Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Костровец Лариса Борисовна
Должность: директор
Дата подписания: 21.10.2026 12:13:22
Уникальный программный ключ:
6882606104c36dbde41c4ab93a65382136a292d6

Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.08 Информационная безопасность информационных систем и сетей

(индекс, наименование дисциплины в соответствии с учебным планом)

09.03.03 Прикладная информатика
(код, наименование направления подготовки/специальности)

Прикладная информатика в управлении корпоративными информационными системами
(наименование образовательной программы)

Очная форма обучения
(форма обучения)

Год набора – 2026
Донецк

Автор(ы)-составитель(и) РПД:

Семичастный Игорь Леонидович, доцент кафедры информационных технологий

Заведующий кафедрой:

Брадул Наталья Валерьевна, канд. физ.-мат. наук, заведующий кафедрой информационных технологий

Рабочая программа дисциплины Б1.В.01.08 Информационная безопасность информационных систем и сетей одобрена на заседании кафедры информационных технологий факультета государственной службы и управления Донецкого филиала РАНХиГС.

Протокол № 7 от «05» марта 2026 г.

СОДЕРЖАНИЕ

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

2. Объем и место дисциплины в структуре образовательной программы

3. Содержание и структура дисциплины

4. Типы оценочных материалов, показатели и критерии их оценивания

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

7. Методические материалы по освоению дисциплины

8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

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

Дисциплина Б1.В.01.08 Информационная безопасность информационных систем и сетей обеспечивает формирование у обучающихся следующих общепрофессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС *(при наличии)* **	**Код компетенции ****	**Наименование Компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
B/06.5 Адаптация бизнес-процессов заказчика ИС к возможностям типовой ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС	ПК-1	Способен адаптировать бизнес-процессы заказчика ИС к возможностям типовой ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС	ПК-1.5	Утверждает у заказчика предлагаемые изменения его бизнес-процессов для реализации их автоматизации в типовой ИС	**Знает** З-4 Коммуникационное оборудование, З-5 Сетевые протоколы, З-10 Основы ИБ организации, З-13 Современные подходы и стандарты автоматизации организации, З-15 Основы организации производства.

** Дисциплина может формировать компетенцию полностью или частично.*
***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Общий объем дисциплины:

3,00 з.е., 108 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 59 ак. час на контактную работу с преподавателем, из них 16 ак. час на лекции и 32 ак. час на практические занятия, 2 часа на КЭ, 9 часов на Каттэк. 31 ак. час на самостоятельную работу обучающихся.

Б1.В.01.08 Информационная безопасность информационных систем и сетей реализуется в 6-м семестре 3-го курса после изучения дисциплин:

- ИТ инфраструктура предприятия;
- Корпоративные информационные системы.

.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИС И СЕТЕЙ															
Тема 1.1	Проблемы информационной безопасности сетей	10	2	0	0	4	0	0	0	0		0	0	4	Контрольные вопросы, практические занятия, КТ1

Тема 1.2	Угрозы и уязвимости проводных корпоративных сетей	10	2	0	0	4	0	0	0	0		0	0	4	Контрольные вопросы, практические занятия, КТ1
Тема 1.3	Технология защиты межсетевого обмена данными. Брандмауэры.	10	2			4								4	Контрольные вопросы, практические занятия, КТ1
Тема 1.4	Технологии VPN.	10	2			4								4	Контрольные вопросы, практические занятия, КТ1
Тема 1.5	ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP	10				4								4	Контрольные вопросы, практические занятия, КТ1
РАЗДЕЛ 2. ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА УРОВНЯХ МОДЕЛИ OSI															

Тема 2.1	Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.	10	2	0	0	4	0	0	0	0		0	0	4	Контрольные вопросы, практические занятия, КТ2
Тема 2.2	Защита на сетевом уровне — протокол IPSec	9	2	0	0	4	0	0	0	0		0	0	3	Контрольные вопросы, практические занятия, КТ2
Тема 2.3	Инфраструктура защиты на прикладном уровне	10	2			4			2	9			18	4	Контрольные вопросы, практические занятия, КТ2
Промежуточная аттестация		**108**	**16**	**0**	**0**	**32**	**0**		**2**	**9**	**0**	**0**	**18**	**31**	**Экзамен**
Итого		**108**	**16**	**0**		**32**	**0**		**2**	**9**	**0**	**0**	**18**	**31**	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИС И СЕТЕЙ

Тема 1.1 Проблемы информационной безопасности сетей. ПК-1.5

Содержание лекции: Технологии информационной безопасности сетей. Структура телекоммуникационной сети. Классификация сетей передачи данных. Сети с коммутацией каналов. Функции маршрутизаторов в них. Сети с коммутацией пакетов. Семиуровневая модель взаимодействия открытых систем. Понятие межуровневого интерфейса. Устройства и единицы информации соответствующих уровней. Сетенезависимые и сетезависимые уровни передачи данных. Процесс инкапсуляции (encapsulation) данных. Инкапсуляция сегмент в пакет данных с заголовком, его содержимое. Инкапсуляция пакета канальном уровне в кадр или фрейм данных. Функции различных уровней в модели OSI.

Практическая подготовка: Сформировать структуру телекоммуникационной сети. Описать процесс передачи сообщения в ней. Разъяснить функции коммутации и маршрутизации. Сформулировать описание работы и основных процессов в сети с коммутацией каналов. Сформулировать описание работы и основных процессов в сети с коммутацией пакетов. Описать содержание пакета передачи данных. Описать процесс адресации в телекоммуникационной сети. Охарактеризовать локальные и глобальные сети. Описать технологии, которые используются в ISDN (Integrated Services Digital Network**)** цифровой сети интегрированных услуг. Дать общую характеристику семиуровневая модели взаимодействия открытых систем (OSI). Объяснить какие виды оборудования работают на конкретных уровня этой модели и какие функции они выполняют в процессе передачи данных.

Тема 1.2. Угрозы и уязвимости проводных корпоративных сетей. ПК-1.5

Содержание лекции: Структура и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности. Протокол пересылки файлов FTP. Его назначение и функции. Протокол Telnet, его назначение и функции. Протокол SNMP (Simple Network Management Protocol) , его назначение и функции. Протокол управления передачей TCP (Transport Control Protocol), назначение и функции. Протокол дейтаграмм пользователя UDP (User Datagram Protocol), его назначение и функции. Функции уровеня межсетевого взаимодействия (Internet). Логические и физические соединения между уровнями стека протоколов TCP/IP. Общие проблемы безопасности IP-сетей. Цели нарушителя, осуществляющего сетевую атаку. Наиболее распространенные виды сетевых атак. Угрозы и уязвимости проводных корпоративных сетей.

