МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
Информационных технологий
и математических методов в экономике

_____ И.Н. Щепина

18.04.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.23 Средства и методы защиты информации

1. **Код и наименование направления подготовки/специальности:**

38.05.01 Экономическая безопасность

2. **Профиль подготовки/специализация:**

Обеспечение экономической безопасности и финансовый мониторинг экономических систем

3. **Квалификация (степень) выпускника:** экономист

4. **Форма обучения:** заочная

5. **Кафедра, отвечающая за реализацию дисциплины:** Кафедра информационных технологий и математических методов в экономике

6. **Составители программы:**
Каляпина Ольга Ивановна, к.т.н., доцент

7. **Рекомендована:** НМС экономического факультета протокол №3 от 21.03.24 г.

8. **Учебный год:** 2025/2026 **Семестр(ы):** 5, 6

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

- получение теоретических знаний и практических навыков в области защиты информации в цифровой экономике;
- развитие информационной культуры и подготовки, необходимых для понимания принципов построения систем защиты информации;
- демонстрация возможностей применения основных категорий мер защиты информации с оценкой их сильных и слабых сторон.

Задачи учебной дисциплины:

- ознакомление с основными понятиями информационной безопасности в цифровой экономике;
- формирование навыков выбора методов и средств защиты информации, соответствующих требованиям защиты информации в конкретных информационных системах;
- формирование навыков оценки соответствия существующих решений в области защиты информации конкретным требованиям;
- формирование навыков разработки предложений по совершенствованию системы обеспечения информационной безопасности в цифровой экономике.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Средства и методы защиты информации» входит в часть учебного плана, формируемую участниками образовательных отношений блока Б1, базовая. Для освоения дисциплины необходимы знания, умения и компетенции, сформированные в результате изучения студентами дисциплин базовой части математического и естественнонаучного цикла. Дисциплина связана с дисциплиной Информационные системы в экономике.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.1	Демонстрирует знание информационных технологий и программных средств, в том числе отечественного производства, применяемых организациями при решении профессиональных задач	Знать: – основы и базовые требования информационной безопасности; – нормативные правовые акты в области защиты информации; – основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности; – основные тенденции и направления формирования и функционирования комплексной системы защиты информации в различных типах предпринимательских структур Уметь: – работать с нормативными документами – использовать средства защиты информации и информационной безопасности Владеть: – навыками разработки нормативных

				документов, регламентирующими защиту государственной и коммерческой тайны и иной служебной информации в организации; – навыками выбора методов и средств защиты информации, соответствующих требованиям защиты информации в конкретных информационных системах.
		ОПК-6.2	Выбирает и применяет современные информационные технологии и программные средства при решении профессиональных задач	Знать: – цель и задачи создания, внедрения и эффективного использования информационных технологий в экономике; – основные виды информационных технологий, области применения информационных технологий в экономике. Уметь: – использовать для решения аналитических и исследовательских задач современные информационные системы и информационные технологии; – применять программные средства обеспечения безопасности данных на автономном ПК и в интерактивной среде. Владеть: – технологией работы с современными программными средствами обработки экономической информации табличного характера, средствами графической интерпретации экономической информации; – информационными технологиями формирования, обработки и представления данных в информационных системах; – методическими основами проектирования автоматизированных информационных систем.
ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1	Знает и понимает принципы работы и возможности современных информационных технологий, предназначенных для решения задач профессиональной деятельности	Знать: – принципы реализации информационных процессов, основные характеристики универсальных информационных технологий ввода, преобразования, переработки, передачи и представления экономической информации; – основные понятия теории защиты информации, основные средства и методы защиты информации в информационных системах. Уметь: – выполнять поиск и обработку экономической информации средствами офисных приложений; – представлять, преобразовывать и анализировать данные экономического характера в табличном и графическом виде. Владеть:

				– навыками работы для эффективного использования возможностей компьютерных сетей; – технологиями использования возможностей справочно-правовых систем; инфокоммуникационными технологиями в экономических информационных системах.

