная мебель: 22 стола, 44 стула; стол и стул для преподавателя, кафедра,
доска аудиторная.

Практические занятия

Аудитория № 102
Аудитория для практических и семинарских занятий, текущего контроля и промежуточной аттестации (для инвалидов и лиц ОВЗ)
Помещение оснащено:
компьютер в комплекте 8 шт: монитор;
Компьютер в комплекте 14 шт: монитор, сетевой фильтр;
имеется выход в сеть Интернет; и с доступом в электронную информационно образовательную среду СамГТУ;
учебная мебель: 23 компьютерных столов, 23 кресла-комфорт, 6 ученических парт, 12 ученических стульев, стол и стул преподавателя

Самостоятельная работа

Аудитория № 212
Учебная аудитория для проведения курсового проектирования групповых и индивидуальных консультаций и самостоятельной работы обучающихся
Помещение оснащено:
при необходимости используют ноутбук 4 шт.
имеется выход в сеть Интернет; с доступом в электронную информационно образовательную среду СамГТУ;
специализированная мебель: 4 ученических стола (2 пос. места), 8 ученических стульев, стол и стул для преподавателя.
Аудитория № 304
Учебная аудитория для самостоятельной работы обучающихся.
Помещение оснащено:
при необходимости используют ноутбук 4 шт,
имеется выход в сеть Интернет; с доступом в электронную информационно образовательную среду СамГТУ;
Учебная мебель: 8 столов, 16 стульев, стол и стул для преподавателя

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;

- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.1.01.12 «Защита информации»

Фонд оценочных средств
по дисциплине
Б1.В.1.01.12 «Защита информации»

Код и направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Информатика и вычислительная техника в нефтехимическом производстве
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2024
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Кафедра-разработчик	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Объем дисциплины, ч. / з.е.	180 / 5
Форма контроля (промежуточная аттестация)	Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способен обслуживать сетевые устройства информационно-коммуникационной системы	ПК-1.1 Планирует архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	Владеть навыками защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем
			Знать методы защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем
			Уметь планировать архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем с учетом защиты информации
		ПК-1.6 Применяет инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы	Владеть навыками применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы
			Знать методы применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы
			Уметь применять инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно□коммуникационной системы
	ПК-2 Способен выполнять работы и управление работами по созданию(модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы на предприятиях нефтехимического производства	ПК-2.1 Анализирует современные методики, методы и инструменты проектирования ИС на предприятиях нефтехимического производства	Владеть навыками анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства
			Знать методы анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства
			Уметь анализировать современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства

		ПК-2.2 Анализирует современные методики управление ИС на предприятиях нефтехимического производства	Владеть навыками анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства
			Знать методы анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства
			Уметь анализировать современные методик защиты информации при управлении ИС на предприятиях нефтехимического производства

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Современные методики защиты информации при управлении ИС на предприятиях нефтехимического производства				
ПК-1.1 Планирует архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	**Владеть** навыками защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	оценочные средства промежуточного контроля	Нет	Да
	Уметь планировать архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем с учетом защиты информации	оценочные средства промежуточного контроля	Нет	Да
	Знать методы защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	оценочные средства промежуточного контроля	Нет	Да
		практические задачи	Да	Нет
ПК-1.6 Применяет инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы	**Знать** методы применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	практические задачи	Да	Нет
	Владеть навыками применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	оценочные средства промежуточного контроля	Нет	Да
	Знать методы применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	оценочные средства промежуточного контроля	Нет	Да
	Уметь применять инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно□коммуникационной системы	оценочные средства промежуточного контроля	Нет	Да

ПК-2.1 Анализирует современные методики, методы и инструменты проектирования ИС на предприятиях нефтехимического производства	**Уметь** анализировать современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Знать методы анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Владеть навыками анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Знать методы анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
ПК-2.2 Анализирует современные методики управление ИС на предприятиях нефтехимического производства	**Знать** методы анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
	Владеть навыками анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Знать методы анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Уметь анализировать современные методик защиты информации при управлении ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
Методы защиты сетевых устройств информационно□коммуникационных систем в том числе и нефтехимических предприятий				
ПК-1.1 Планирует архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	**Знать** методы защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	оценочные средства промежуточного контроля	Нет	Да
	Уметь планировать архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем с учетом защиты информации	оценочные средства промежуточного контроля	Нет	Да
	Владеть навыками защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	оценочные средства промежуточного контроля	Нет	Да
	Знать методы защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	практические задачи	Да	Нет
	Уметь планировать архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем с учетом защиты информации	практические задачи	Да	Нет

	Владеть навыками защиты информации при планировании архитектуры и функционировании информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем	практические задачи	Да	Нет
ПК-1.6 Применяет инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы	**Уметь** применять инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	практические задачи	Да	Нет
	Знать методы применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	практические задачи	Да	Нет
	Владеть навыками применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	практические задачи	Да	Нет
	Уметь применять инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	оценочные средства промежуточного контроля	Нет	Да
	Знать методы применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	оценочные средства промежуточного контроля	Нет	Да
	Владеть навыками применения инструкций по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно коммуникационной системы	оценочные средства промежуточного контроля	Нет	Да
ПК-2.1 Анализирует современные методики, методы и инструменты проектирования ИС на предприятиях нефтехимического производства	**Владеть** навыками анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Знать методы анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Уметь анализировать современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Владеть навыками анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
	Уметь анализировать современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
	Знать методы анализа современные методик, методов и инструментов защиты информации при проектировании ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет

ПК-2.2 Анализирует современные методики управление ИС на предприятиях нефтехимического производства	**Знать** методы анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
	Уметь анализировать современные методик защиты информации при управлении ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
	Владеть навыками анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	практические задачи	Да	Нет
	Знать методы анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Уметь анализировать современные методик защиты информации при управлении ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да
	Владеть навыками анализа современных методик защиты информации при управлении ИС на предприятиях нефтехимического производства	оценочные средства промежуточного контроля	Нет	Да

Направление подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА (ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА В НЕФТЕХИМИЧЕСКОМ ПРОИЗВОДСТВЕ)

