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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.06 Корпоративные информационные системы

1. Код и наименование направления подготовки:

01.04.02 Прикладная математика и информатика

2. Профиль подготовки:

"Математическое и программное обеспечение информационных систем"

Квалификация (степень) выпускника: магистр

3. Форма обучения: очная

4. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

5. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

6. Рекомендована:

НМС факультета ПММ, протокол № 5 от 22.03.2024

7. Учебный год: 2025/2026 **Семестр(ы):** 4

8. Цели и задачи учебной дисциплины

Цели изучения дисциплины: изучение архитектурных особенностей различных типов корпоративных информационных систем; изучение основ администрирования файловых систем и системного программного обеспечения инфокоммуникационной системы; получение базовых навыков осуществления научного руководства проведения исследований по отдельным задачам

Задачи изучения дисциплины:

– ознакомление с современными и перспективными архитектурами корпоративных информационных систем;

– приобретение навыков планирования научно-исследовательских работ;

– приобретение навыков поиска информации, необходимой для выполнения профессиональных задач, в том числе, подготовки и решения задач с использованием различных типов корпоративных информационных систем;

– получение опыта по планированию структур каталогов (директорий), пользователей и групп пользователей, использования процедур защиты информации и процедур регистрации пользователей, инсталляций файл-сервера и программного обеспечения рабочих станций.

9. Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к части, формируемой участниками образовательных отношений части Блока 1.

10. 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)	Индикаторы(ы)	Планируемые результаты обучения
ПК-2	Способен осуществлять научное руководство проведением исследований по отдельным задачам	ПК-2.1	Формирует план проведения научно-исследовательских работ	Умеет: формировать план проведения научно-исследовательских работ.
ПК-4	Способен осуществлять администрирование файловых систем и системного программного обеспечения инфо-коммуникационной системы, проводить анализ системных проблем обработки информации на уровне инфо-коммуникационной системы	ПК-4.2	Осуществляет самостоятельный поиск информации, необходимой для выполнения профессиональных задач, использует специальные процедуры для повышения производительности и восстановления в случае сбоев дисковой подсистемы	Знает: – процедуры для повышения производительности и восстановления в случае сбоев дисковой подсистемы; – правила планирования структур каталогов (директорий), пользователей и групп пользователей, процедур защиты информации и процедур регистрации пользователей. Умеет: – осуществлять поиск информации, необходимой для выполнения профессиональных задач; – использовать специальные процедуры для повышения производительности и восстановления в случае сбоев дисковой подсистемы; – производить инсталляции файл-сервера и программного обеспечения рабочих станций; – осуществлять планирование структур каталогов (директорий), пользователей и групп пользователей, процедур защиты информации и процедур регистрации пользователей.
		ПК-4.3	Производит инсталляции файл-сервера и программного обеспечения рабочих станций, осуществляет планирование структур каталогов (директорий), пользователей и групп пользователей, процедур защиты информации и процедур регистрации пользователей	

11. Объем дисциплины в зачетных единицах/час – 2/72.
Форма промежуточной аттестации – зачет с оценкой.

12. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			4			
Аудиторные занятия	36		36			
в том числе: лекции	24		24			
Практические						
Лабораторные	12		12			
Самостоятельная работа	36		36			
Контроль						
Итого:	72		72			
Форма промежуточной аттестации	Зачет с оценкой		Зачет с оценкой			

12.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основные принципы построения корпоративных информационных систем.	Анализ архитектурных особенностей современных ВС и подходов к обеспечению их отказоустойчивого функционирования. Аппаратное обеспечение отказоустойчивости – резервирование различных типов. Временная и информационная избыточности: многократный счёт; альтернативные алгоритмы функционирования; альтернативные программы решения вычислительных и/или управляющих задач.	Б1.В.06 Корпоративные информационные системы (01.04.02 ПМИ) https://edu.vsu.ru/course/view.php?id=16204
1.2	Многопроцессорные системы.	Классификация систем параллельной обработки данных. Модели связи и архитектуры памяти. Многопроцессорные системы с общей памятью. Многопроцессорные системы с локальной памятью.	
1.3	Системы высокой готовности.	Основные определения. Подсистемы внешней памяти высокой готовности. Требования, предъявляемые к системам высокой готовности. Кластеризация как способ обеспечения высокой готовности системы.	
1.4	Облачные технологии в создании корпоративных информационных систем.	Виртуализация. Облачные технологии. Защита корпоративных сетей. Обзор средств защиты информации в системах с распределенной обработкой. Модели безопасности основных операционных систем. Алгоритмы аутентификации пользователей. Аутентификация пользователей при удаленном доступе. Протоколы удаленного доступа пользователя к компьютерной системе. Методы и средства защиты информации в сети. Технология виртуализации. Обеспечение безопасности в облачных платформах. Безопасность Облачных платформ. Интернет вещей, мобильные и носимые устройства. Big Data.	
2. Лабораторные работы			
2.1	Лабораторная работа №1.	Создание и настройка виртуальных машин.	Б1.В.06 Корпоративные информационные системы (01.04.02 ПМИ) https://edu.vsu.ru/course/view.php?id=16204
2.2	Лабораторная работа №2.	Создание и настройка доменной инфраструктуры с применением Windows Server.	
2.3	Лабораторная работа №3.	Проверка работоспособности доменной инфраструктуры.	
2.4	Лабораторная работа №4.	Общие принципы работы с GPO.	
2.5	Лабораторная работа №5.	Работа с разделом пользователи в GPO.	