Практическая подготовка: Дать определение телекоммуникационной сети. Дать определение процессу маршрутизации. Определить, что такое телекоммуникационная сеть с коммутацией каналов. Определить, что такое телекоммуникационная сеть с коммутацией пакетов. Дать определение сетевому протоколу. Определить, что такое семиуровневая модель взаимодействия открытых систем. Обозначить функцию, которую в сетях с коммутацией каналов, выполняют телекоммуникационные узлы. Описать, что необходимо задавать в телекоммуникационной сети для создания маршрута. Объяснить, почему сети, работающие на основе технологии IP являются дейтаграммными. Разъяснить в каком виде происходит Виртуальный обмен между соответствующими уровнями конечных узлов в модели OSI происходит. Описать, что **является единицами** виртуального обмена между соответствующими уровнями конечных узлов на транспортном уровне модели OSI

Тема 1.3 Технология защиты межсетевого обмена данными. Брандмауэры. ПК-1.5

Содержание лекции: Брандмауэр как программно-аппаратный комплекс. Функции, которые выполняет брандмауэр. Виды брандмауэров. Преимущества использования брандмауэра. Угрозы использования брандмауэров. Два типа атак на брандмауэры. Последствия успешных атак, приведших к разрушению защиты сети на основе использования брандмауэров.
Межсетевой экран как средство от защиты от вторжения из Интернет. NGFW Основные функции NGFW **(Next-Generation Firewall)**. Функциональные требования и компоненты межсетевых экранов. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. основные режимы использования брандмауэра MS Windows

Практическая подготовка: Дать определение брандмауэру как программно-аппаратному средству, которое фильтрует входящий и исходящий трафик на основе заданных правил. Перечислить и проиллюстрировать его основные функции: блокировка несанкционированного доступа, защита от вредоносных программ, ограничение перемещения злоумышленников внутри сети. Сформулировать и продемонстрировать принципы работы, такие как фильтрация по IP-адресам, портам, протоколам, и в продвинутых решениях — по конкретным приложениям. Осуществить настройку брандмауэра (на примере Windows) через «Панель управления». Создать правила для разрешения или блокировки трафика по конкретным критериям: программам, портам, протоколам, IP-адресам. Осуществить доступ к настройкам брандмауэра через «Панель управления» или команду wf.msc. Осуществить настройку исключений для приложений, которые должны иметь особый доступ. Блокировать исходящий трафик для повышения безопасности и создание правил для разрешения только необходимого трафика (например, для обновлений, DNS, корпоративных сервисов). Ручная проверка брандмауэра

через попытки подключения к защищаемым сервисам или «пинг» узла. Использование инструментов для сканирования портов и проверки доступности сервисов, для проверки конкретных портов и протоколов. Анализ журналов брандмауэра на предмет заблокированных, но легитимных попыток соединения.

Тема 1.4 Технологии VPN. ПК-1.5

Содержание лекции: Концепция построения виртуальных защищенных сетей VPN - Основные понятия и функции сети VPN. Определение вмртуальной защищенной сети (VPN (Virtual Private Network). Туннель VPN. Три базисных технологии, на которых осована защита информации в процессе ее передачи по туннелю VPN. VPN-клиент и VPN-сервер. Шлюз безопасности VPN (security gateway). Ваоианты реализации шлюаз безопасности VPN (security gateway). Суть технологии ткннелирования. Варианты построения виртуальных защищенных каналов. Туннелирование как средство защиты не только конфиденциальности содержимого пакета, но и его целостности и аутентичности. Распространение электронной цифровой подписи на все поля пакета**.** Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей. Классификация сетей VPN. Основные варианты архитектуры VPN. Некоторые изменения в технологиях VPN после 2022 года Преимущества применения технологий VPN

Практическая подготовка: Установить Jami на ПК и на смартфоне. Далее выполнить между ними обмен сообщениями, отразите эти процессы в презентации-отчете. При защите отчета по работе необходимо осуществить коммуникацию с преподавателем, пользуясь версией Jami на своем смартфоне. Установить Chattii на ПК и на смартфоне. Далее выполните между ними обмен сообщениями, отразить эти процессы в презентации-отчете. При защите отчета по работе необходимо осуществить коммуникацию с преподавателем, пользуясь версией Chattii на своем смартфоне. Установить Olvid на ПК и на смартфоне. Далее выполнить между ними обмен сообщениями, отразить эти процессы в презентации-отчете. При защите отчета по работе необходимо осуществить коммуникацию с преподавателем, пользуясь версией Olvid на своем смартфоне. Сформулировать ответ на вопрос: работают ли три изученных нами мессенджера без VPN. Сформулировать недостатки мессенджера Telegram, обосновав каждую позицию в вашем перечне. Сформулировать список требований к современному надежному мессенджеру, обосновав каждую позицию в списке. Дать ответ на вопрос: соответствуют ли три изученных вами мессенджера, предъявленным в вашем списке требованиям. Дать оценку по 100-балльной шкале каждому из них

Тема 1.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP. ПК-1.5.

Содержание лекции: Распространение стека протоколов TCP/IP, стек как основы для глобальной сети Интернет. Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/протокол интернета) как сетевая модель, описывающая процесс передачи цифровых данных. Уровневая модель TCP/IP в сравнении с уровневой моделью OSI. Канальный уровень (link layer). Межсетевой уровень (internet layer). IPv4 и IPv6. ICMP (Internet Control Message Protocol) как сетевой протокол, который используется для обмена диагностическими и управляющими сообщениями между устройствами в сети. Транспортный уровень (transport layer). TCP ((Transmission Control Protocol, протокол управления передачей). UDP ((User Datagram Protocol, протокол пользовательских датаграмм). Прикладной уровень (application layer). Протоколы прикладного уровня, их назначение. DNS (Domain Name System) , цели использования службы. Point-to-Point (PPP) протокол от точки к точке. И два его подвида

♦ **Практическая подготовка:** Сбор и анализ данных о компаниях и физических лицах. Проверить юридические лица через **ЕГРЮЛ**, **Росреестр**, **реестр ФССП**.

Проверить юридическое лицо через ЕГРЮЛ можно несколькими способами, все они обеспечивают доступ к актуальной информации из единого государственного реестра юридических лиц. С помощью сайта https://vsednr.ru/perechen-proizvoditeley-produkcii-n/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (Все о ДНР) найдите информацию о следующих предприятиях на территории ДНР (использовать различные задания)

- трех производителях кабельной продукции;
- трех производителях продукции коксохимии;
- ФИЛИАЛЕ №1 «ХАРЦЫЗСКИЙ СТАЛЕПРОВОЛОЧНЫЙ-КАНАТНЫЙ ЗАВОД «СИЛУР» ООО «РОСТЭКСПОСНАБ 8»;
- трех предприятиях машиностроительной промышленности;
- трех предприятиях химической промышленности;
- трех предприятиях фармацевтической промышленности;
- трех предприятиях бумажной промышленности;
- трех предприятиях легкой промышленности;

Найдя эти предприятия в ДНР, зафиксируйте их наименования, ИНН и найдите по ним информацию на **egrul.nalog.ru (**https://egrul.nalog.ru/index.html)

1. Проверить, есть ли эта информация на Госуслугах
2. Проверить свой e-mail и номера телефонов на наличии утечки с помощью сервиса Have I Been Pwned (https://haveibeenpwned.com/).
3. Придумать пароль и проанализировать его на устойчивость и утечки с помощью сервиса **Hibp Passwords.** Проверьте несколько паролей длиной в 10, 12,16 и 20 символов с помощью https://haveibeenpwned.com/Passwords. Отразить результаты проверки в отчете -презентации

4. С помощью ресурса https://xn--b1aew.xn--p1ai/wanted проверить не находится ли человек в розыске по линии МВД РФ. Установите через какое время после запроса пользователю предоставляется ответ
5. Задание. Найти через ГлазБога (Телеграм) информацию о себе

С помощью чат-бота Телеграма «Глаз Бога» (**https://t.me/glaszbogazsearch)** вы найдите информацию о себе (**Слайы на с .6)**)
«Глаз Бога» - это инструмент OSINT