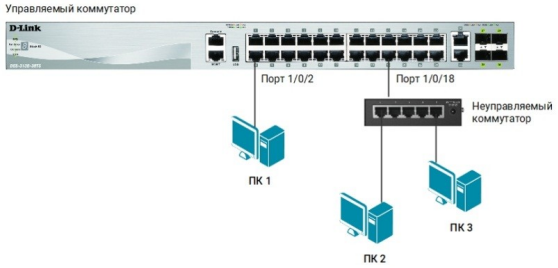
Дисциплина: «ЗАЩИТА ИНФОРМАЦИИ»

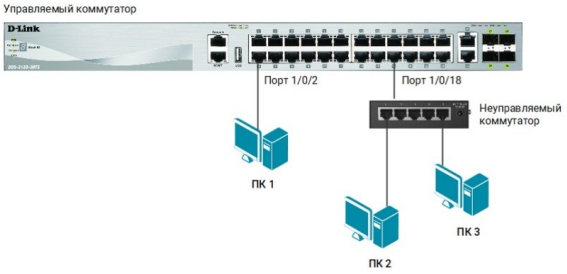
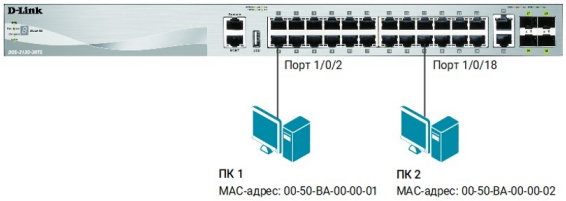
Перечень компетенций и индикаторов достижения компетенций, для оценки сформированности которых используется данный ФОС

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции, реализуемые дисциплиной**
ПК-1 Способен обслуживать сетевые устройства информационно-коммуникационной системы	ПК-1.1 Планирует архитектуру и функционирование информационных систем хранения, обработки и передачи информации на базе сетевых устройств информационно-коммуникационных систем
	ПК-1.6 Применяет инструкции по охране труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы

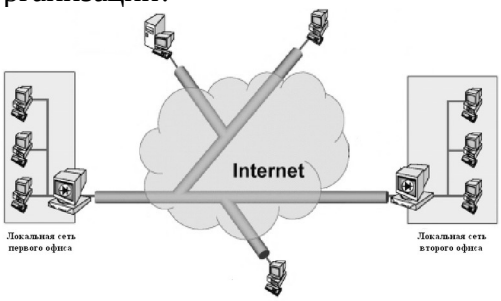
Номер задания	Содержание вопроса	Правильный ответ на задание
1.	Выберите правильный вариант ответа Одним из основных принципов обеспечения информационной безопасности в информационно-коммуникационных средах являются _____ который предполагает необходимость учета всех слабых и уязвимых мест АСОИ, возможных объектов и направлений атак, высокую квалификацию злоумышленника, текущих и возможных в будущем каналов реализации угроз. A) принцип разумной достаточности B) принцип непрерывности защиты C) принцип комплексности **D) принцип системности**	D
2.	Выберите правильный вариант ответа Одним из основных принципов обеспечения информационной безопасности в информационно-коммуникационных средах являются _____ который предполагает возможность варьировать уровень ее защищенности A) принцип системности B) принцип комплексности C) принцип непрерывности защиты **D) принцип гибкости управления и применения системы защиты**	D
3.	Выберите правильный вариант ответа.	C

Номер задания	Содержание вопроса	Правильный ответ на задание
	Анализ сетевого трафика в информационно-коммуникационных средах осуществляется путем его перехвата является внутрисегментной атакой и направлен на перехват и анализ информации, предназначенной для любого ПК, расположенного в том же сегменте сети, что и злоумышленник и называется A) DoS атаками (DoS – Denied of Service) B) Маскарад (spoofing) **C) Сниффинг (sniffing)** D) Фишинг (fishing)	
4.	Выберите правильный вариант ответа. При организации безопасности доступа в информационно-коммуникационных средах межсетевые экраны осуществляют фильтрацию входящих в сеть и исходящих из сети пакетов на основе информации, содержащихся в их TCP и IP заголовках, называются **A) фильтрующие маршрутизаторы** B) шлюзы сетевого уровня C) шлюзы прикладного уровня D) маршрутизаторы защиты	A
5.	Выберите правильный вариант ответа. Поставленная задача: Настроить функцию Port Security коммутатора серии DES-3810 на режим запоминания MAC-адресов; по умолчанию все порты находятся в режиме continuous. Выберите параметр настройки **A) learn-mode** B) mac-address C) action D) address-limit F) clear-intrusion-flag	A
6.	Выберите правильный вариант ответа. Поставленная задача: Настроить функцию Port Security коммутатора серии DES-3810 на статическое задание разрешенных MAC-адресов для режимов static и configured A) learn-mode **B) mac-address** C) action D) address-limit F) clear-intrusion-flag	B
7.	Выберите правильный вариант ответа. Поставленная задача: Настроить функцию Port Security коммутатора серии DES-3810 на максимальное количество MAC-	D

Номер задания	Содержание вопроса	Правильный ответ на задание
	адресов, которое будет разрешено на порту A) learn-mode B) mac-address C) action **D) address-limit** F) clear-intrusion-flag	
8.	Выберите правильный вариант ответа. Поставленная задача: Дана схема сети (рисунок). Опишите действия внесенных настроек  Switch# configure terminal Switch(config)#interface range ethernet 1/0/1-24 Switch(config-if-range)#switchport port-security Switch(config-if-range)#switchport port-security maximum 1 **A) включена на портах 1/0/1-24 функция Port Security и установлено максимальное количество изучаемых каждым портом MAC-адресов равное 1** B) установлен режим работы фунции Delete on Timeout C) указано действие при превышении максимального числа MAC-адресов — ограничение (Restrict) D) настроено время жизни для динамически изученных MAC-адресов равное 3 минутам	A
9.	Выберите правильный вариант ответа. Поставленная задача: Дана схема сети (рисунок). Опишите действия внесенных настроек	D