12.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Основные принципы построения корпоративных информационных систем.	4	0	4	8	0	16
1.2	Многопроцессорные системы.	4	0	0	8	0	12
1.3	Системы высокой готовности.	4	0	4	10	0	18
1.4	Облачные технологии в создании корпоративных информационных систем.	12	0	4	10	0	26
	Итого:	24	0	12	36	0	72

13. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к зачету с оценкой.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: учеб. пособие. – СПб.: Питер, 2005.
2	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600. — Режим доступа: для авториз. пользователей.
4	Корнеев В.В. Вычислительные системы. - М.: Гелиос АРВ. 2004. - 512 с.
5	Хорафас Д.Н. Системы и моделирование / Д.Н.Хорафас. – М.: Мир, 2001. – 320 с.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
6	Электронно-библиотечная система «Университетская библиотека online (доступ осуществляется по адресу: https://biblioclub.ru/);
7	Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»);
8	Электронно-библиотечной системе «Лань» (доступ осуществляется по адресу: https://e.lanbook.com/),
9	ЭБС «BOOK» (доступ осуществляется по адресу: https://book.ru).
10	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
11	Б1.В.06 Корпоративные информационные системы (01.04.02 ПМИ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/view.php?id=16204

15. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

16. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.06 Корпоративные информационные системы (01.04.02 ПМИ)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15 в.11.

17. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий *лекционного типа*, семинарского типа, организации самостоятельной работы, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации: специализированная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения), допускается использование переносного оборудования.

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office, Notepad ++ (свободное и/или бесплатное ПО), 7-zip (свободное и/или бесплатное ПО).

Учебная аудитория для проведения практических занятий, *лабораторных работ, организации самостоятельной работы*, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или

бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО); PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО), 1С:Предприятие 8.3 (лицензионное ПО).

18. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Основные принципы построения корпоративных информационных систем.	ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
		ПК-4	ПК-4.2	
			ПК-4.3	
2	Многопроцессорные системы.	ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
		ПК-4	ПК-4.2	
			ПК-4.3	
3	Системы высокой готовности.	ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
		ПК-4	ПК-4.2	
			ПК-4.3	
4	Облачные технологии в создании корпоративных информационных систем.	ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
		ПК-4	ПК-4.2	
			ПК-4.3	
Промежуточная аттестация, форма контроля – зачет с оценкой				Перечень вопросов (КИМ№1)

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:

- лабораторные работы.

Перечень лабораторных работ

1	Лабораторная работа №1.	Создание и настройка виртуальных машин.
2	Лабораторная работа №2.	Создание и настройка доменной инфраструктуры с применением Windows Server.
3	Лабораторная работа №3.	Проверка работоспособности доменной инфраструктуры.
4	Лабораторная работа №4.	Общие принципы работы с GPO.
5	Лабораторная работа №5.	Работа с разделом пользователи в GPO.

Технология проведения

Все лабораторные работы обязательны для выполнения. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);

– оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету с оценкой.