6. Найти в сети информацию о себе, используя ШаралокБот https://t.me/sharalok_bot) @sharalok_bot.м
7. Найти в сети инструменты по пробиву информации о себе на VK
8. Сформулируйте, как пользуясь фреймворком https://osintframework.com/ , систематизировать открытые данные об физлице или организации. Приведите свой пример использования этого инструмента и дайте ему оценку
9. На ваш взгляд, является ли этот инструмент инструментом поиска цифрового следа человека или организации в Интернет? Обоснуйте свой ответ

РАЗДЕЛ 2. РАЗДЕЛ 2. ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА УРОВНЯХ МОДЕЛИ OSI

Тема 2.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне. ПК-1.5

Содержание лекции: Протоколы формирования защищенных каналов на канальном уровне. Протокол PPTP (Point-to-Point Tunneling Protocol). Пакеты, передаваемые в рамках сессии PPTP. Архитектура протокола PPTP. Аутентификация удаленного пользователя в рамках протокола PPTP. Схема туннелирования при прямом соединении удаленного компьютера с Интернетом. Схема туннелирования при подключении удаленного компьютера к Интернету по через провайдера. Протокол L2F (Layer-2 Forwarding) как протокол защищенного туннелирования PPP-трафика через сети общего назначения с произвольной средой. Протокол L2TP с возможностью открывать между конечными абонентами нескольких туннелей, каждый из которых может быть выделен для отдельного приложения. Три этапа формирования защищенного виртуального канала в протоколе L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL/TLS. Протокол SSL как протокол защищенного канала, работающего на сеансовом уровне модели OSI. Использование инфраструктуры открытых ключей PKI (Public Key Infrastructure). Протокол TLS (Transport Layer Security), который базируется на протоколе SSL, как современный стандарт Интернета. Технологии защиты беспроводных сетей. Стандарт WPA (Wi-Fi Protected Access). Аутентификация пользователей по протоколу RADIUS, обеспечивающим централизованную аутентификацию, авторизацию и учёт пользователей.

Практическая подготовка: Изучить разделы методических указаний и ответить на вопросы для самопроверки, приведенные в конце темы. Скачать с сайта https://gpg4usb.org/download.html и установить программу с помощью архива gpg4usb 0.3.3.-2.zip. Изучите ее интерфейс и функциональные

возможности. Скачайте с ЯндексДиска и установите программу Free File View Pro, пользуясь ссылкой https://disk.yandex.ru/d/2UPIJp81VZmrlg. Создать свои открытый и закрытый ключи, пользуясь программой gpg4usb 0.3.3.-2. Сохранить их для дальнейшего использования. Зашифровать с помощью открытого ключа файл, затем расшифровать его. Обменяться открытыми ключами с товарищем по группе. Осуществить передачу файлов с ним по электронной почте или в мессенджере. Осуществить операции подписания и зашифрования, расшифрования с этими файлами

Тема 2.2. Защита на сетевом уровне — протокол IPSec. ПК-1.5

Содержание лекции: Защита информации на сетевом уровне. Стек протоколов IPSec как инструмент для аутентификации участников обмена, туннелирования трафика и шифрования IP-пакетов. Протокол аутентифицирующего заголовка AH. Основные протоколы IPSec: протоколы AH (Authentication Header) и ESP (Encapsulating Security Payload). База данных политик безопасности SPD (Security Policy Database). База данных безопасных ассоциаций SAD (Security Association Database). Управление политикой безопасности и безопасными ассоциациями SA. Архитектура стека протоколов IPSec. Протокол согласования параметров виртуального канала и управления ключами IKE (Internet Key Exchange). Особенности протоколов защиты виртуального канала верхнего уровня архитектуры IPSec (AH и ESP). Нижний уровень архитектуры IPSec - домен интерпретации DOI (Domain of Interpretation), его роль как фундамента уровня архитектуры IPSec. Сравнительный анализ протоколов ESP и AH. Протокол управления криптоключами IKE. Установление безопасной ассоциации SA(Security Associations). Основные схемы применения IPSec

Практическая подготовка: С сайта разработчика https://www.gpg4win.org/download.html скачать программу gpg4win 0.4.4 и установить ее. Установить программу Kleopatra на своем ПК, изучить ее интерфейс и функциональные возможности. Сгенерировать с ее помощью свои публичный (открытый) и закрытый ключи. Сохранить их для дальнейшей работы. Переслать свой публичный (открытый) ключ участникам электронного обмена информацией. Получить публичные (открытые) ключи от участников электронного обмена информацией. Сохранить их в программе gpg4win 0.4.4. Подписать ключи партнёров и установить к ним доверие. Создайть файл(ы) в MS Word, зашифровать их, подписать электронной подписью и передайть участнику обмена информацией, ключом которого шифровался файл. Получить от участников обмена информацией зашифрованные и подписанные файлы и расшифровать их. Создайть отчет по работе в формате презентации, в котором отобразить выполненные задания

Тема 2.3. Инфраструктура защиты на прикладном уровне. ПК-1.5

Содержание лекции: Защита на прикладном уровне. Управление идентификацией и доступом: процесс создания доверенной среды; управление доступом, позволяющее авторизованным пользователям получать доступ к требуемым ресурсам; шифрование, гарантирующее, что связь между пользователем и базовой инфраструктурой защищена; неотказуемость, означающую, что пользователи не могут позднее отказаться от выполненной транзакции (обычно реализуется с помощью цифровой подписи и инфраструктуры открытых ключей). Особенности управления доступом: управление сетевым доступом (регулирует доступ к ресурсам внутренней сети организации); управление Web-доступом (регулирует доступ к Web-серверам и их содержимому). Функционирование системы управления доступом. Средства управления сетевым доступом. Средства управления Web-доступом. Протоколы аутентификации удаленных пользователей: протокол PAP, протокол CHAP. Централизованный контроль удаленного доступа. Использование централизованной службы аутентификации и авторизации. Протоколы TACACS (Terminal Access Controller Access Control System) и RADIUS (Remote Authentication Dial-In User Service).

Практическая подготовка: Анализ сетевого трафика с помощью программы Wireshark.
Загрузить и установить программу Wireshark (необязательно при использовании ПО на удаленном сервере). Изучить функции и категории модели OSI и ответить на вопросы, описывающие работу Wireshark. Ознакомиться с методическими рекомендациями при использовании программы Wireshark. Собрать и провести анализ данных протокола ICMP по локальным узлам в программе Wireshark. Начать и остановить сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам. Найти данные об IP- и MAC-адресах в полученных PDU. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark. Начать и остановить сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам. Найти данные об IP- и MAC-адресах в полученных PDU. Пояснить, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов. При этом описать все протоколы, используемые утилитой. Описать все поля протоколов. Составить диаграмму взаимодействия машин при работе утилиты *ping*. Захватить 100 произвольных пакетов. Определить статистические данные: процентное соотношение трафика разных протоколов в сети; среднюю скорость кадров/сек; среднюю скорость байт/сек; минимальный, максимальный и средний размеры пакета; степень использования полосы пропускания канала (загрузку сети); на примере любого IP-пакета указать структуры протоколов Ethernet и IP, отметить поля заголовков и описать их.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.01.08 Информационная безопасность информационных систем и сетей входят в

состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа – это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы

Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр

Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2. Продумать логику и полноту ответа. 3. Записать ответ, используя четкие компактные формулировки. 4. В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3. Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Оценка по шкале ECTS	**Сумма баллов за все виды учебной деятельности**	**Оценка по государственной шкале**	**Определение**
A	90 – 100	«Отлично»	Отличное выполнение с незначительным количеством неточностей
B	80 – 89	«Хорошо»	в целом правильно выполненная работа с незначительным количеством ошибок (до 10%)
C	75 – 79		в целом правильно выполненная работа с незначительным количеством ошибок (до 15%)
D	70 – 74	«Удовлетворительно»	неплохо, но со значительным количеством недостатков
E	60 – 69		Выполнение удовлетворяет минимальные критерии
FX	35 – 59	«Не удовлетворительно»	с возможностью повторной сдачи
F	0 – 34		с обязательным повторным изучением дисциплины (выставляется комиссией)

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
100 баллов	100 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины Б1.В.01.08 Информационная безопасность информационных систем и сетей используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Контрольные вопросы для проведения опроса, задания открытого типа на практических занятиях, контрольные задания

Таблица 5.1.