12. Объем дисциплины в зачетных единицах/час. (*в соответствии с учебным планом)* — 3/108.

Форма промежуточной аттестации *(зачет/экзамен)***:** экзамен

13. Трудоемкость по видам учебной работы:

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			Зимняя сессия 5 семестр	Летняя сессия 6 семестр
Аудиторные занятия				
в том числе:	лекции	6	4	2
	практические	6	4	2
	лабораторные	-	-	-
Самостоятельная работа		87	28	59
Контрольная работа		-	-	-
Форма промежуточной аттестации (экзамен)		9	-	9
Итого:		108	36	72

13.1. Содержание дисциплины:

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
	1. Лекции		
1.1	Основы информационной безопасности. Основные понятия и определения. Меры обеспечения защиты информации	Понятие информации. Доступ к информации. Информационные системы. Организация защиты информации. Организационные меры защиты информации. Законодательные меры защиты информации. Административные меры защиты информации. Организационно-технические меры защиты информации.	
1.2	Обзор криптографических методов защиты информации	Понятие шифра. Шифр простой замены и его анализ. Шифры перестановки и их анализ. Варианты усложнения шифра простой замены. Шифр многоалфавитной замены и его анализ.	
1.3	Техническая защита информации	Основные понятия технической защиты информации. Технические каналы утечки информации. Акустический канал утечки информации. Оптический канал утечки информации. Радиоэлектронный канал утечки информации.	
1.4	Программно-технические мерызащиты информации	Сервисы безопасности. Антивирусная защита. Типы вредоносных программ. Принципы обнаружения вредоносных программ. Выбор антивирусных средств. Межсетевое экранирование.	
	2. Практические занятия		
2.1	Основы информационной безопасности. Основные понятия и определения	Обработка информации. Защита информации. Информационная безопасность. Социальная инженерия Определение IP- и MAC- адреса в Windows Настройка Защитника (Defender) Windows	https://edu.vsu.ru/mod/assign/view.php?id=1264136 https://edu.vsu.ru/mod/assign/view.php?id=1264142
2.2	Организационные меры защитыинформации Программно-технические мерызащиты информации	Организационно-технические меры защиты информации: физическая защита объекта информатизации, защита поддерживающей инфраструктуры. Определение актуальных угроз безопасности по методике ФСТЭК России. Инструменты определения уязвимостей	https://edu.vsu.ru/mod/assign/view.php?id=1269805

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основы информационной безопасности. Основные понятия и определения. Меры обеспечения защиты информации	2	2	-	12	16
2	Организационные меры защиты информации			-	10	10
3	Методы контроля и разграничения доступа		2	-	10	12
4	Обзор криптографических методов защиты информации	2		-	12	14

5	Криптографические методы защиты информации			-	12	12
6	Стеганографическая защита информации			-	10	10
7	Техническая защита информации	-		-	11	11
8	Программно- технические меры защиты информации	2	2	-	10	14
9	Экзамен			-		9
	Итого:	6	6	-	87	108

14. Методические указания для обучающихся по освоению дисциплины:

(рекомендации обучающимся по освоению дисциплины: указание наиболее сложных разделов, работа с конспектами лекций, презентационным материалом, рекомендации по выполнению курсовой работы, по организации самостоятельной работы по дисциплине и др.)

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, практические занятия, а также различные виды самостоятельной работы обучающихся.

В процессе лекций обучающимся рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к текущей и промежуточной аттестации.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы формулируются кратко и лаконично, их целесообразно записывать. В конце лекции обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

В ходе подготовки к практическим занятиям обучающемуся рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях.

Прежде чем приступать к выполнению практических заданий, обучающемуся необходимо ознакомитьсяс соответствующими разделами программы дисциплины по учебной литературе, рекомендованной программой курса; получить от преподавателя информацию о порядке выполнения заданий, критериях оценки результатов работы; получить от преподавателя конкретное задание и информацию о сроках выполнения, о требованиях к оформлению и форме представления результатов.