Перечень вопросов к экзамену (КИМ №1)

1. Системы распределенной обработки данных
2. Системы распределенных баз данных
3. Режимы использования баз данных
4. Архитектура клиент-сервер
5. Структура типового приложения
6. Модель удаленного управления данными (модель файлового сервера).
7. Модель сервера баз данных
8. Способы распараллеливания запросов.
9. Трехзвенная модель сервера приложений.
10. Модель монитора транзакций.
11. Распределенная база данных. Достоинства и недостатки.
12. Основные принципы создания и функционирования распределенных БД.
13. Поддержка соответствия БД вносимым изменениям.
14. Модель тиражирования данных.
15. Монопольный и коллективный доступ к данным.
16. Полная блокировка, блокировка от записи, предохраняющая блокировка от записи, предохраняющая полная блокировка.
17. Взаимные и односторонние тупики.
18. Классификация угроз безопасности по виду защищаемой от угроз безопасности информации.
19. Классификация угроз безопасности по способу реализации угрозы безопасности.
20. Классификация угроз безопасности по типу информационных систем
21. Классификация уязвимостей программного обеспечения.
22. Примеры уязвимостей протоколов стека протоколов TCP/IP.
23. Общая характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия.
24. Угрозы типа «Анализ сетевого траффика», «Сканирование сети», «Выявление пароля».
25. Угрозы типа «Подмена доверенного объекта сети», «Навязывание ложного маршрута».
26. Угрозы типа «Внедрение ложного объекта», «Отказ в обслуживании», «Удаленный запуск приложений»
27. Метод подстановок и перестановок в криптографии
28. Основные принципы криптографии. Одноразовые блокноты.
29. Алгоритмы с симметричным криптографическим ключом.
30. Цифровые подписи.
31. Подписи с открытым ключом
32. Брандмауэры
33. Виртуальные частные сети
34. Безопасность в беспроводных сетях
35. Протоколы аутентификации
36. Угрозы безопасности по типу информационных систем
37. Уязвимости программного обеспечения.
38. Совместимость и мобильность программного обеспечения
39. Виды виртуализации
40. Модели развертывания облачных решений
41. Что представляют собой корпоративные информационные системы и какие задачи они решают в организации?

42. Какие основные компоненты входят в структуру корпоративной информационной системы?
43. Какие угрозы информационной безопасности могут возникнуть в корпоративных информационных системах, и как их можно предотвратить?
44. Что такое политика безопасности информации, и какие элементы она включает?
45. Какие методы мониторинга и аудита применяются для контроля информационной безопасности в корпоративных системах?
46. Какова роль баз данных в корпоративных информационных системах, и какие виды баз данных используются?
47. Какие методы аутентификации и авторизации применяются для обеспечения доступа к корпоративным информационным системам?
48. Какие требования к хранению и обработке персональных данных, согласно законодательству, применяются к корпоративным информационным системам?
49. Какие виды облачных вычислений могут быть использованы в корпоративных информационных системах, и какие преимущества они предоставляют?
50. Какие методы резервного копирования и восстановления данных используются для обеспечения надежности корпоративных информационных систем?
51. Цели и задачи применения корпоративной информационной системы.
52. Надёжность систем распределенного хранения данных.

Критерии оценки ответов на вопросы зачета с оценкой

Для оценивания результатов обучения на зачете с оценкой используется – 4-балльная шала:
«отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.
Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». Приэтом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ПК-2 Способен осуществлять научное руководство проведением исследований по отдельным задачам.

ПК-4 Способен осуществлять администрирование файловых систем и системного программного обеспечения инфо-коммуникационной системы, проводить анализ системных проблем обработки информации на уровне инфо-коммуникационной системы.

Задание 1

Дополните

... является основным видом обеспечения информационно-управляющих вычислительных систем.

Техническое обеспечение

Задание 2

Дополните

… определяет правила организации и управления каналами связи между элементами сети.

Физический уровень

Задание 3

Дополните

... определяет информационные порции для передачи за один сеанс, их форматы и способы передачи, а также правила совместного использования физического уровня несколькими процессами.

Канальный уровень

Задание 4

Укажите правильный вариант

... является основным видом обеспечения информационно-управляющих вычислительных систем.

1. Техническое обеспечение +
2. Физический уровень
3. Канальный уровень

Задание 5

Укажите правильный ответ

… определяет правила организации и управления каналами связи между элементами сети.

1. Физический уровень +
2. Техническое обеспечение
3. Канальный уровень

Задание 6

Укажите правильный ответ

... определяет информационные порции для передачи за один сеанс, их форматы и способы передачи, а также правила совместного использования физического уровня несколькими процессами.

1. Канальный уровень +
2. Физический уровень
3. Техническое обеспечение

Задание 7

Дополните

... управляет адресацией, буферизацией и маршрутизацией в сети.

Сетевой уровень

Задание 8

Дополните

... управляет сетевым уровнем при решении проблем достоверности передаваемых сообщений.