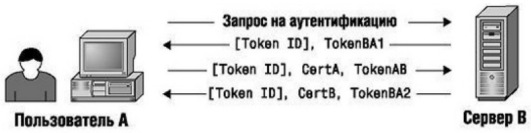
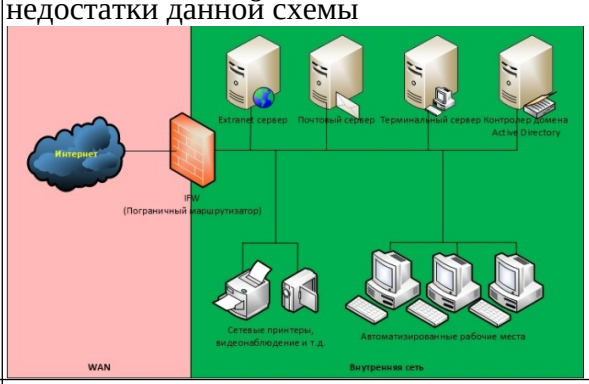
Номер задания	Содержание вопроса	Правильный ответ на задание
	 Switch(config-if-range)# switchport port-security aging time 3 A) включена на портах 1/0/1-24 функция Port Security и установлено максимальное количество изучаемых каждым портом MAC-адресов равное 1 B) установлен режим работы фунции Delete on Timeout C) указано действие при превышении максимального числа MAC-адресов — ограничение (Restrict) **D) настроено время жизни для динамически изученных MAC-адресов равное 3 минутам**	
10.	Выберите правильный вариант ответа. Поставленная задача: Дана схема сети (рисунок). Опишите действия внесенных настроек  Switch(config)#mac-address-table static 0050.BA00.0001 vlan 1 interface ethernet 1/0/2 Switch(config)#mac-address-table static 0050.BA00.0002 vlan 1 interface ethernet 1/0/18 A) включена на портах 1/0/1-24 функция Port Security и установлено максимальное количество изучаемых каждым портом MAC-адресов равное 1 **B) созданы статические записи для**	B

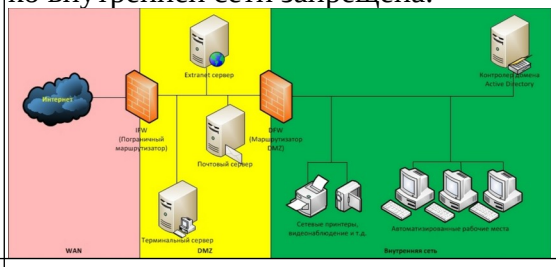
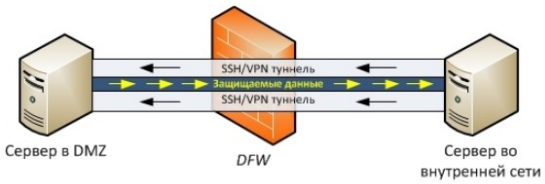
Номер задания	Содержание вопроса	Правильный ответ на задание
	MAC-адресов рабочих станций, подключённых к портам 1/0/2 и 1/0/18 C) указано действие при превышении максимального числа MAC-адресов — ограничение (Restrict) D) настроено время жизни для динамически изученных MAC-адресов равное 3 минутам	
11.	Выберите правильный вариант ответа. На рисунке показана схема _____.  **A) DDoS атаками (Distributed Denial of Service)** B) Маскарад (spoofing) C) Сниффинг (sniffing) D) Фишинг (fishing)	A
12.	Выберите правильный вариант ответа. Высшую степень защиты обеспечивает метод шифрования информации _____. A) хеширование **B) гаммирование** C) закрытых ключей D) профилей пользователей	B
13.	Выберите правильный вариант ответа. Active Directory использует протокол **A) LDAP (Lightweight Directory Access Protocol)** B) ICMP (Internet Control Message Protocol) C) SNMP (Simple Network Management Protocol) D) RAMUS	A
14.	Выберите правильный вариант ответа. Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием. A) UDP (User Datagram Protocol) B) SNMP (Simple Network Management Protocol) C) RSVP (Resource ReSerVation Protocol) **D) RADIUS (Remote Authentication in Dial-In User Service)**	D

Номер задания	Содержание вопроса	Правильный ответ на задание
15.	Выберите правильный вариант ответа. Криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. **A) Схема Эль-Гамаля** B) Протокол MTI/A(C) Протокол Диффи—Хеллмана D) Протокол Station-to-Station	A
16.	На рисунке представлена схема сети с обеспечением безопасной передачи данных. На основе какой технологии организованная безопасность в информационно-коммуникационной среде организации? 	Безопасность в информационно-коммуникационной среде данной организации организованна на основе виртуальной частной сети.
17.	Укажите технологию организации безопасного доступа в информационно-коммуникационных системах при информационном скрытии речевой.	При организации безопасности доступа в информационно-коммуникационных системах информационное скрытие речевой информации обеспечивается техническим закрытием аналоговым скремблированием и шифрованием сигналов речевой информации, передаваемых по кабелям и радиоканалам.

18.	Опишите действие команды коммутатора серии DES-3810 функцию Port Security
	`switch(config)# port-security 10 clear-intrusion-flag`
	`switch(config)# interface 10 enable`
		Включение порта 10 после того, как он был выключен Port Security, то есть после его блокировки

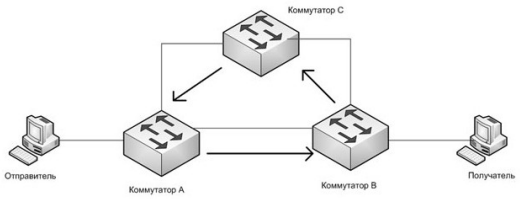
19.	Опишите действие команды коммутатора серии DES-3810 функцию Port Security `switch(config)# aaa port-access authenticator 10 control auto`	Настроена функия Port Security с аутентификацией 802.1X на порт 10. Режим контроля auto
20.	На рисунке показана схема аутентификации методом_сертификатов. Приведите примеры протоколов которые	Аутентификацию при помощи сертификатов обеспечивают несколько распространенных протоколов, в