Распределение баллов по видам учебной деятельности (БРС)

Раздел/Темы	Формы текущего контроля		КТ
	УО	ПЗ	
Р-1. / Т-1.1	3	3	
Р-1. / Т-1.2	3	5	6
Р-1. / Т-1.3	3	3	
Р-1. / Т-1.4	3	5	7
Р-2. / Т-2.1	3	4	
Р-2. / Т-2.2	3	5	8
Р-2. / Т-2.3	4	4	
Р-2. / Т-2.4.	3	4	12
Р-2. / Т-2.5.	4	5	
Итого: 100 б	**29**	**38**	**33**

УО – устный опрос;
ТЗ – тестовое задание;
КЗ – контрольные задания;
ПЗ – практическое занятие;
Д – доклад;
КТ – контрольные точки.

Критерии оценивания опроса:

Балы	Описание критерия
4	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
2-3	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
1	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал

0* - в журнал академической группы не выставляется

Критерии оценивания практических занятий:

Балы	Описание критерия	
4-5	Свыше 90% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
2-3	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
1	Реализовано более 50% поставленных задач	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0	Реализовано менее 30% поставленных задач.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

0* - в журнал академической группы не выставляется

Критерии оценивания контрольных заданий:

Балы	Описание критерия
10-12	Обучающимся задание выполнено без ошибок и в полном объеме.
7-9	Обучающимся в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.
5-6	Обучающимся допущены отдельные ошибки при выполнении задания
0-4	У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

0* - в журнал академической группы не выставляется

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИС И СЕТЕЙ

Тема 1.1. Проблемы информационной безопасности сетей

Контрольные вопросы для проведения опроса:

1. Сформулируйте, что собой представляют телекоммуникационные сети?
2. Объясните, чем принципиально отличаются сети с коммутацией каналов от сетей с коммутацией сообщений? Приведите примеры
3. Опишите, какие функции выполняет маршрутизатор?
4. Разъясните, что собой представляет метрика протокола маршрутизации?
5. Разъясните, в чем различие коммутации пакетов или сообщений?
6. Объясните, в чем различие между локальными и глобальными сетями передачи данных?

Практические занятия:

Задания открытого типа с развернутым ответом.

Разъяснитm, какую роль в инфраструктуре открытых ключей (Public Key Infrastructure, PKI) играет удостоверяющий Центр (УЦ)

Описать функции сертификатов УЦ, а также их содержание

Описать алгоритм RCA. Разъясните, какую роль в его реализации выполняет функция Эйлера

Сформулировать преимущества асимметричных криптосистем

Описать структуру криптосистемы PGP

Объяснить, какую роль в криптосистеме PGP играет механизм цифровой подписи

Сформулировать, каким образом в криптосистеме PGP реализуется механизм цифровой подписи

Описать недостатки криптосистеме PGP

Сформулировать, какие криптоалгоритмы могут использоваться для защиты передачи данных

Сформулировать, чем алгоритм Диффи-Хеллмана отличается от симметричных алгоритмов

Тема 1.2. Угрозы и уязвимости проводных корпоративных сетей

Контрольные вопросы для проведения опроса:

1. Опишите процесс инкапсуляция данных и ту роль, которую он выполняет в стеке TCP/IP
2. Разъясните, какие устройства функционируют на Уровне 3 модели OSI?
3. Опишите, какие устройства функционируют на Уровне 2 модели OSI?
4. Сформулируйте и опишите, какие устройства функционируют на Уровне 1 модели OSI?
5. Перечислите уровни модели TCP/IP и опишите основные функции каждой из них.
6. Сформулируйте, какие три системы адресации используются в сетевых технологиях?

Практические занятия:

Задания открытого типа с развернутым ответом.

Разъяснить, что определяет модель OSI в рамках функционала процессов стандартизации

Объяснить, что такое стек протоколов на примере стека TCP/IP

Разъяснить, какие функции выполняет каждый из протоколов в этом стеке

Сформулировать неоспоримые преимущества стека протоколов TCP/IP

Объяснить, какие уровни модели OSI соответствуют прикладному уровню стека протоколов TCP/IP и какие протоколы на нем функционируют

Объяснить, какие уровни модели OSI соответствуют транспортному уровню стека протоколов TCP/IP и какие протоколы на нем функционируют

Объяснить, какие уровни модели OSI соответствуют уровню межсетевого взаимодействия стека протоколов TCP/IP и какие протоколы на нем функционируют

Объяснить, какие уровни модели OSI соответствуют уровню сетевого интерфейса стека протоколов TCP/IP и какие протоколы на нем функционируют

Разъяснить, в чем заключается основной недостаток стека протоколов TCP/IP

Тема 1.3. Технология защиты межсетевого обмена данными. Брандмауэры.

Контрольные вопросы для проведения опроса:

1. Опишите четырехуровневую технологическую модель подсистемы информационной безопасности
2. Опишите структуру и функциональность стека протоколов TCP/IP
3. Разъясните, как реализуются логические и физические соединения между уровнями стека протоколов TCP/IP
4. Опишите угрозы и уязвимости проводных корпоративных сетей
5. Опишите функциональные требования и компоненты межсетевых экранов
6. Сформулируйте и опишите основные схемы сетевой защиты на базе межсетевых экранов.

Практические занятия:

Задания открытого типа с развернутым ответом.

Сформулировать, как реализуется протокол P2P (точка-точка). В чем заключается его основная особенность

Приведите примеры сервисов, работа которых построена на использовании протокола P2P на примере использования программы Jami

Для этого установить его на смартфоне и осуществить электронную коммуникацию с преподавателем

Провести звонок на смартфон преподавателя с помощью программы Jami, осуществить видеотрансляцию и передачу файлов

Объяснить, в чем заключаются особенности протокола P2P в реализации

Разъяснить как происходит ее реализация без использования VPN при работе с программой Jami

Установить программу Olvid на смартфоне. Провести звонок на смартфон преподавателя, осуществить видеотрансляцию и передачу файлов

Сформулировать, какие ограничения, на ваш взгляд, имеют место в работе протокола P2P

Сформулируйте, для каких сервисов применим протокол P2P в первую очередь

Разъяснить, распространение каких угрозы, на ваш взгляд, может быть связано с применением протокола P2P

.

Тема 1.4. Технологии VPN

Контрольные вопросы для проведения опроса:

1. Сформулируйте, что такое виртуальная защищенная сеть и туннель VPN.
2. Опишите, на каких технологиях основана защита информации в процессе ее передачи по туннелю VPN?
3. Приведите описание таким категориям, как VPN-клиент, VPN-сервер и шлюз безопасности VPN
4. Разъясните, как реализуется технология туннелирования
5. Сформулируйте, как технология туннелирования решает проблему защиты конфиденциальности, целостности и аутентичности передаваемой информации
6. Разъясните, какие протоколы играют роль протокола-«пассажира», несущего протокола и протокола туннелирования в технологии VPN

Практические занятия:

Задания открытого типа с развернутым ответом.