Транспортный уровень

Задание 9

Дополните

... регламентирует процесс передачи и приема во времени, т.е. определяет допустимые моменты начала, конца, повтора передач, точки синхронизации процессов, в которых осуществляется контрольный обмен между процессами, подтверждающими корректность совершенных к этому моменту передач.

Сеансовый уровень

Задание 10

Укажите правильный ответ

... управляет адресацией, буферизацией и маршрутизацией в сети.

1. Сетевой уровень +
2. Транспортный уровень
3. Сеансовый уровень

Задание 11

Укажите правильный ответ

... управляет сетевым уровнем при решении проблем достоверности передаваемых сообщений.

1. Транспортный уровень +
2. Сетевой уровень
3. Сеансовый уровень

Задание 12

Укажите правильный ответ

... регламентирует процесс передачи и приема во времени, т.е. определяет допустимые моменты начала, конца, повтора передач, точки синхронизации процессов, в которых осуществляется контрольный обмен между процессами, подтверждающими корректность совершенных к этому моменту передач.

1. Сеансовый уровень +
2. Транспортный уровень
3. Сетевой уровень

Задание 13

Дополните

... управляет преобразованием информации, связанным с использованием в сети несовместимых компьютеров, разных ОС, способов кодировки, форматов данных.

Представительный уровень

Задание 14

Дополните

... – обеспечивает взаимодействие между заданиями одного процесса и их исполнением другим процессом, при этом управляет взаимодействием нескольких зданий или исполнителей.

Прикладной уровень

Задание 15

Выберите правильный ответ.

... – это совокупность установок, устройств и оборудования, которые предназначены для преобразования материально-энергетических потоков в некий продукт, пригодный для потребления.

+ Технологические объекты

- Организационные объекты

- Объекты управления

Задание 16

Дополните

... – это разбиение задачи управления на подзадачи, решаемые соответствующими подсистемами.

Декомпозиция

Задание 17

Дополните

… - это объединение подсистем в единую систему снизу вверх, с последовательной проверкой свойств интегрированных подсистем и системы в целом на соответствие заданным свойствам.

Композиция

Задание 18

Дополните

… – это документ (инструкция), в котором описывается вся работа объекта с учетом

действий человека, всех приборов, материалов и норм безопасности.
Регламент

Задание 19

Дополните

… описывает работу объекта на основе условного графического обозначения.

Графический способ

Задание 20

Дополните

… – часть вещества или энергии обратно возвращается в технологический процесс.

Рецикл

Задание 21

Дополните

… метод исследования свойств одного объекта посредством изучения свойств другого объекта, более удобного для исследования и находящегося в определенном соотношении с первым объектом

Моделирование

Задание 22

Дополните

Существует … типа описания алгоритма графическим способом.

+ три

+ 3

Задание 23

Дополните

... служит для выбора наиболее эффективного алгоритма.

Паспорт

Задание 24

Дополните

… отработка возмущающих воздействий с целью поддержания выходных координат в заданных пределах.

Стабилизация

Задание 25

Дополните

... это математическая формулировка целей управления.

Критерий

Задание 26

Дополните

... системы автоматизации предназначен для функций визуализации, мониторинга и архивирования данных технологического процесса, а также для действий оператора.

Верхний уровень

Задание 27

Укажите правильный ответ

... управляет преобразованием информации, связанным с использованием в сети несовместимых компьютеров, разных ОС, способов кодировки, форматов данных.

1. Представительный уровень +
2. Прикладной уровень
3. Канальный уровень

Задание 28

Укажите правильный ответ

... – обеспечивает взаимодействие между заданиями одного процесса и их исполнением другим процессом, при этом управляет взаимодействием нескольких зданий или исполнителей.

1. Прикладной уровень +
2. Представительный уровень
3. Сетевой уровень

Задание 29

Дополните

… представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке данных.
+Вычислительные системы.

Задание 30

Дополните

…– это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.
+Среда распространения информативного сигнала
+Среда распространения информационного сигнала

Задание 31

Дополните

NMap – это …
+ Сетевой сканер.