Номер задания	Содержание вопроса	Правильный ответ на задание
	при этом используются.  	частности, наиболее известный и широко распространенный протокол SSL, который применяется практически в каждом web-браузере. Помимо него применяются протоколы TLS, IKE, S/MIME, PGP и Open PGP.
21.	Опишите для чего используется Протокол Диффи — Хеллмана (Diffie–Hellman key exchange protocol, DH).	Протокол Диффи — Хеллмана — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.
22.	Перечислите источники угроз в Ethernet.	Источник угроз делят на 2 типа: 1) источники угроз в самой системе; 2) источники угроз вне системы.
23.	На рисунке представлена схема плоской сети. Доступ узлов в Интернет осуществляется через NAT, а доступ к сервисам из Интернет через Port forwarding. Опишите достоинства т недостатки данной схемы  	Плюсы варианта предложенной схемы плоской сети: 1) Минимальные требования к функционалу IFW (можно сделать практически на любом, даже домашнем роутере). 2) Минимальные требования к знаниям специалиста, осуществляющего реализацию варианта. 3) Минусы варианта: 4) Минимальный уровень безопасности.
24.	На рисунке представлена схема сети с DMZ. Для увеличения информационной безопасности, данные доступные из Интернет, помещают в специально выделенный сегмент – демилитаризованную зону (DMZ). DMZ организуется с помощью межсетевых экранов, отделяющих ее от Интернет (IFW) и от внутренней сети (DFW). При этом правила фильтрации межсетевых экранов выглядят следующим образом: 1.Из внутренней сети можно инициировать соединения в DMZ и в WAN (Wide Area Network).	Плюсы варианта предложенной схемы сети с DMZ: 1.Повышенная защищённость сети от взломов отдельных сервисов. Даже если один из серверов будет взломан, Нарушитель не сможет получить доступ к ресурсам, находящимся во внутренней сети (например, сетевым принтерам, системам видеонаблюдения и т.д.). Минусы варианта: 1.Сам по себе вынос серверов в DMZ не повышает их защищенность. Необходим дополнительный МЭ для

Номер задания	Содержание вопроса	Правильный ответ на задание
	2.Из DMZ можно инициировать соединения в WAN. 3.Из WAN можно инициировать соединения в DMZ. 4.Инициация соединений из WAN и DMZ ко внутренней сети запрещена. 	отделения DMZ от внутренней сети.
25.	На рисунке представлена схема сети с DMZ. Общая схема работы данного варианта выглядит следующим образом: 1.На сервер в DMZ инсталлируется SSH/VPN сервер, а на сервер во внутренней сети инсталлируется SSH/VPN клиент. 2.Сервер внутренней сети инициирует построение сетевого туннеля до сервера в DMZ. Туннель строится с взаимной аутентификацией клиента и сервера. 3.Сервер из DMZ в рамках построенного туннеля инициирует соединение до сервера во внутренней сети, по которому передаются защищаемые данные. 4.На сервере внутренней сети настраивается локальный межсетевой экран, фильтрующий трафик, проходящий по туннелю. Перечислите положительные свойства использования OpenVPN, 	Важные положительные свойства использования OpenVPN в данной схеме сети: 1. Кроссплатформенность. 2. Возможность построения туннелей с взаимной аутентификацией клиента и сервера. 3. Возможность использования сертифицированной криптографии.
26.	Дайте описание понятию Гамма шифра.	Гамма шифра – псевдослучайная последовательность, вырабатываемая по определенному алгоритму, используемая для зашифровки открытых данных и дешифровки шифротекста. Используется при шифровании методом гаммирования.
27.	Опишите понятие криптоаналитическая атака компьютерной сети.	Любая попытка со стороны злоумышленника расшифровать

Номер задания	Содержание вопроса	Правильный ответ на задание
		шифротекст C и получить открытый текст M не имея подлинного ключа, называется криптоаналитической атакой.
28.	Перечислите основные принципы используемые при построении стойких шифров.	При построении стойких шифров необходимо использовать два основных принципа – рассеивание и перемешивание.
29.	Механизмы безопасной удаленной аутентификации пользователей.	Для обеспечения подлинности канала связи, и защиты от атак повторами обычно используют метод запрос-ответ, либо механизм отметки времени.
30.	Приведите не менее трех протоколов удаленной аутентификации пользователей.	Три примера можно выбрать из данного списка протоколов удаленной аутентификации пользователей: - CHAP - EAP - IPSec - SSH - TLS v 1.2
31.	Приведите не менее трех изменений при динамической сегментации сети	Три примера можно выбрать из данного списка изменений при динамической сегментации сети: - правила контроля доступа; - состав групп пользователей; - местонахождение групп пользователей и т.д.
32.	Перечислите условия для проведения сегментации сети с использованием стандарта 802.1Q	Для проведения сегментации с использованием стандарта 802.1Q необходимо: - Четкая адресация сети, маски, network address, broadcast address. - Принцип логического разделения сети: по отделам, этажам, типу трафика и т.д. В одном сегменте рекомендуется держать не более 126 устройств. - Коммутаторы, поддерживающие 802.1Q. Маршрутизатор с поддержкой 802.1Q.
33.	Поставлена задача: Организовать определение принадлежность пользователя к нужной группе при его подключении к сети. Опишите кратко ваши предложения по решению данной задачи.	Данная задача обычно решается с помощью аутентификации и авторизации с использованием протокола 802.1x на RADIUS-сервере (часто с использованием данных из корпоративной службы каталогов, например Active Directory). Возможно применение и других методов — статического помещения

Номер задания	Содержание вопроса	Правильный ответ на задание
		пользователей в зависимости от порта подключения, VLAN’а, IP-подсети, авторизации по MAC-адресу и так далее в зависимости от возможностей используемого сервера AAA и оборудования.
34.	Поставлена задача: Изолировать трафик пользователя группы1 от трафика пользователей других групп при передаче по сети.	Данная задача традиционно решается путем создания отдельных виртуальных топологий для каждой группы пользователей. Как правило, это делается с помощью тех или иных средств виртуализации сети. В случае небольших сетей этими средствами обычно являются VLAN’ы и транки 802.1Q. Для больших сетей характерно применение MPLS VPN.
35.	Поставлена задача: Обеспечить доступ пользователя к тем ресурсам, к которым он должен иметь доступ и, заблокировать доступ ко всем остальным ресурсам	Данная задача как правило, решается пакетной фильтрацией на основе IP-адресов. Контроль доступа может быть реализован как такими «грубыми» средствами, как списки контроля доступа (ACL) на элементах сетевой инфраструктуры, так и «тонкой» фильтрацией на системах защиты нового поколения (NGFW, NGIPS),
36.	Перечислите виды ACL	Списки доступа бывают: Стандартные Расширенные Динамические Рефлексивные Повременные
37.	Перечислите два основных способа позволяющих устанавливать членство в VLAN.	Существуют два основных способа, позволяющих устанавливать членство в VLAN: 1) статические VLAN; 2) динамические VLAN.
38.	Возможно ли использование VLANов как метода защиты от широковещательного шторма?	Одним из методов защиты от широковещательного шторма является разделение сети на VLANы или на различные сети канального уровня, что локализует шторм в пределах одного VLAN/одной подсети.
39.	На рисунке представлена схема сети. Опишите какие необходимы настройки для исключения широковещательного шторма в петле.	Необходимо настроить протокол STP стандарте IEEE 802.1D или протоколы семейства STP (RSTP, MST).