При выполнении практических заданий необходимо привести развёрнутые пояснения хода решения и проанализировать полученные результаты. При необходимости обучающиеся имеют возможность задать вопросы преподавателю по трудностям, возникшим при решении задач.

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем и вопросов учебной дисциплины. Самостоятельная работа является обязательной для каждого обучающегося. При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Рекомендованные методические материалы, задания к лабораторным работам, исходные данные для моделирования размещаются на странице курса «Средства и методы защиты информации 2 поток» на портале «Электронный университет ВГУ» https://edu.vsu.ru/course/view.php?id=29638 автор Каляпина О.И.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник

1	Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник : [16+] / Б. И. Филиппов, О. Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. – URL:https://biblioclub.ru/index.php?page=book&id=499170
2	Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков,С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. – URL: https://biblioclub.ru/index.php?page=book&id=562348

б) дополнительная литература:

№ п/п	Источник
3	Шилов, А. К. Управление информационной безопасностью : учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. — URL: https://biblioclub.ru/index.php?page=book&id=500065
4	Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485
5	Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084
6	Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. – URL: https://biblioclub.ru/index.php?page=book&id=574729

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
7	http://edu.vsu.ru/
8	http://www.lib.vsu.ru
9	http://biblioclub.ru
10	http://www.e-library.ru
11	http://www.ibooks.ru
12	Электронный университет ВГУ» LMS Moodle, https://edu.vsu.ru/

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных), курсовых работ и др.)

№ п/п	Источник
1	МУДЛ (Портал «Электронный университет ВГУ» – Moodle: URL: https://edu.vsu.ru/course/view.php?id=29638
2	Моргунов, А. В. Информационная безопасность: учебно-методическое пособие: [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с. – URL: https://biblioclub.ru/index.php?page=book&id=576726
3	Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем : учебное пособие : [16+] / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. — Москва : Прометей, 2018. — 173 с. — URL: https://biblioclub.ru/index.php?page=book&id=494850

17. Образовательные технологии, используемые для реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение): реализация учебной дисциплины предполагает применение дистанционных образовательных технологий (работу на образовательном портале «Электронный университет ВГУ»).

Дисциплина реализуется с элементами электронного обучения и дистанционных образовательных технологий в рамках электронного курса (ЭК) Средства и методы защиты информации, размещенного на портале «Электронный университет ВГУ» (https://edu.vsu.ru/course/view.php?id=29638). ЭК включает учебные материалы для самостоятельной работы обучающихся, а также обеспечивает возможность проведения контактных часов/аудиторных занятий в режиме онлайн.

Программа дисциплины реализуется с применением дистанционных образовательных технологий.

Для организации занятий требуется:

-персональный компьютер и видеопроекционное оборудование;

-программное обеспечение общего назначения Microsoft Office;

-специализированное программное обеспечение при изучении дисциплины не используется.

18. Материально-техническое обеспечение дисциплины:

— учебная аудитория: специализированная мебель, ноутбук, проектор, экран для проектора;
— помещение для самостоятельной работы: специализированная мебель, компьютеры с возможностью подключения к сети "Интернет";
— программное обеспечение OS Ubuntu, Okular, Mozilla Firefox, LibreOffice, WPS Office, Microsoft Office, RStudio, Gretl, Консультант+.

19. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Темы 1-3	ОПК-6	ОПК–6.1, ОПК–6.2	Задания для практических занятий 1-6
2.	Темы 4-8	ОПК-7	ОПК–7.1	Задания для практических занятий 7-17

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: выполнением заданий на практических занятиях.

Текущие аттестации проводятся в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета.

Перечень заданий для практических занятий

Практическое занятие № 1 *Подключение* сетевого оборудования

1. Изучите классификацию сетевых кабелей.
2. Произведите обжим сетевого кабеля типа «витая пара».

Практическое занятие № 2 Компьютерные сети. Адресация в сети.

Задача № 1

Определите номер узла в IP-адресе 200.77.125.68 если известно, что адрес относится к одному из трех классов – A, B или C.