Задание 32

Отметьте правильный ответ

... – это сетевой сканер.
+ NMap
- WireShark
-VirtualBox
-Linux

Задание 33

Дополните

Уязвимость … – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении, которые могут быть использованы для реализации угрозы безопасности данным.
+Информационной системы

Задание 34

Отметьте правильный ответ

Атака типа UPD-шторм используется в том случае, если на жертве открыт как минимум
1 порт
+2 порта
3 порта
4 порта
5 портов

Задание 35

Отметьте правильный ответ

Угроза типа «Анализ сетевого траффика» реализуется с помощью специальной …
+ программы-анализатора пакетов
- утилиты межсетевого взаимодействия
- операционной системы
- СУБД

Задание 36

Отметьте правильный ответ

... – это программа-анализатор пакетов.
- NMap
+ WireShark
-VirtualBox
-Linux

Задание 37

Отметьте правильный ответ

Подмена доверенного объекта сети реализуется в системах, где применяются … алгоритмы идентификации и аутентификации хостов, пользователей
+Нестойкие
-Стойкие
-Полиморфные
-Инкапсулированные

-Распределенные

Задание 38

Отметьте правильный ответ

Внедрение ложного объекта возможно через протокол

+ARP

-FTP

-POP3

-IMAP

-SMTP

Задание 39

Дополните

… - это угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

+Отказ в обслуживании

Задание 40

Отметьте правильный ответ

Вирус Морриса – это пример реализации угрозы

+Удаленного запуска приложений

-Навязывание ложного маршрута

-Отказ в обслуживании

-Внедрение ложного объекта

Задание 41

Отметьте правильный ответ

Слово криптография происходит от греческих слов, означающих

+ «скрытное письмо»

- «скрытный шифр»

-«скрытная весть»

-«тайное сообщение»

-«скрытное сообщение»

Задание 42

Дополните

… - эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией.

+Внедрение ложного объекта сети

Задание 43

Отметьте правильный ответ

Реализация данной угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы.

-сканирование сети

-угроза выявления пароля

-анализ сетевого трафика

+навязывание ложного маршрута

Задание 44

Дополните

… — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

+Межсетевой экран, +сетевой экран, +файервол, +брандмауэр

Задание 45

Дополните

… - стандартная утилита конфигурирования сетевого экрана в ОС Linux.

+iptables

Задание 46

Дополните

… - технология, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

VPN, Virtual Private Networt, Виртуальная частная сеть

Задание 47

Дополните

… - проверка соответствия (подлинности) сущности предъявленному ею идентификатору.

Аутентификация

Вопросы с вариантами ответов

Критерий оценивания	Шкала оценок
Верный ответ	1 балл
Неверный ответ	0 баллов

1. ... является основным видом обеспечения информационно-управляющих вычислительных систем.

1. *Техническое обеспечение*
2. Физический уровень
3. Канальный уровень

2. С каким типом атаки не может справиться брандмауэр

1. *DDOS*
2. Сканирование портов
3. UDP-шторм

3. Для работы алгоритма RSA на начальном этапе выбирают

1. *два простых числа*
2. два составных числа
3. два мнимых числа
4. два взаимно простых числа

4. Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP носит название

1. IPS
2. *IPsec*
3. IPC
4. IPCrypt
5. IPEnc

5. Какой слой в структуре системы управления кибербезопасности выделяется в качестве отдельного?

1. Процессы, персонал
2. Правила, нормативная база
3. *Данные*
4. Технологии, средства защиты информации

6. Какой процесс ITSM необходимо внедрять в первую очередь при построении системы кибербезопасности в организации?

1. Управление инцидентами
2. Управление изменениями
3. *Управление активами*
4. Управление конфигурациями

7. Какие подходы могут применяться при построении системы управления кибербезопасностью организации? Выберите все правильные ответы.

1. Вероятностный
2. Директивный
3. *Регуляторный*
4. *Риск-ориентированный*
5. Технологический
6. Объектный

8. Какие из перечисленных киберугроз являются ключевыми в текущих реалиях? Выберите все правильные ответы.

1. *Устройства IoT как площадка для реализации атак*
2. Спам
3. *Программы-вымогатели*
4. *Criminal-as-a-service (переход киберпреступников на сервисную модель)*
5. Программы-шпионы
6. *«Призраки интернета прошлого» (угрозы от устаревшего программного и программно-аппаратного обеспечения, которое находится в интернете)*
7. Программы-майнеры
8. Скимминг

9. Что из нижеперечисленного является тенденциями сетевой информационной безопасности? Выберите все правильные ответы.