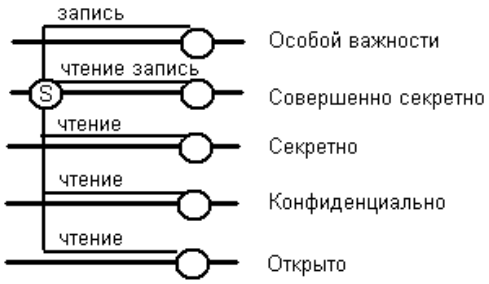
Номер задания	Содержание вопроса	Правильный ответ на задание
		
40.	Для чего в сетях используют Алгоритм связующего дерева (Spanning-Tree Algoritm) (sta)	Алгоритм STA предусматривает свободное от петель подмножество топологии сети путем размещения таких мостов, которые, если они включены, то образуют петли в резервном (блокирующем) состоянии. Порты блокирующего моста могут быть активированы в случае отказа основного канала, обеспечивая новый тракт через объединенную сеть.
41.	Перечислите возможные решения обеспечения безопасности корпоративной сети на основе D-Link.	D-Link предлагает комплексный подход к решению вопросов обеспечения безопасности, который включает в себя следующие решения: 1) Защита конечного пользователя — обеспечивает защиту внутренней сети от внутренних атак; 2) Защита средствами межсетевых экранов — обеспечивает защиту внутренней сети от внешних атак; 3) Объединенная безопасность — связующее звено между двумя предыдущими предложениями, объединяющее использование межсетевых экранов и коммутаторов для защиты сети.
42.	Какой функцией в коммутаторах D-Link реализован контролировать доступа компьютеров в сеть на основе их IP- и MAC-адресов.	Функция IP-MAC-Port Binding (IMPB), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения.
43.	При активизации функции IMPB на порте администратор должен указать режим его работы. Как работает порт в режиме Strict Mode?	Strict Mode — в этом режиме порт по умолчанию заблокирован.
44.	При активизации функции IMPB на порте администратор должен указать режим его работы. Как работает порт в режиме Loose Mode?	Loose Mode — в этом режиме порт по умолчанию открыт.
45.	При активизации функции IMPB включен режим работы DHCP Snooping mode. Действия коммутатора в данном режиме?	Режим DHCP Snooping используется коммутатором для динамического создания записей IP-MAC на основе анализа DHCP-пакетов и привязки их к

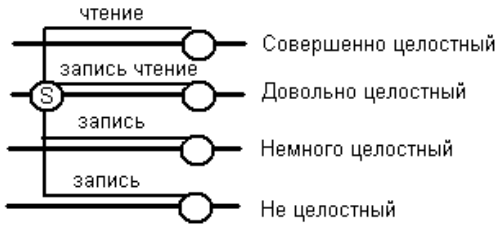
Номер задания	Содержание вопроса	Правильный ответ на задание
		портам с включенной функцией IMPB (администратору не требуется создавать записи вручную).
46.	Одним из методов организации механизма ограничения административного доступа к управлению коммутатором является настройка коммутатора на работу с протоколом SSH. Опишите данный протокол.	SSH (Secure SHell, "безопасная оболочка") — сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.
47.	Для чего используют физический стек коммутаторов 3-го уровня D-Link.	Под физическим стекированием понимается объединение нескольких коммутаторов в одно логическое устройство с целью увеличения количества портов, удобства управления и мониторинга. Объединенные в стек коммутаторы имеют общие таблицы коммутации и маршрутизации (для коммутаторов 3 уровня).
48.	В корпоративной сети при настройке коммутатора D-Link использовалась команда ip access-list std1 10. Для чего использовалась данная команда?	Команда ip access-list используется для создания именованных списков доступа, в данном случае создание списка с именем std1 и номером 10.
49.	В корпоративной сети при настройке коммутатора D-Link использовалась команда mac access-list extended mac1 6010. Для чего использовалась данная команда?	В данном случае создан расширенный список доступа MAC с именем mac1 и номером 6010.
50.	Дайте описание понятия IPsec в рамках защиты информации в информационной системе.	IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

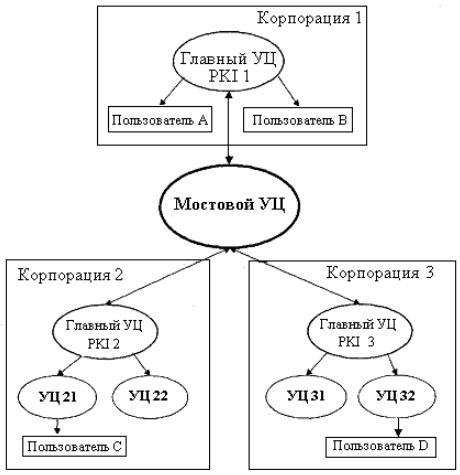
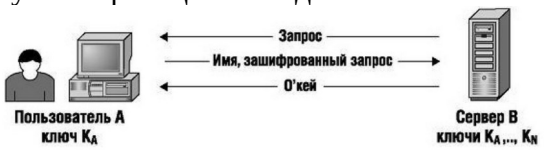
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции, реализуемые дисциплиной**
ПК-2 Способен выполнять работы и управление работами по созданию(модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы в нефтехимическом производстве	ПК-2.1 Анализирует современные методики, методы и инструменты проектирования ИС на предприятиях нефтехимического производства
	ПК-2.2 Анализирует современные методики управление ИС на предприятиях нефтехимического производства

Номер задания	Содержание вопроса	Правильный ответ на задание
1.	Выберите правильный вариант ответа. В вашей организации используются	А