1) 200.77.125.68 2) 77.125.68 3) 125.68 4) 68

Задача № 2

Определите адрес сети в IP-адресе 192.89.51.188 если известно, что адрес относится к одному из трех классов – A, B или C.

1) 192.89.51.188 2) 192.89.51.0 3) 192.89.0.0 4) 192.0.0.0

Задача № 3

Укажите какие значения из представленных в таблице не могут быть маской подсети. Запишите последовательно их номера, например, 134

1	255.255.252.0
2	255.255.230.0
3	255.255.255.128
4	255.255.255.240

Задача № 4

Заданы маска подсети 255.255.255.224 и IP-адрес компьютера в сети 192.168.250.152. Порядковый номер компьютера в сети равен _____

Задача № 5

Задана маска подсети 255.255.255.224. Максимально возможное количество узлов в сети равно _____

Практическое занятие № 3 Адресация в сетях TCP/IP

1. Структура MAC-адреса
2. Отображение символьных адресов на IP-адреса: служба DNS
3. Автоматизация назначения IP-адресов узлам сети - протокол DHCP

Практическое занятие № 4 Определение IP- и MAC-адреса в Windows

1. Панель управления - Сеть и Интернет - Центр управления сетями и общим доступом - Просмотр сетевых компьютеров и устройств

В появившемся списке в группе устройств Сетевая Инфраструктура изучите контекстное меню Свойства – вкладка Сетевое Устройство. Выпишите в тетрадь MAC-адрес и IP-адрес устройства

2. Панель управления - Сеть и Интернет - Центр управления сетями и общим доступом - Просмотр состояния сети и задач

Изучите информацию, представленную в этом окне. Сделайте скриншот архитектуры Вашей домашней сети.

3. В правом нижнем углу в Панели Задач щелкните по ярлыку Сети и изучите доступные подключения, Текущее Подключение, протокол его работы. Сделайте скриншот этого окна.

4. Панель управления - Сеть и Интернет – Свойства Браузера

Сделайте скриншот окна Свойства: Интернет и изучите вкладки в этом окне

5. Выполните команды ipconfig /all и tracert google.com на домашнем компьютере и проанализируйте ответ

Практическое занятие № 5 Знакомство с функциями "Безопасности Windows" и их настройка

Выполните эти команды на домашнем ПК и проанализируйте ответ

1. Пуск – Панель управления – Система и Безопасность Windows 10 – Windows Defender Защитник

2. Пуск – Панель управления – Система и Безопасность – Брандмауер Windows

Практическое занятие № 6 Инструменты определения уязвимостей

1. Скачайте на домашний ПК с сайта ФСТЭК России программу ScanOval
2. Запустите ScanOval и скачайте к ней обновленную БД.
3. Обратите внимание, что ScanOval загрузит уязвимости, их можно смотреть по одной или все вместе.
4. Для того, чтобы проверить, какие уязвимости не закрыты в системе, необходимо нажать кнопку «Выполнить аудит».
5. Ограничить права доступа работников. Выберите некоторый файл, из контекстного меню выберите команду Свойства, вкладка Безопасность. Можно Удалить/Добавить пользователей этого файла. В нижнем окне задать права доступа для каждого пользователя, например, Чтение и т.п. Т.е. только читать файл, но не изменять его
6. Ограничьте доступ к различным программным продуктам – разрешите доступ к 2-3 продуктам, а к остальным запретите.
7. Проверьте состояние встроенной антивирусной системы. Проверьте, какие есть угрозы, какие вирусы обнаружены и как на них отреагировала система, непосредственно следите за обновлениями.