1. Установка накладных средств защиты на сетевые устройства
2. *Интеграция с решениями по расследованию сетевых инцидентов*
3. *Инспектирование зашифрованного трафика*
4. Развитие общего сетевого периметра
5. *Интеграция с Threat Intelligence*
6. Уход от использования виртуальных и облачных межсетевых экранов
7. *Мониторинг аномалий во внутренней сети*
8. Внедрение протокола TLS 1.1 для защиты веб-трафика

10. Что из нижеперечисленного является тенденциями хостовой информационной безопасности? Выберите все правильные ответы.

1. *Сдвиг в сторону EDR-решений*
2. Применение узкоспециализированных решений
3. *Использование локальной и облачной песочницы для анализа подозрительных файлов*
4. *Обмен данными и командами с решениями по защите сетевых устройств*
5. Избегание SAAS-модели как несущей повышенные риски с точки зрения ИБ
6. Выбор в пользу единственного корпоративного антивируса и antimalware-движка

11. ... – обеспечивает взаимодействие между заданиями одного процесса и их исполнением другим процессом, при этом управляет взаимодействием нескольких заданий или исполнителей.

1. *Прикладной уровень*
2. Представительный уровень
3. Сетевой уровень

12. ... – это сетевой сканер.

1. *NMap*
2. WireShark
3. VirtualBox
4. Linux

13. Атака типа UPD-шторм используется в том случае, если на жертве открыт как

минимум

1. 1 порт
2. *2 порта*
3. 3 порта
4. 4 порта
5. 5 портов

14. Угроза типа «Анализ сетевого траффика» реализуется с помощью специальной …

1. *программы-анализатора пакетов*
2. утилиты межсетевого взаимодействия
3. операционной системы
4. СУБД

15. ... – это программа-анализатор пакетов.

1. NMap
2. *WireShark*
3. VirtualBox
4. Linux

16. Подмена доверенного объекта сети реализуется в системах, где применяются … алгоритмы идентификации и аутентификации хостов, пользователей

1. *Нестойкие*
2. Стойкие
3. Полиморфные
4. Инкапсулированные
5. Распределенные

17. Вирус Морриса – это пример реализации угрозы

1. *Удаленного запуска приложений*
2. Навязывание ложного маршрута
3. Отказ в обслуживании
4. Внедрение ложного объекта

18. Реализация данной угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы.

1. сканирование сети
2. угроза выявления пароля
3. анализ сетевого трафика
4. *навязывание ложного маршрута*

19. Внедрение ложного объекта возможно через протокол

1. *ARP*
2. FTP
3. POP3
4. IMAP
5. SMTP

20. … определяет правила организации и управления каналами связи между элементами сети.

1. *Физический уровень*
2. Техническое обеспечение
3. Канальный уровень

21. ... определяет информационные порции для передачи за один сеанс, их форматы и способы передачи, а также правила совместного использования физического уровня несколькими процессами.

1. *Канальный уровень*
2. Физический уровень
3. Техническое обеспечение

Вопросы с кратким текстовым ответом

Критерий оценивания	Шкала оценок
Должен быть сформулирован ответ из указанных вариантов (один или несколько) или аналогичные, по сути, ответы с альтернативными терминами и определениями	2 балла
Неверный ответ	0 баллов

2 – верный ответ
0 – неверный ответ

1. ... – это разбиение задачи управления на подзадачи, решаемые соответствующими подсистемами.
Ответ: Декомпозиция

2. … - это объединение подсистем в единую систему снизу вверх, с последовательной проверкой свойств интегрированных подсистем и системы в целом на соответствие заданным свойствам.
Ответ: Композиция

3. … – это документ (инструкция), в котором описывается вся работа объекта с учетом действий человека, всех приборов, материалов и норм безопасности.
Ответ: Регламент

4. … описывает работу объекта на основе условного графического обозначения.
Ответ: Графический способ

5. … – часть вещества или энергии обратно возвращается в технологический процесс.
Ответ: Рецикл

6. … метод исследования свойств одного объекта посредством изучения свойств другого объекта, более удобного для исследования и находящегося в определенном соотношении с первым объектом
Ответ: Моделирование

7. Существует … типа описания алгоритма графическим способом.
Ответ: три / 3

8. ... служит для выбора наиболее эффективного алгоритма.
Ответ: Паспорт

9. … отработка возмущающих воздействий с целью поддержания выходных координат в заданных пределах.
Ответ: Стабилизация

10. ... это математическая формулировка целей управления.
Ответ: Критерий

11. ... системы автоматизации предназначен для функций визуализации, мониторинга и архивирования данных технологического процесса, а также для действий оператора.
Ответ: Верхний уровень

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).