Номер задания	Содержание вопроса	Правильный ответ на задание
	операционные системы Windows. Какая политика безопасности применима на данном предприятии? **A) ролевая политика безопасности** B) дискреционная политика безопасности C) Политика избирательного разграничения доступа D) мандатная модель управления доступом	
2.	Выберите правильный вариант ответа. В информационно-коммуникационных средах операционной системой основанной на дискреционной политике безопасности, операционной системой является A) OS/2 **B) Linux** C) Windows D) SkyOS	B
3.	Выберите правильный вариант ответа. При организации безопасности доступа в информационно-коммуникационных средах протокол Диффи-Хеллмана используется при подходе к распределению ключевой информации в компьютерной сети. Этот подход называется A) Распределение ключевой информацией с использованием одного либо нескольких центров распределения ключей **B) Прямой обмен сеансовыми ключами между пользователями** C) Взаимное подтверждение подлинности участников сеанса D) подтверждение достоверности сеанса для защиты от атак методом повторов	B
4.	Выберите правильный вариант ответа. В модульной архитектуре системы защиты ПО от несанкционированного использования функции определения факта легальности запуска защищаемой программы, сравнивая текущие значения параметров среды с эталонными выполняет A) Блок установки характеристик среды B) Подсистема реализации защитных функций **C) Блок сравнения характеристик среды** D) Подсистема противодействия нейтрализации защитных механизмов	C
5.	Выберите правильный вариант ответа. При организации безопасности доступа в	B

Номер задания	Содержание вопроса	Правильный ответ на задание
	информационных системах основными элементами поддержания изолированной программной среды являются A) поиском критических участков кода методом семантического анализа **B) контроль целостности и активности процессов** C) определение точки входа в ПЗУ D) защитой данных	
6.	Выберите правильный вариант ответа. Нарушение конфиденциальности информационного обмена в ИС, осуществляемого по каналам связи абонентов систем и сетей организаций, с помощью их «прослушивания»; данный вид угроз для компьютерных сетей получил название A) Маскарад (spoofing) B) DoS атаками (DoS – Denied of Service) **C) Сниффинг (sniffing)** D) Фишинг (fishing)	C
7.	Выберите правильный вариант ответа. На рисунке показана схема демонстрации правила NWD (нет записи вниз). Какая политика безопасности поддерживает данное правило?  **A) политика безопасности Белла-ЛаПадулы** B) ролевая политика безопасности C) политика безопасности контроля целостности информационных ресурсов D) мандатная модель целостности Биба	A
8.	Выберите правильный вариант ответа. На рисунке показана схема демонстрации правила NWD (нет записи вверх). Какая политика безопасности поддерживает данное правило?	D

Номер задания	Содержание вопроса	Правильный ответ на задание
	 A) политика безопасности Белла-ЛаПадулы B) ролевая политика безопасности C) политика безопасности контроля целостности информационных ресурсов **D) мандатная модель целостности Биба**	
9.	Выберите правильный вариант ответа. Под _____ понимают подтверждение пользователем предъявленного идентификатора, проверка его подлинности и принадлежности именно данному пользователю. A) идентификация **B) аутентификацией** C) авторизация D) шифрование	B
10.	Выберите правильный вариант ответа. _____ — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий A) идентификация B) аутентификацией **C) авторизация** D) шифрование	C
11.	Выберите правильный вариант ответа. Поставлена задача: Определить минимальную длину паролей L при мощности парольной системы A, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T. Исходные данные – P=10-6, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю, A=26 (символы английского алфавита). A) L=4 **B) L=8** C) L=6	B
12.	Выберите правильный вариант ответа.	C

Номер задания	Содержание вопроса	Правильный ответ на задание
	Поставлена задача: Определить минимальную длину паролей L при мощности парольной системы A, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T. Исходные данные – P=10-6, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю, A=36 (малые латинские буквы и цифры). A) L=4 B) L=8 **C) L=6**	
13.	Выберите правильный вариант ответа. На рисунке показана схема архитектуры  **A) Гибридная архитектура PKI (инфраструктура открытых ключей)** B) Централизованная архитектура PKI (инфраструктура открытых ключей) C) Блочная архитектура PKI (инфраструктура открытых ключей) D) Сертифицированная архитектура PKI (инфраструктура открытых ключей)	A
14.	Выберите правильный вариант ответа. На рисунке показана схема аутентификации методом  **A) «запрос-ответ»** B) неявного запроса C) Kerberos D) с использованием идентификационной	A

Номер задания	Содержание вопроса	Правильный ответ на задание
	таблицы	
15.	Выберите правильный вариант ответа. На рисунке показана схема аутентификации методом  **A) «запрос-ответ»** B) неявного запроса C) Kerberos D) с использованием идентификационной таблицы	-
16.	Дайте краткое описание понятию Формальные модели политик безопасности	Формальные модели политик безопасности позволяют описать поведение подсистемы безопасности в рамках строгих математических моделей, правил.
17.	Дайте краткое описание понятию Неформальные модели политик безопасности	Неформальные модели политик безопасности предполагают описание поведения подсистемы безопасности в рамках вербальных (словесных) утверждений, не обладающих математической строгостью.
18.	Перечислите основные множества ролевой политики безопасности в рамках которых осуществляется формализация.	Формализация ролевой модели осуществляется в рамках следующих множеств: 1) множество пользователей компьютерной системы. 2) множество ролей. 3) множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа. 4) множество сеансов работы пользователей с компьютерной системой.
19.	Опишите состав учетной записи пользователя	Совокупность идентификатора и пароля пользователя - основные составляющие его учетной записи.
20.	Что содержит База данных пользователей парольной системы?	База данных пользователей парольной системы содержит учетные записи всех пользователей корпоративной информационной системы.
21.	Приведите не менее трех широко распространенных технических устройств, используемых для решения задач	Три примера можно выбрать из данного списка трех широко распространенных технических

Номер задания	Содержание вопроса	Правильный ответ на задание
	идентификации/аутентификации пользователей	устройств, используемых для решения задач идентификации/аутентификации пользователей: - идентификаторы iButton (Touch Memory); - бесконтактные радиочастотные карты proximity; - пластиковые карты; - ключи e-Token.
22.	Перечислите процессы электронной цифровой подписи в соответствии с ГОСТ 34.10-2018.	Механизм цифровой подписи определяется посредством реализации двух основных процессов 1) формирование подписи; 2) проверка подписи.
23.	Назначение электронной цифровой подписи в соответствии с ГОСТ 34.10-2018.	Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение.
24.	Перечислите свойства сообщения при использовании электронной цифровой подписи в соответствии с ГОСТ 34.10-2018.	Использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения: 1) осуществление контроля целостности передаваемого подписанного сообщения; 2) доказательное подтверждение авторства лица, подписавшего сообщение; 3) защита сообщения от возможной подделки.
25.	Дать описание понятию Дайджест Данных (Data Digest).	Дайджест Данных - Относительно небольшой блок данных, вычисленный с применением к оригинальному блоку данных (обычно большего размера) специальных дайджест-функций (хэш-функций).
26.	Задача: Предприятию необходимо получить квалифицированный электронный сертификат на организацию ЭЦП для защиты данных ИС. В какую организацию необходимо обратиться?	Аккредитованный удостоверяющий центр (УЦ) — это организация, получившая доступ к Единому реестру, имеющая право на сбор и хранение ключевой информации. Она имеет право на создание квалифицированного электронного сертификата и распространение лицензий на криптографию.
27.	Перечислите свойства информации с точки зрения Защиты информации	Свойства информации, которые могут приводить к потере ценности информации: 1) конфиденциальность;