Практическое занятие № 7 Синтаксис языка программирования Python

Практическое занятие № 8 Библиотека NumPy

Практическое занятие № 9 Вычисление логических выражений

Практическое занятие № 10 Программирование операций обработки строк

Практическое занятие № 11 Программирование пользовательских функций

Практическое занятие № 12 Библиотека Pandas. Программирование операций с датафреймами

Практическое занятие № 13 Программирование функций анализа данных на Pandas

Практическое занятие № 14 Визуализация графиков, диаграммы рассеяния и двумерной гистограммы с помощью библиотеки Matplotlib

Практическое занятие № 15 Визуализация тенденции ряда (из датафрейма) с помощью библиотеки Matplotlib

Практическое занятие № 16 Шифрование и криптография в Python. Генерация случайного пароля

Практическое занятие № 17 Программа хэширования пароля с использованием библиотеки Cryptography

20.2. Промежуточная аттестация

Для оценивания результатов обучения на экзамене используются следующие показатели:

- владение понятийным аппаратом и теоретическими основами дисциплины;
- способность иллюстрировать ответ примерами практического использования теоретического материала;
- способность связать вопросы теории с практическими заданиями, применять теоретические знания для решения практических задач;
- ориентация в функциональных возможностях изучаемых программных продуктах;
- грамотная, уверенная, связанная речь при устном ответе;
- способность быстро ориентироваться в материале, отвечая на дополнительные вопросы в рамках изучаемого объема.

Для оценивания результатов обучения на экзамене используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом и теоретическими основами дисциплины, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач в области информационной безопасности.	Повышенный уровень	Отлично
Обучающийся владеет теоретическими основами дисциплины, способен применять теоретические знания для решения практических задач в области информационной безопасности, допускает незначительные ошибки в ответах на дополнительные вопросы	Базовый уровень	Хорошо
Обучающийся частично владеет теоретическими основами дисциплины, допускает незначительные ошибки при решении практиче1ских заданий, дает неполные ответы на дополнительные вопросы	Пороговый уровень	Удовлетворительно
Обучающийся демонстрирует отрывочные, фрагментарные знания, теоретических основ дисциплины, допускает грубые ошибки при решении практических заданий, затрудняется ответить на дополнительные вопросы.	–	Неудовлетворительно

20.3 Перечень вопросов к экзамену:

1. Понятие ИБ. Соотношение ИБ и кибербезопасности. Безопасность в экономической сфере. Понятия угрозы и уязвимости.
2. Доктрина ИБ РФ. Основные информационные угрозы и состояние ИБ
3. Доктрина ИБ РФ. Стратегические цели и основные направления обеспечения ИБ.
4. Доктрина ИБ РФ. Основные направления обеспечения ИБ в экономической сфере
5. Связь ЗИ и экономической безопасности
6. Методы ЗИ – краткая характеристика и взаимосвязь всех методов.
7. Организационно-правовая защита – как метод ЗИ
8. Программная ЗИ
9. Контроль доступа – идентификация, аутентификация и авторизация
10. Основные принципы и методы идентификации и аутентификации
11. Техническая и физическая ЗИ
12. Криптографическая ЗИ
13. Информация как объект защиты. Понятие информации. Классификация информации по степени конфиденциальности
14. Классификация информации, подлежащей защите в соответствии с законодательством РФ
15. Понятия персональных данных и коммерческой тайны