С помощью сайта https://vsednr.ru/perechen-proizvoditeley-produkcii-n/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (Все о ДНР) найдите информацию о следующих предприятиях на территории ДНР (использовать различные задания):

трех предприятиях машиностроительной промышленности;

трех предприятиях угольной промышленности;

трех предприятиях металлургической промышленности;

трех предприятиях мебельной промышленности.

трех предприятиях промышленности строительных и нерудных

материалов.

Разъяснить, каковы варианты построения виртуальных защищенных каналов при использовании VPN

Объяснить, почему вариант, при котором конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений, с точки зрения обеспечения информационной безопасности является лучшим?

Разъяснить, с помощью каких компонент в узлах защищенного соединения сети VPN создается туннель

Описать, как обеспечивается конфиденциальность, а также целостность и подлинность инкапсулируемых пакетов при туннелировании в сети VPN

Разъяснить, что понимают под конфиденциальностью, целостностью и доступностью с точки зрения критериев VPN безопасности?

Тема 1.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP

Контрольные вопросы для проведения опроса:

1. Разъяснить как работает протокол TCP.
2. Описать работу протокола UDP.
3. Построить четырехуровневую модель стека протоколов TCP/IP
4. Объяснить, как работают протоколы прикладного уровня в стеке TCP/IP
5. Сформулировать, какую роль выполняют в нем библиотеки и программные интерфейсы приложений (API, Application Programming Interface)
6. Разъяснить, какую роль выполняет порт на этом уровне и что означает термин «сокет»

Практические занятия:

Задания открытого типа с развернутым ответом.

Разъяснить с какой целью был разработан стек протоколов TCP/IP.

Построить семиуровневую модель OSI.

Построить четырехуровневую модель стека протоколов TCP/IP

Выполнить сравнительный анализ двух уровневых моделей

Объяснить, для каких целей применяется на практике семиуровневую модель OSI и четырехуровневую модель стека протоколов TCP/IP

Сформулировать, какие протоколы применяются на канальном, межсетевом и транспортном уровне.

РАЗДЕЛ 2. ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА УРОВНЯХ МОДЕЛИ OSI

Тема 2.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.

Контрольные вопросы для проведения опроса:

1. Разъясните, в чем заключается назначение средств VPN, которые используются на канальном и сеансовом уровне
2. Опишите, какие протоколы используются на канальном и сеансовом уровне, для формирования защищенных каналов в сети VPN
3. Сформулируйте, какие функции необходимо реализовывать протоколам на канальном и сеансовом уровне в сети VPN, для создания защищенного соединения
4. Опишите протоколы формирования защищенных каналов на сеансовом уровне в сети VPN
5. Сформулируйте, какие функции необходимо реализовывать протоколам на сеансовом уровне в сети VPN

Практические занятия:

Задания открытого типа с развернутым ответом.

С помощью программы gpg4usb 0.3.3.-2 (https://gpg4usb.org/download.html) выполнить следующие действия

Установить программу локально на своем ПК

Сгенерировать с помощью Менеджера ключей сначала открытый. а затем и закрытый ключ

Осуществить операцию подписания текстового сообщения для его передачи абоненту

Осуществить операции подписать и зашифровать передаваемый текст

Выполнить операцию Проверить для подписанного текста

Выполнить операцию Расшифровать для данного текста

Рязъяснить связь ЭЦП и асимметричного шифрования на примере использования программы gpg4usb 0.3.3.-2

Разъяснить какую функцию выполняет открытый ключ в процессе шифрования

Разъяснить назначение секретного ключа в процессе Расшифрования

Тема 2.2. Защита на сетевом уровне — протокол IPSec

Контрольные вопросы для проведения опроса:

1. Сформулируйте преимущества средств безопасности IPSec
2. Опишите основные схемы применения IPSec
3. Опишите архитектуру стека протоколов IPSec и изобразите его в виде схемы
4. Опишите структуру заголовок протокола AH и назначение его полей
5. Сформулируйте и опишите функции протокола инкапсулирующей защиты ESP, а также режимы его использования
6. Опишите структуру алгоритма HMAC
7. Сформулируйте и опишите функции протокола управления криптоключами IKE

Практические занятия:

Задания открытого типа с развернутым ответом.

С сайта разработчика https://www.gpg4win.org/download.html скачайте программу gpg4win 0.4.4 и установите ее. Установите программу **Клеопатра**

С помощью программы Клеопатра совершить обмен по крайней мере с одним абонентом (студентом группы):

- текстовым документом;
- изображением;
- электронной таблицей;
- видеофайлом.

Проделанные операции необходимо также отразить в отчете-презентации по данной работе. При этом описывается пошагово вся процедура:

создание пары ключей и сохранение резервной копии закрытого ключа;

получение открытого ключа абонента и отправка ему своего открытого ключа;

зашифровывание текста, который пересылается абоненту его открытым ключем;

получение от него файла, зашифрованного вашим открытым ключем и его расшифрование;

заверение сертификата вашего ключа и аналогичная процедура для ключа, полученного от другого абонента;

зашифруйте как минимум одну вашу папку с помощью программы Клеопатра;

опишите как осуществляется ее расшифрование в программе Клеопатра;

изучите как выполняется операция «Создать запрос сертификата S/MIME» в программе Клеопатра и опишите все объекты, которые вам необходимо иметь на своем ПК для ее выполнения.

Тема 2.3. Инфраструктура защиты на прикладном уровне

Контрольные вопросы для проведения опроса:

1. Сформулируйте, решение каких задач необходимо для обеспечение информационной безопасности организации на прикладном уровне
2. Объясните, какую систему управления доступом пользователей к информации необходимо организовать для обеспечения информационной безопасности организации на прикладном уровне
3. Разъясните, как осуществляется управление идентификацией и доступом на прикладном уровне на примере электронного бизнеса
4. Изобразите схематично в виде рисунка и опишите механизм функционирование системы управления доступом из глобальной сети к разрешенным для удаленных пользователей ресурсам в организации
5. Объясните, как в механизме удаленного доступа к ресурсам в организации используются такие инструменты, как Web-доступ, VPN-доступ или удаленный доступ с использованием серверов RADIUS
6. Разъясните, какие типы аутентификации могут использоваться в механизме удаленного доступа пользователей к разрешенным ресурсам в организации
7. Сформулируйте, какие средства управления сетевым доступом или программные агенты используются в механизме удаленного доступа пользователей к разрешенным ресурсам в организации

Практические занятия:

Задания открытого типа с развернутым ответом.

Установить программу Whireshark, скачав ее с сайта разработчика (https://www.wireshark.org/)

Задать в строке фильтрации значение фильтра dns. Пояснить перехваченные сниффером пакеты. Сохранить пакеты в папке DNS

Задать в строке фильтрации значение фильтра udp. Пояснить перехваченные сниффером пакеты.