Номер задания	Содержание вопроса	Правильный ответ на задание
		2) целостность; 3) доступность.
28.	Перечислите стадии жизненного цикла вируса.	Жизненный цикл вирусов включает в себя две основные стадии – хранение (латентная фаза) и исполнение.
29.	Технические средства борьбы с компьютерными вирусами.	Технические средства борьбы с компьютерными вирусами – применение антивирусных мониторов и сканеров, программных и аппаратных средств, недопускающих возможность заражения объектов компьютерной системы.
30.	Перечислите виды источников угроз безопасности персональных данных.	Источники угроз безопасности персональных данных: 1. Антропогенные 2. Стихийные 3. Техногенные
31.	Дайте описание атакам MITM (Man-in-the-Middle).	Атака MITM происходит, когда хакеры внедряются в двустороннее информационное взаимодействие. После перехвата трафика они могут фильтровать и красть данные.
32.	Дайте описание атакам Фишинг	Вымогатели используют поддельные сообщения, например, e-mail, чтобы обманным путем заставить получателя открыть его и выполнить определенное действие.
33.	Приведите не менее трех биометрических характеристик, используемых для идентификации и аутентификации ИС.	Три примера можно выбрать из данного списка биометрических характеристик, используемых для идентификации и аутентификации ИС: - отпечатки пальцев; - геометрическая форма рук; - узор радужной оболочки и сетчатки глаз; - форма и размеры лица; - особенности голоса; - биомеханические характеристики почерка; - биомеханические характеристики «клавиатурного почерка».
34.	Перечислите особенности использования биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем И/АУ.	Особенностью применения биометрических систем следующие: 1.Необходимость длительного обучения биометрической системы. 2.Возможность ошибочных отказов и ошибочных подтверждений при аутентификации пользователей.

Номер задания	Содержание вопроса	Правильный ответ на задание
		3.Необходимость использования специальных технических устройств.
35.	Поставлена задача: Приобретение российской программы управления ключами для организации. Приведите примеры российских программ управления ключами.	Российские программы управления ключами: ViPNet PKI Client Guardant Sign семейство Крипто и т.д.
36.	Является ли обязательным предоставление физическими лицами своих биометрических персональных данных в соответствии с Федеральным законом от 29 декабря 2022 г. N 572-ФЗ	Предоставление физическими лицами своих биометрических персональных данных в целях, предусмотренных настоящим Федеральным законом, не может быть обязательным.
37.	Дайте описание понятию биометрический процесс в соответствии ГОСТ Р 54411-2018/ISO/IEC TR 24722:2015.	Биометрический процесс - автоматический процесс, использующий одну или более биометрических характеристик одного индивида для биометрической регистрации, верификации или идентификации.
38.	Дайте описание понятию Непрерывный биометрический параметр процесс в соответствии ГОСТ Р 52633.4-2011.	Непрерывным считается биометрический параметр, значения которого составляют континуальное множество и ограничены только точностью представления.
39.	Перечислите меры защиты программных продуктов используемые для противодействия попыткам несанкционированного использования программного обеспечения.	Для противодействия попыткам несанкционированного использования программного обеспечения используются следующие меры защиты программных продуктов: 1.Организационно-экономические меры 2.Правовые меры 3.Технические меры
40.	Перечислите типы систем защиты программного обеспечения по способу ассоциации (внедрения) защитного механизма.	Системы защиты ПО от несанкционированного использования по способу ассоциации (внедрения) защитного механизма можно подразделить на два типа: 1) встроенные системы (внедряются при создании ПО); 2) пристыковочные системы (подключаются к уже готовому ПО).
41.	Опишите основную функцию службы Active Directory (службы активного каталога).	Службы Active Directory (службы активного каталога) представляют собой распределённую базу данных, которая содержит все объекты

Номер задания	Содержание вопроса	Правильный ответ на задание
		домена. Доменная среда Active Directory является единой точкой аутентификации и авторизации пользователей и приложений в масштабах предприятия.
42.	Дайте описание понятию контроллер домена в рамках Active Directory (службы активного каталога).	База данных Active Directory хранится на выделенных серверах – контроллерах домена
43.	Дайте описание понятию Группы безопасности в рамках Active Directory (службы активного каталога).	Группы безопасности — это способ сбора учетных записей пользователей, учетных записей компьютеров и других групп в управляемые единицы.
44.	Перечислите области действия групп Active Directory	Active Directory определяет следующие три области группы: 1.Универсальное. 2.Глобальный. 3.Локальный домен.
45.	Перечислите компоненты Active Directory	Active Directory включает в себя следующие компоненты: Объекты. Домены. Организационные единицы. Деревья. Леса.
46.	Задача: На нефтехимическом предприятии в медпункте предприятия с помощью медицинских информационных систем сотрудники медпункта обрабатывают персональные медицинские данные в МИС. Определите какой уровень защищенности необходимо организовать для выполнения ФЗ N 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».	В зависимости от количества обрабатываемых субъектов персональных данных и типа актуальных угроз безопасности в МИС требуется обеспечить второй или третий уровень защищенности персональных данных.
47.	Задача: На нефтехимическом дочернем предприятии ведется обработка бухгалтерских данных и затем по защищенному каналу передается в головное отделения предприятия. Работников дочернего предприятия более 100 000 субъектов. Определите какой уровень защищенности необходимо организовать для выполнения ФЗ N 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных	В данном случае требуется обеспечить третий уровень защищенности персональных данных и выше.