16. Телекоммуникационные сети как объект защиты. Структура эталонной сетевой модели OSI/ISO
17. Сетевая модель TCP/IP. Понятие протокола и стека протоколов
18. Инкапсуляция и декапсуляция при передаче данных в сети, способы обеспечения целостности данных, передаваемых в сети
19. Виды сетевого оборудования, назначение и характеристики
20. Активное и пассивное сетевое оборудование – связь с ИБ
21. Классификация сетевых кабелей. Основные шаги процедуры обжима «витой пары»
22. Компьютерные сети. Адресация в IP-сетях – классовая и бесклассовая адресация. Маска подсети
23. MAC-адрес: формат, структура, назначение
24. Отображение символьных адресов на IP-адреса: служба DNS
25. Автоматизация назначения IP-адресов узлам сети: протокол DHCP
26. Определение IP- и MAC-адреса в Windows. Просмотр состояния сети и задач
27. Настройка «Защитника Windows» (Defender). Использование межсетевого экрана для закрытия уязвимостей системы
28. Инструменты аналитика ИБ. Сетевые инструменты сбора информации – Nmap, Scapy и Shodan
29. Локальный анализ ИБ. Настройка операционной системы и ее компонентов
30. Инструменты определения уязвимостей. Методы закрытия уязвимостей.
31. Аудит ИБ: сущность, этапы и реализация
32. Аудит ИБ программой ScanOval. База данных угроз и уязвимостей ФСТЭК России
33. Системы обнаружения и предотвращения вторжений IDS/IPS
34. Межсетевой экран следующего поколения: NGFW
35. Типы IDS/IPS-систем: NIPS, HIPS, WIPS, NBA
36. Методы обнаружения и предотвращения вторжений IDS/IPS-систем
37. Классификация IT-инцидентов.
38. Типы параметров мониторинга состояния серверов и сетевого оборудования
39. Типы параметров мониторинга трафика в сети
40. Типы параметров мониторинга безопасности сети
41. Средства криптографической ЗИ. Виды СКЗИ
42. Симметричное шифрование, асимметричное шифрование, гибридное шифрование. Хеш-функции.
43. Криптография в блокчейне. Электронная подпись
44. Перестановочные шифры. Пример
45. Требования к выбору надежного пароля для обеспечения безопасности аккаунта
46. Средства антивирусной защиты информации
47. Стеганографическая ЗИ: принцип действия. Виды стеганографии
48. Стеганография и NFT-технологии
49. Применение стеганографии для осуществления кибератак

20.3.2 Перечень практических заданий

1. Используя шифр Виженера, зашифруйте сообщение "Несмотря на широкую распространённость, категория и нформации остаётся одной из самых дискуссионных в науке." В качестве ключа используйте слово "кино".

2. Используя шифр Виженера, зашифруйте сообщение "Несмотря на широкую распространённость, понятие информации остаётся одним из самых дискуссионных в науке." В качестве ключа используйте слово "защита".

3. Используя алфавит "l" "e" "k" "f" "v" "j" "p" "d" "t" "s" "c" "r" "h" "u" "x" "n" "y" "z" "a" "g" "q" "o" "i" "m" "w" "b", зашифруйте сообщение "Unus pro omnibus, omnes pro uno!" шифром Виженера. Ключ: "ave".

4. Используя алфавит "x" "r" "y" "k" "s" "d" "m" "f" "i" "a" "c" "q" "n" "e" "g" "l" "p" "t" "w" "j" "v" "o" "u" "h" "z" "b", зашифруйте сообщение "Unus pro omnibus, omnes pro uno!" шифром Виженера. Ключ: "ave".

20.4 Тестовые задания

Перечень заданий для проверки сформированности компетенций ОПК-6, ОПК-7:

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
   - разработка аппаратных средств обеспечения правовых данных
   - разработка и конкретизация правовых нормативных актов обеспечения безопасности
   - разработка и установка во всех компьютерных правовых сетях журналов учета действий

2. Основными рисками информационной безопасности являются:
   — техническое вмешательство, выведение из строя оборудования сети
   — потеря, искажение, утечка информации
   — искажение, уменьшение объема, перекодировка информации

3. Конфиденциальностью называется:
   — описание процедур
   — защита от несанкционированного доступа к информации
   — защита программ и программных комплексов, обеспечивающих технологию разработки, отладки ивнедрения создаваемых программных продуктов

4. В каком документе отражено понятие автоматизированной системы
   — Федеральный закон № 149-ФЗ
   — ГОСТ Р 34.003-90
   — ГОСТ 51275-2006

5. Согласно 149-ФЗ «Об информации, информационных технологиях и о защите информации», *информация* определяется как:
   — вся совокупность сведений об окружающем нас мире, о всевозможных протекающих в нем процессах, которые могут быть восприняты живыми организмами, электронными машинами и другими информационными системами.
   — совокупность сведений, подлежащих хранению, передаче, обработке и использованию в человеческой деятельности.
   — все то, чем могут быть дополнены наши знания и предположения.
   — сведения независимо от формы их представления