Задать в строке фильтрации arp. Поясните перехваченные сниффером пакеты. Сохраните пакеты в папке ARP

Задать в строке фильтрации http. Разъясните отсутствие результатов фильтрации программой Wireshark

Capture-Options-Input, задать в поле Capture filter for selected interface net 192.168.0.103. Затем Start. Объяснить перехваченный трафик

Организовать перехват пакетов, удовлетворяющих выражению:

tcp.port == 80 || udp.port == 80

Объясните, что означает это выражение

Осуществить операцию Stop, затем File-Save или Save As

Остановить работу программы. File – Export Objects – HTTP. Сохранить захваченные пакеты в папку ExportObjectsHTTP

Собрать и провести анализ данных протокола ICMP по локальным узлам в программе Wireshark

Начать и остановить сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.

Найти данные об IP- и MAC-адресах в полученных PDU.

Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.

Найдите данные об IP- и MAC-адресах в полученных PDU.

Поясните, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов.

При этом описать все протоколы, используемые утилитой. Описать все поля протоколов. Составить диаграмму взаимодействия машин при работе утилиты ping.

Захватить 100 произвольных пакетов. Определить статистические данные:

процентное соотношение трафика разных протоколов в сети;

среднюю скорость кадров/сек;

среднюю скорость байт/сек;

минимальный, максимальный и средний размеры пакета;

степень использования полосы пропускания канала (загрузку сети)

на примере любого IP-пакета указать структуры протоколов Ethernet и IP, отметить поля заголовков и описать их.

5.3 Один или несколько тематических блоков дисциплины завершаются контрольной точки по разделу (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной работы	Максимальное количество баллов за работу в рамках КР, которое может набрать студент	Коэффициент веса контрольной работы	Результат контрольной работы, участвующий в формировании итоговой балльной оценки по дисциплине
КТ 1	100	0,5	50
КТ 2	100	0,5	50
Итого:	х	1,0	100

Формула расчета результата контрольной работы:

Результат контрольной работы = Количество баллов за точку в рамках КТ Х Коэффициент веса контрольной точки.

5.4Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ-1

Задание 1. Установить отличия сетей с коммутацией каналов от сетей с коммутацией пакетов

Определить ключевые особенности сетей с коммутацией каналов по следующим характеристикам: фазам работы, фиксированной пропускной способности, низкой задержке, резервированию ресурсов, ограничениям. Привести примеры

Сформулировать ключевые особенности сетей с коммутацией пакетов по следующим характеристикам: динамической маршрутизации, буферизации, двум режимам работы, возможной задержке и потере пакетов, более эффективному использованию ресурсов.

Задание 2. Определить, что такое телекоммуникационная сеть

Необходимо описать структуру современной телекоммуникационной сети как совокупности образуется совокупностью абонентов и узлов связи, соединенных линиями, или каналами связи.

Задание 3. Сформулировать ключевые особенности пакетной организации обмена информацией

Текст задания

Сформулировать ключевые особенности пакетной организации обмена информацией. Описать следующие характеристики процесса: разбиение

данных на пакеты. структуру пакета, процесс независимой маршрутизации пакетов, механизмы обеспечения надёжности передачи, процесс буферизации, зависимость от протоколов. гибкость использования ресурсов сети, возможные задержки.

КТ-2

Задание 1. Дать определение и привести примеры ключевых характеристик для многоуровневой сети - протокола и интерфейса.

Текст задания

Раскрыть понятие многоуровневой сети

Сформулировать определение протокола для многоуровневой сети

Разъяснить понятие интерфейса для многоуровневой сети

Задание 2. Провести сравнительный анализ двух ключевых подходов к описанию и организации сетевого взаимодействия

Текст задания

Провести сравнительный анализ модели ISO/OSI и стека протоколов TCP/IP по следующим характеристикам: количеству уровней, методология разработки, стандартам и протоколам, детализации, области применения

Задание 3. Определение логических и физических соединений между уровнями стека протоколов TCP/IP

Текст задания

Описать логические и физические соединения между уровнями стека TCP/IP

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Для решения контрольных заданий обучающийся использует компьютер.

6. Методические материалы по освоению дисциплины

Получение углубленных знаний по изучаемой дисциплине достигается за счет дополнительных часов к аудиторной работе самостоятельной работы студентов. Выделяемые часы целесообразно использовать для знакомства с дополнительной научной литературой по проблематике дисциплины, анализа научных концепций и современных подходов к осмыслению рассматриваемых проблем. К самостоятельному виду работы студентов относится работа в библиотеках, в электронных поисковых системах и т.п. по сбору материалов, необходимых для проведения практических занятий или выполнения конкретных заданий преподавателя по изучаемым темам. Студенты могут установить диалог с преподавателем, получать консультации по выполнению заданий. В качестве оценочных средств на протяжении семестра используются тестовые и иные задания.

Обучение по дисциплине «Информационная безопасность информационных систем и сетей» предполагает изучение курса на аудиторных занятиях (лекции, практические занятия) и самостоятельную работу студентов. Практические занятия дисциплины предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения студент должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

– знакомит с новым учебным материалом;
– разъясняет учебные элементы, трудные для понимания;
– систематизирует учебный материал;
– ориентирует в учебном процессе.

Работа обучающегося на лекции:

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся.

Подготовка к практическим занятиям:

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения

обязательной и дополнительной литературы, рекомендованную к данной теме. практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенных методических указаний. Выполняемые практические задания становятся основой для выполнения курсового проекта по дисциплине Б1.В.01.06 «Геоинформационные системы».

Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Устный опрос.

2. Обсуждение теоретических вопросов, определенных программой дисциплины.

3. Выполнение практических заданий с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома.

4. Подведение итогов занятия.

Работа с литературными источниками:

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1 Промежуточная аттестация проводится в форме *экзамена* в шестом семестре.

6.2 Типовые оценочные материалы промежуточной аттестации.

РАЗДЕЛ 1. ТЕХНОЛОГИИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИБ

Тема 1.1 Основные понятия ИБ. ИБ в системе национальной безопасности России. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба

Экзаменационные вопросы

1. Охарактеризовать информационную войну как угрозу информационной безопасности национального уровня на основе Доктрины информационной безопасности РФ
2. Объекты и субъекты информационного пространства. Привести примеры.
3. Субъекты информационных отношений и их интересы.

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Достаточно надежное закрытие информации» с ключем «Алгоритм» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования.

Тема 1.2. Угрозы информационной безопасности. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Экзаменационные вопросы

4. Три уровня управления политикой безопасности на предприятии.
5. Варианты построения виртуальных защищенных каналов.
6. Понятие «модели злоумышленника». Привести примеры.
7. Конфиденциальность информации. Способы обеспечения конфиденциальности информации в организации.

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Сообщение: Чу, я слышу пушек гром!» методом Цезаря со сдвигом, равным 10. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 1.3. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Экзаменационные вопросы

8. Практические методы аутентификации, используемые в настоящее время
9. Классификация каналов проникновения в систему и утечки информации
10. Политика информационной безопасности организации.
11. Содержание политики безопасности организации.
12. Определение информационной безопасности и ее составляющие.

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Достигнута высокая скорость шифрования» с ключем «Обращение» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 1.4 Технологии защиты от вредоносных программ и спама. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность

Экзаменационные вопросы

13. Причины роста компьютерной преступности. Компьютерные преступления против государственных и общественных интересов.
14. Ключевые категории (понятия) безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.
15. Классификация вредоносных программ.
16. Сигнатурные методы обнаружения вредоносного ПО.
17. Проактивные методы обнаружения вредоносного ПО.
18. Тенденции развития современных антивирусных программ
19. Модули и режимы работы современных антивирусных программ.
20. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
21. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
22. Модель нарушителя антивирусной безопасности. Рекомендуемые

методы защиты для классов нарушителей.