Номер задания	Содержание вопроса	Правильный ответ на задание
	данных».	
48.	На складе предприятия по беспроводной сети передают информацию о принятых и отправленных грузах. Опишите методы защиты передаваемых данных по беспроводной сети.	В описываемой ситуации достаточно стандартных вариантов шифрования данных при передаче по беспроводной сети (протоколы WPA 3, CKIP, TKIP, AES-CCMP и т.д.).
49.	Поставлена задача: необходимо пошагово проанализировать работу ОС. На какие программные средства вы будите использовать?	Отладчики – программные средства, позволяющие выполнять программу в пошаговом режиме, контролировать ее выполнение, вносить изменения в ход выполнения.
50.	Поставлена задача: необходимо проанализировать работу реестра ОС Windows. На какие программные средства вы будите использовать?	Мониторы операций с реестром – предоставляет возможность собрать информацию об обращениях к реестру Windows.

Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процессы формирования компетенций

Характеристика процедуры текущего контроля успеваемости и промежуточной аттестации по дисциплине

Оценивание знаний, умений, навыков и опыта деятельности проводятся на основе сведений, приводимых в матрице соответствия оценочных средств запланированным результатам обучения.

Цель текущего контроля успеваемости и промежуточной аттестации по учебным дисциплинам в семестре – проверка приобретаемых обучающимися знаний, умений, навыков в контексте формирования установленных образовательной программой компетенций в течение семестра.

Шкала оценивания:

«Отлично» – выставляется, если сформированность заявленных образовательных результатов компетенций оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно»: студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций;

«Хорошо» – выставляется, если сформированность заявленных образовательных результатов компетенций оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки

«неудовлетворительно», допускается оценка «удовлетворительно»: обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций;

«Удовлетворительно» – выставляется, если сформированность заявленных образовательных результатов компетенций оценивается критериями «удовлетворительно», «хорошо» и «отлично»: обучающийся показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой;

«Неудовлетворительно» – выставляется, если при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

Ответы и решения, обучающихся оцениваются по следующим общим критериям: распознавание проблем; определение значимой информации; анализ проблем; аргументированность; использование стратегий; творческий подход; выводы; общая грамотность.

Обучающиеся обязаны сдавать все задания в сроки, установленные преподавателем. Оценка

«Удовлетворительно» по дисциплине, может выставляться и при неполной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

Текущий контроль осуществляется через систему оценки преподавателем всех видов работ обучающихся, предусмотренных рабочей программой дисциплины и учебным планом.

Критерии оценки теста.

Количество верных ответов:

80-100% -оценка «отлично»: обучаюшийся демонстрирует глубокое знание учебно-программного материала, умение свободно выполнять задания, усвоивший взаимосвязь основных понятий дисциплины; способный самостоятельно приобретать новые знания и умения; способный самостоятельно использовать углубленные знания;

71-85% -оценка «хорошо»: обучающийся демонстрирует полное знание учебно-программного материала, успешно выполняющий предусмотренные программой задания, показывающий систематический характер знаний по дисциплине и способный к их самостоятельному пополнению и обновлению в ходе дальнейшего обучения в вузе и в будущей профессиональной деятельности;

50-70% -оценка «удовлетворительно»: обучающийся обнаруживает знание основного учебного программного материала в объеме, необходимом для дальнейшего обучения, выполняющего задания, предусмотренные программой, допустившим неточности в ответе, но обладающим необходимыми знаниями для их устранения;

менее 50% -оценка «неудовлетворительно»: обучающийся демонстрирует пробелы в знаниях основного учебного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.

На этапе промежуточной аттестации используется система оценки успеваемости обучающихся, которая позволяет преподавателю оценить сформированность планируемых результатов обучения, а также уровень освоения материала обучающимися.

Форма оценки знаний: оценка - 5 «отлично»; 4 «хорошо»; 3 «удовлетворительно»; 2 «неудовлетворительно». возможно использовать балльно-рейтинговые оценки.

Основанием для определения оценки на зачете служит уровень освоения обучающимся материала и формирования компетенция, предусмотренных учебным планом.

Успеваемость на зачете определяется оценками: «зачтено»; «не зачтено».

Оценка	Критерии оценивания	Балльно-рейтинговая оценка
«Зачтено»	Обучающийся освоил компетенции дисциплины на 51-100 % и показал хорошие знания изученного учебного материала, логично и последовательно изложил и полностью раскрыл смысл предлагаемого вопроса; продемонстрировал умение применить теоретические знания для решения практической задачи; выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	51-100
«Не зачтено»	Обучающийся освоил компетенции дисциплины менее чем на 51% и при ответе на предлагаемый вопрос выявились существенные пробелы в знаниях учебного материала, неумение с помощью преподавателя получить правильное решение практической задачи; не в полном объеме выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	0- 50

Основанием для определения оценки на экзамене служит уровень освоения обучающимся учебного материала, умение решать практические задачи и формирования компетенция, предусмотренных учебным планом.

Успеваемость на экзамене определяется оценками: «отлично»; «хорошо; «удовлетворительно»; «не удовлетворительно».

Оценка	Критерии оценивания	Балльно-рейтинговая оценка
«Отлично»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования на 86-100 %, показал глубокие знания учебного материала, логично и последовательно изложил содержание ответов на вопросы билета; продемонстрировал умение иллюстрировать теоретические положения конкретными примерами и свободно выполнять экзаменационные задания; усвоил основную и ознакомился с дополнительной литературой; выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	86-100
«Хорошо»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования на 61-85 %, показал глубокие знания учебного материала, логично и последовательно изложил содержание ответов на вопросы билета, но допустил несущественные неточности; продемонстрировал умение иллюстрировать теоретические положения конкретными примерами и выполнять экзаменационные задания; усвоил основную и ознакомился с дополнительной литературой; выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	61-85
«Удовлетворительно»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования на 51-60 %, показал знания учебного материала в объеме, необходимом для дальнейшего освоения учебных программ, но допустил погрешности в изложении ответов на вопросы билета и при выполнении экзаменационных заданий; ознакомился с основной литературой, рекомендованной программой; справился с контрольными заданиями, предусмотренными рабочей программой дисциплины	51-60
«Не удовлетворительно»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования менее чем на 51 %, обнаружил пробелы в знаниях учебного материала, допустил принципиальные ошибки в	0-50

	выполнении контрольных заданий, предусмотренных рабочей программой дисциплины	

Интегральная оценка

Критерии	Традиционная оценка	Балльно-рейтинговая оценка
5	5	86 - 100
4	4	61-85
3	3	51-60
2 и 1	2, Незачет	0-50
5, 4, 3	Зачет	51-100