6. Криптографические методы ЗИ могут быть не эффективны для:
   — Внутренних нарушителей, имеющих физический доступ к носителям информации
   — Нарушителя, использующего средства несанкционированного получения информации, обрабатываемой техническими средствами в открытом виде
   — Внешнего нарушителя, вступающего в сговор с легальными пользователями

7. Укажите уровни защиты информации:
   — Административный
   — Законодательный
   — Индустриальный
   — Промышленный

8. Криптографические методы ЗИ эффективны для:
   — Нарушителей, способных осуществить сетевую атаку на ИС и получить доступ к конкретным информационным объектам
   — Нарушителей, обладающих значительными вычислительными ресурсами
   — Угроз утечки речевой и видовой информации по техническим каналам
   — Нарушителя, использующего халатность или ошибки легальных пользователей
9. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры понимается под ...
   — Информационной безопасностью
   — Целостностью информации
   — Конфиденциальностью информации
   — Доступностью и гибкостью информации

10. К организационным мерам защиты информации НЕ относится:
    — Законодательные меры ЗИ
    — Криптографические методы ЗИ
    — Административные меры ЗИ

11. 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:
    — Обеспечении распространения информации
    — Осуществлении права на поиск, получение, передачу и распространение информации

— Обеспечении уничтожения информации
— Обеспечении защиты информации

12. Что не относится к свойствам информационной безопасности:
— целостность
— закрытость
— конфиденциальность
— доступность

13. К программно-техническим средствам защиты информации НЕ относится:
— Организационно-технические меры ЗИ
— Стеганографические методы ЗИ
— Методы и средства технической ЗИ

14. Установите правильный порядок процедур обеспечения информационной безопасности, выполнение которых обеспечивают системы управления доступом:
О Аутентификация
О Отчетность
О Авторизация
О Идентификация

15. К какому типу методов обеспечения информационной безопасности относится «разработка и конкретизация правовых нормативных актов обеспечения безопасности»? _____ (К правовым методам)

16. Что относится к средствам перехвата передаваемых по Сети данных?
О **анализаторы протоколов**
О **трояны**
О **снифферы**
О уволенные и недовольные сотрудники
Укажите не менее двух вариантов ответа

17. Какие принципы планирования относятся к модели планировщика операционной системы «первый вошел - первый обслужен»?
О Используется механизм не вытесняющей многозадачности
О Используется механизм вытесняющей многозадачности
+ О Все задачи стоят в очереди, независимо от времени отработки программы
О Процесс, поступивший первым, ждет в очереди по количеству отработок
+ О Процесс, поступивший первым, выполняется до его завершения
О Если задача с большим временем выполнения, она передвигается после наиболее короткой

18. Сеть, в которой объединены компьютеры в различных странах на различных континентах – это _____ сеть.
О региональная
О персональная
О локальная
О **глобальная**

19. Дан адрес файла: D:\TABLE\DESK\kot.doc . Укажите имя файла (без расширения). (**kot**)

20. По заданному IP-адресу узла 217.19.128.131 и маске 255.255.192.0 определите IP-адрес сети _____

21. Сколько секунд потребуется модему, передающему сообщения со скоростью 28800 бит/с, чтобы передать цветное растровое изображение размером 800*600 пикселей, при условии, что в палитре 8 цветов? ____**50**_____

22. Для передачи информации в интернете используют пакеты. Каждый компьютер в Сети обрабатывает не отдельный файл, а фрагмент информации. Если один узел окажется недоступен, то поток информации не уйдет в никуда и будет передан дальше. Какая технология отвечает за бесперебойную передачу пакетов? __**TCP/IP**_____

23. Для решения какой задачи может быть использована технология «блокчейн»?
(Укажите не менее двух вариантов ответа)
О **запись данных о происхождении и перемещении**
О **управление идентификацией**
О прогнозирование вероятности банкротства компании
О **ускорение проведения трансграничных денежных переводов**