Экзаменационное практическое задание:
Зашифруйте и расшифруйте сообщение «Теоретически нераскрываемый шифр» с ключем «Богемия» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

РАЗДЕЛ 2. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1. Основные принципы и методы в области технической защиты информации

Экзаменационные вопросы

23. Методика создания демилитаризованных зон в корпоративной сети предприятия
24. Защита информации от утечки по электромагнитным каналам
25. Технические каналы утечки информации. Защита от утечек информации по техническим каналам
26. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
27. Технология обеспечения безопасности ИС при беспроводном соединении
28. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.

Экзаменационное практическое задание:
Зашифруйте и расшифруйте сообщение «Сообщение: Чу, я слышу пушек гром!» методом Цезаря со сдвигом, равным 9. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 2.2. Противодействие несанкционированному доступу к конфиденциальной информации. Социальная инженерия

Экзаменационные вопросы

29. Система обнаружения и предотвращения вторжений.
30. Технологии обеспечения безопасности в ОС Windows 7.
31. Способы защиты информации в организации. Характеристика защитных действий
32. Защита информации от утечки по визуально оптическим каналам.
33. Способы защиты информации в организации. Характеристика защитных действий

34. Направления обеспечения ИБ предприятия. Правовая и организационная защита.

35. Технология обеспечения безопасности ИС при беспроводном соединении

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Проблемы реализации методов защиты» с ключем «Диалог» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 2.3. Классификация криптографических методов защиты. Симметричные криптографические алгоритмы

Экзаменационные вопросы

36. Термины и определения криптографии.

37. Классификация криптографических алгоритмов

38. Симметричные алгоритмы шифрования. Примеры

39. Криптографический алгоритм Цезаря. Преимущества и недостатки.

40. Криптографический алгоритм Виженера. Преимущества и недостатки.

41. Технологии биометрической аутентификации пользователя.

42. Преимущества и недостатки симметричных алгоритмов шифрования

43. Порядок использования систем с симметричными ключами.

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «В этом устройстве применен алгоритм шифрования» с ключем «Конфидент» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования.

Тема 2.4. Асимметричные криптографические алгоритмы

Экзаменационные вопросы

44. Преимущества и недостатки асимметричных систем шифрования.

45. Порядок использования систем с асимметричными ключами

46. Охарактеризовать методы социальной инженерии и технологию борьбы с ними

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Сообщение: «Чу, я слышу

пушек гром!» методом Цезаря со сдвигом, равным 4. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования.

Тема 2.5. Цифровая электронная подпись (ЭЦП). Технологии аутентификации

Экзаменационные вопросы

47. Технологии строгой аутентификации пользователя.
48. Технология использование электронной цифровой подписи.
49. Классификация механизмов аутентификации пользователей

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Потенциальная возможность нарушения режима» с ключем «Угроза» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИС И СЕТЕЙ

Тема 3.1 Проблемы информационной безопасности сетей

Экзаменационные вопросы

50. Сформулируйте, что собой представляют телекоммуникационная сеть
51. Проблемы безопасности IP-сетей
52. Объясните, чем принципиально отличаются сети с коммутацией каналов от сетей с коммутацией сообщений. Приведите примеры
53. Опишите, какие функции выполняет маршрутизатор
54. Структура и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности.

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Перекрытие каналов утечки» с ключем «Процедура» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 3.2. Угрозы и уязвимости проводных корпоративных сетей

Экзаменационные вопросы

55. Структура и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности.

56. Распространенные виды сетевых атак и способы защиты от них.

57. Угрозы и уязвимости проводных корпоративных сетей.

58. Опишите процесс инкапсуляция данных и ту роль, которую он выполняет в стеке TCP/IP.

59. Сформулируйте проблемы безопасности IP-сетей

60. Сформулируйте неоспоримые преимущества стека протоколов TCP/IP

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Потенциальная возможность нарушения режима» с ключем «Угроза» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования.

Тема 3.3. Технология защиты межсетевого обмена данными. Брандмауэры.

Экзаменационные вопросы

61. Разъясните функции, которые выполняет брандмауэр

62. Опишите основные схемы сетевой защиты на базе межсетевых экранов

63. Сформулируйте функциональные требования и опишите компоненты межсетевых экранов

64. Объясните преимущества шлюзов прикладного уровня по сравнению с фильтрующими маршрутизаторами

65. Опишите угрозы и уязвимости проводных корпоративных сетей

66. Сформулируйте и опишите достоинства и недостатки брандмауэра Windows

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Сообщение: Чу, я слышу пушек гром!» методом Цезаря со сдвигом, равным 15. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 3.4 Технологии VPN

Экзаменационные вопросы

67. Сформулируйте, что такое виртуальная защищенная сеть и туннель VPN.

68. Опишите, на каких технологиях основана защита информации в процессе ее передачи по туннелю VPN?

69. Приведите описание таким категориям, как VPN-клиент, VPN-сервер и шлюз безопасности VPN

70. Разъясните, как реализуется технология туннелирования

71. Сформулируйте, как технология туннелирования решает проблему защиты конфиденциальности, целостности и аутентичности передаваемой информации

72. Разъясните, какие протоколы играют роль протокола-«пассажира», несущего протокола и протокола туннелирования в технологии VPN

73. Разъясните, каковы варианты построения виртуальных защищенных каналов при использовании VPN

74. Объясните, почему вариант, при котором конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений, с точки зрения обеспечения информационной безопасности является лучшим?

75. Разъясните, с помощью каких компонент в узлах защищенного соединения сети VPN создается туннель

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «В этом устройстве применен алгоритм шифрования» с ключем «Криптоанализ» методом Виженера. Для этой цели составьте алгоритм и программу на Excel, Visual Basic или C++.

Тема 3.5 ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP

Экзаменационные вопросы

76. Объясните, какие уровни модели OSI соответствуют прикладному уровню стека протоколов TCP/IP и какие протоколы на нем функционируют

77. Объясните, какие уровни модели OSI соответствуют транспортному уровню стека протоколов TCP/IP и какие протоколы на нем функционируют

78. Объясните, какие уровни модели OSI соответствуют уровню межсетевого взаимодействия стека протоколов TCP/IP и какие протоколы на нем функционируют

79. Объясните, какие уровни модели OSI соответствуют уровню сетевого интерфейса стека протоколов TCP/IP и какие протоколы на нем функционируют

80. Разъясните, в чем заключается основной недостаток стека протоколов TCP/IP

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Такая замена равносильна введению ключа» с ключем «Случайно» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

РАЗДЕЛ 4. ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА УРОВНЯХ МОДЕЛИ OSI

Тема 4.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне

Экзаменационные вопросы

81. Разъясните, в чем заключается назначение средств VPN, которые используются на канальном и сеансовом уровне
82. Опишите, какие протоколы используются на канальном и сеансовом уровне, для формирования защищенных каналов в сети VPN
83. Сформулируйте, какие функции необходимо реализовывать протоколам на канальном и сеансовом уровне в сети VPN, для создания защищенного соединения
84. Опишите схему туннелирования при прямом подсоединении компьютера удаленного пользователя к Интернет
85. Сформулируйте и опишите функции протоколов канального уровня
86. Сформулируйте и опишите функции протоколов сеансового уровня

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Сообщение: Чу, я слышу пушек гром!» методом Цезаря со сдвигом, равным 10. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 4.2. Защита на сетевом уровне — протокол IPSec

Экзаменационные вопросы

87. Опишите для как создавался протокол IPSec и для каких целей это делалось.
88. Опишите для реализации каких функций используется стек протоколов IPSec. Можно ли считать его стеком протоколов и почему?
89. Опишите структуру IP-пакета и объясните какие задачи

обеспечения безопасности IP-пакетов он решает.