24. Сколько секунд потребуется модему, передающему информацию со скоростью 32000 бит/с, чтобы передать 16-цветное растровое изображение размером 800*600 пикселей, при условии что в одном байте

закодировано максимально возможное целое число пикселей? ___**240 с**____

25. На какие виды делят современные цифровые технологии, применяемые по типу пользовательского интерфейса?
(Укажите не менее двух вариантов ответа)
- О **автоматизированные**
- О **диалоговые**
- О распределенные
- О **пакетные (автоматические)**

26. _____ доступ заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. **Несанкционированный**

27. Как называется указанная структура адреса?
https://en.wikipedia.org/wiki/Uniform_resourse_locator

URL - это стандартизированный способ указания адреса ресурса в Интернете

28. Какие обозначенные элементы относятся к основным классам операционных систем?
(Укажите не менее двух вариантов ответа)
- О **однопользовательские однозадачные**
- О распределенные однозадачные
- О **однопользовательские многозадачные**
- О многопользовательские сплоченные
- О **многопользовательские многозадачные**

29. Соотнесите типы и источники возникновения информационных угроз в условиях применения информационных технологий для решения задач профессиональной деятельности:
1. раскрытие данных – это…
2. раскрытие трафика локальных вычислительных сетей – это …
3. подмена трафика локальных вычислительных сетей – это…

2 О произойдет в результате доступа к информации или ее чтения человеком и возможного ее разглашения случайным или намеренным образом, тогда, когда информация передается через локальные вычислительные сети
3 О использование легальным способом, когда появляются сообщения, имеющие такой вид, будто они посланы законным заявленным отправителем, а, на самом деле, это не так
1 О наступает в результате получения доступа к информации

30. Ethernet имеет _____ топологию.
- О кольцевую
- О **звездообразную**
- О шинную
- О древовидную

31. Установите соответствие типа операционных систем и классификационного признака:
1. в зависимости от числа параллельно выполняемых процессов – это …
2. в зависимости от универсальности - это …
3. в зависимости от числа пользователей – это …

2 О переносимые
1 О однозадачные
3 О многопользовательские

32. В слове «небо» при кодировании кодами ASCII содержится ___ бит информации. (**32**)

33. Игра Pokemon Go, собравшая более 100 миллионов пользователей по всему миру за очень короткое время, является примером реализации такой технологии, как _____ реальность. (**виртуальная**)

34. Установите соответствие между левой и правой колонками таблицы:
1. сервисы, позволяющие пользователям сохранять и загружать информацию в облачное хранилище и делиться ими с другими людьми – это ….
2. сервисы, позволяющие пользователям создавать профили, делиться контентом, коммуницировать с друзьями, отслеживать новости – это …
3. сервисы, предоставляющие пользователю информацию по запросам, позволяя найти нужную информацию в Интернете – это …

1 О OneDrive
3 О Yandex.ru
2 О TikTok

35. Какие выделяют состояния процессов работы операционных систем?

(Укажите не менее двух вариантов ответа)

О **прерываемое состояние**

О **готовность**

О **ожидание**

О прорыв

36. Что из перечисленного является примером использования технологии «блокчейн»?

(Укажите не менее двух вариантов ответа)

О **функционирование цифровых площадок для покупки, продажи, обмена и хранения криптовалют**

О **обеспечение прозрачности доступа к информации о местоположении, происхождении, состоянии грузов для всех участников цепочки поставок**

О сотрудничество с разными работодателями без постоянного трудоустройства в какой-либо организации

О проведение сбора средств на реализацию и поддержание научных, творческих, социальных, экологических и других идей

37. _____ - это выстроенная по определенным правилам непрерывная последовательность цепочки блоков, содержащих информацию. (**блокчейн**)

Критерии оценивания тестовых заданий	Шкала оценок
Обучающийся дал верные ответы не менее, чем на 70% вопросов.	Зачтено
Обучающийся дал верные ответы менее, чем на 70% вопросов.	Не зачтено