90. Сформулируйте преимущества средств безопасности IPSec

91. Опишите основные схемы применения IPSec

92. Опишите архитектуру стека протоколов IPSec и изобразите его в виде схемы

93. Опишите структуру заголовок протокола AH и назначение его полей

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Разделяют две разновидности гаммирования» с ключем «Качество» методом Виженера. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

Тема 4.3. Инфраструктура защиты на прикладном уровне

Экзаменационные вопросы

94. Сформулируйте, решение каких задач необходимо для обеспечение информационной безопасности организации на прикладном уровне

95. Объясните, какую систему управления доступом пользователей к информации необходимо организовать для обеспечения информационной безопасности организации на прикладном уровне

96. Разъясните, как осуществляется управление идентификацией и доступом на прикладном уровне на примере электронного бизнеса

97. Изобразите схематично в виде рисунка и опишите механизм функционирование системы управления доступом из глобальной сети к разрешенным для удаленных пользователей ресурсам в организации

98. Объясните, как в механизме удаленного доступа к ресурсам в организации используются такие инструменты, как Web-доступ, VPN-доступ или удаленный доступ с использованием серверов RADIUS

Экзаменационное практическое задание:

Зашифруйте и расшифруйте сообщение «Сообщение: Чу, я слышу пушек гром!» методом Цезаря со сдвигом, равным 7. Для этой цели составьте алгоритм и программу на C++, C#, Python или другом языке программирования

6.3. Критерии и шкала оценивания на основе БРС.

Соответствие государственной шкалы оценивания академической успеваемости и шкалы ECTS при дифференцированном зачете

Оценка по шкале ECTS	**Сумма баллов за все виды учебной деятельности**	**Оценка по государственной шкале**	**Определение**
A	90 – 100	«Отлично»	Отличное выполнение с незначительным количеством неточностей
B	80 – 89	«Хорошо»	в целом правильно выполненная работа с незначительным количеством ошибок (до 10%)
C	75 – 79		в целом правильно выполненная работа с незначительным количеством ошибок (до 15%)
D	70 – 74	«Удовлетворительно»	неплохо, но со значительным количеством недостатков
E	60 – 69		выполнение удовлетворяет минимальные критерии
FX	35 – 59	«Не удовлетворительно»	с возможностью повторной сдачи
F	0 – 34		с обязательным повторным изучением дисциплины (выставляется комиссией)

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий

Компьютер с операционной системой Windows, на котором установлена одной последних версий браузера Chrome или ЯндексБраузер.

7. Методические материалы по освоению дисциплины

Получение углубленных знаний по изучаемой дисциплине достигается за счет дополнительных часов к аудиторной работе самостоятельной работы студентов. Выделяемые часы целесообразно использовать для знакомства с дополнительной научной литературой по проблематике дисциплины, анализа научных концепций и современных подходов к осмыслению рассматриваемых проблем. К самостоятельному виду работы студентов относится работа в библиотеках, в электронных поисковых системах и т.п. по сбору материалов, необходимых для проведения практических занятий или выполнения конкретных заданий преподавателя по изучаемым темам. Студенты могут установить диалог с преподавателем, получать консультации по выполнению заданий. В качестве оценочных средств на протяжении семестра используются тестовые и иные задания.

Обучение по дисциплине «Технологии обеспечения информационной безопасности» предполагает изучение курса на аудиторных занятиях (лекции, практические занятия) и самостоятельную работу студентов. Практические занятия дисциплины предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения студент должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

– знакомит с новым учебным материалом;
– разъясняет учебные элементы, трудные для понимания;
– систематизирует учебный материал;
– ориентирует в учебном процессе.

Работа обучающегося на лекции:

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся.

Подготовка к практическим занятиям:

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенных методических указаний. Выполняемые практические задания становятся основой для выполнения курсового проекта по дисциплине Б1.В.01.06 «Технологии обеспечения информационной безопасности».

Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

10. Устный опрос.

11. Обсуждение теоретических вопросов, определенных программой дисциплины.

12. Выполнение практических заданий с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома.

13. Подведение итогов занятия.

Работа с литературными источниками:

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий

спектр мнений по изучаемой проблеме. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1 Основная литература

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.
2. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : МИСИС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/360344 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.
3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ИНФРА-М, 2026. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-16-021164-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2207574 (дата обращения: 12.06.2026). – Режим доступа: по подписке.
4. Михнев, И. П. Информационная безопасность : учебное пособие / И. П. Михнев. — Москва : Дело РАНХиГС, 2019. — 82 с. — ISBN 978-5-7786-0776-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/466877 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.
5. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 7-е изд., стер. — Санкт-Петербург : Лань, 2026. — 124 с. — ISBN 978-5-507-56325-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/515187 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.

8.2 Дополнительная литература

1. Киреева, Н. В. Методические рекомендации по выполнению лабораторных работ по дисциплине «Информационная безопасность инфокоммуникационных сетей и систем» : учебно-методическое пособие / Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2022. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/411743 (дата обращения: 12.06.2026). — Режим

доступа: для авториз. пользователей.

2. Беккалиева, Наталья Климентьевна. Информационная безопасность : практикум для студентов вузов / Н. К. Беккалиева ; Федеральное государственное бюджетное образовательное учреждение высшего образования Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Поволжский институт управления им. П. А. Столыпина. — Саратов : Поволжский ин-т упр. им. П. А. Столыпина - фил. РАНХиГС, 2019. — 97 с. : табл. : 21 см.; ISBN 978-5-8180-0573-7.

8.3 Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации. – Текст : электронный // Сайт Президента Российской Федерации. – URL: http://www.kremlin.ru/acts/constitution

8.4 Интернет-ресурсы

1. Информационно-правовой портал ГАРАНТ.РУ. – URL: https://www.garant.ru/
2. Научная электронная библиотека eLIBRARY.RU. – URL: https://elibrary.ru/
3. Научная электронная библиотека «КиберЛенинка». – URL: https://cyberleninka.ru
4. Электронно-библиотечная система «Лань». – URL: http://e.lanbook.com
5. Федеральный закон от 27 июля 2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/
6. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных». URL: https://www.consultant.ru/document/cons_doc_LAW_112701/
7. Федеральный закон от 26.07.2017 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_220885/
8. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_48699/
9. Федеральный закон от 6 апреля 2011 г.63-ФЗ «Об электронной подписи». URL: https://www.consultant.ru/document/cons_doc_LAW_112701/

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Материально-техническое обеспечение дисциплины включает в себя:

- лекционные аудитории, оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном;
- помещения для проведения семинарских и практических занятий, оборудованные учебной мебелью.

Дисциплина поддержана соответствующими программными продуктами с открытой лицензией: KeePass, VeraCrypt, 360 Total Sequrity, gpg4usb 0.3.3.-2, gpg4win 0.4.4, Whireshark.

Вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Помещения для самостоятельной работы обучающихся включают следующую оснащенность: столы аудиторные, стулья, доски аудиторные, компьютеры с подключением к локальной сети института (для компьютерных аудиторий) и Интернет. Для изучения учебной дисциплины используются автоматизированная библиотечная информационная система и электронные библиотечные системы.