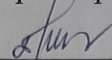


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Дагестанский государственный университет»
Колледж

УТВЕРЖДАЮ

директор Колледжа ДГУ

 Д.Ш. Пирбудагова

«30» 04 2022г.

Фонд оценочных средств

по учебной дисциплине

**МДК.01.04. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

10.02.05 Обеспечение информационной безопасности автоматизированных
систем

Махачкала -2022


Составитель/ составители:

Шахбанова М.И. - преподаватель кафедры естественнонаучных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

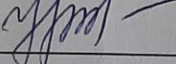
Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Фонд оценочных средств дисциплины рассмотрен и рекомендован к утверждению кафедрой специальных дисциплин Колледжа ДГУ.

Протокол № 8 от « 30 » 04 2022г.

Зав.кафедрой специальных дисциплин  Магомедова К.К.

Утверждена на заседании учебно-методического совета колледжа ДГУ

Ст. методист  /Шамсутдинова У.А./

ПАСПОРТ фонда оценочных средств

по дисциплине

ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1	Раздел I Разработка защищенных автоматизированных (информационных) систем	ОК 1; ОК2; ОК 3; ОК 4; ОК 5; ОК 6.	Устный опрос; тестирование; коллоквиум; самостоятельная работа; контрольная работа.
2	Раздел II Эксплуатация защищенных автоматизированных систем	ОК 9; ОК10.	Устный опрос; коллоквиум; тестирование; самостоятельная работа.
3	Раздел III Защита от несанкционированного доступа к информации в автоматизированных системах	ПК 1.2; ПК 1.3.	Устный опрос; коллоквиум; тестирование; контрольная работа.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3	4
1	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
2	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
3	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
4	Расчетно графическая работа/ Лабораторная работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий для выполнения расчетно-графической работы/ лабораторные работы по темам дисциплин
5	Устный опрос/ собеседование/	Средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
6	Самостоятельная работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий
7	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
8	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов

Критерии оценивания по дисциплине

№ п/п	Наименование оценочного средства	Критерии оценивания на «неудовлетв-но»	Критерии оценивания на «удовлетв-но»	Критерии оценивания на «хорошо»	Критерии оценивания на «отлично»
2	Коллоквиум	у студента обнаруживается незнание или непонимание большей или наиболее существенной части содержания учебного материала; не способен применять знание теории к решению задач профессионального характера; не умеет определить собственную оценочную позицию; допускает грубое нарушение логики изложения материала. допускает принципиальные ошибки в ответе на вопросы; не может исправить ошибки с помощью наводящих вопросов.	студент в основном знает программный материал в объёме, необходимом для предстоящей работы по профессии, но ответ, отличается недостаточной полнотой и обстоятельностью изложения; допускает существенные ошибки и неточности в изложении теоретического материала; в целом усвоил основную литературу; обнаруживает неумение применять государственно-правовые принципы, закономерности и категории для объяснения конкретных фактов и явлений; требуется помощь со стороны (путем наводящих вопросов, небольших разъяснений и	студент дает ответ, отличающийся меньшей обстоятельностью и глубиной изложения: обнаруживает при этом твёрдое знание материала; допускает несущественные ошибки и неточности в изложении теоретического материала; исправленные после дополнительного вопроса; опирается при построении ответа только на обязательную литературу; подтверждает теоретические постулаты отдельными примерами из юридической практики; способен применять знание теории к решению задач профессионального характера; наблюдается незначительное нарушение логики изложения	студент дает полный и правильный ответ на поставленные и дополнительные (если в таковых была необходимость) вопросы: обнаруживает всестороннее и системное и глубокое знание материала; обстоятельно раскрывает соответствующие теоретические положения; демонстрирует знание современной учебной и научной литературы; владеет понятийным аппаратом; демонстрирует способность к анализу и сопоставлению различных подходов к решению заявленной проблематики; подтверждает теоретические постулаты примерами из юридической практики; способен творчески применять знание теории к решению профессиональных задач; имеет собственную оценочную позицию и умеет аргументировано и

			т.п.); испытывает существенные трудности при определении собственной оценочной позиции; наблюдается нарушение логики изложения материала.	материала.	убедительно ее раскр ыть; четко излагает материал в логической последовательности.
4	Тест	0% -50% правильных ответов – оценка «неудовлетворител ьно»	51% - 64% правильных ответов – оценка «удовлетворител ьно»	65% - 84% правильных ответов – оценка «хорошо»,	85% - 100% правильных ответов – оценка «отлично»
5	Лаборато рная работа	студент не осуществил программную реализацию поставленной задачи; студент при программной реализации задачи допустил существенные ошибки, не смог обосновать выбор методов и приемов программирования , ответил не на все поставленные теоретические вопросы.	студент не осуществил программную реализацию поставленной задачи; студент при программной реализации задачи допустил существенные ошибки, не смог обосновать выбор методов и приемов программирован ия, ответил не на все поставленные теоретические вопросы.	студент в целом осуществил программную реализацию задачи с небольшими недочетами, не обосновал некоторый выбор методов и приемов программировани я, ответил не на все поставленные теоретические вопросы. студент осуществил программную реализацию задачи без ошибок, обосновал выбор методов и приемов программировани я, ответил на все поставленные теоретические вопросы.	студент в целом осуществил программную реализацию задачи с небольшими недочетами, не обосновал некоторый выбор методов и приемов программирования, ответил не на все поставленные теоретические вопросы; студент осуществил программную реализацию задачи без ошибок, обосновал выбор методов и приемов программирования, ответил на все поставленные теоретические вопросы.
6	Контрол ьная работа	Материал раскрыт не по существу, допущены грубые ошибки в	Вопросы письменной работы в целом раскрыты, но при этом допущена	Вопросы письменной работы раскрыты полностью и правильно, на	Работа соответствует заявленной теме, целям и задачам; характерна: - полнота и конкретность ответа;

	изложении и содержании теоретического материала; контрольная работа выполнена не по установленному варианту.	существенная ошибка или ответ неполный, несвязный, однако содержит некоторые обоснованные выводы, которые не в полной мере раскрывают тему.	основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки.	- последовательность и в изложении материала; - связь теоретических положений с практикой; - высокий уровень анализа и обобщения информационного материала, полноты обзора состояния вопроса; - обоснованность выводов.
--	--	---	---	--

Самостоятельная работа № 1

Тема № 1. «**Основы информационных систем как объекта защиты**»

1. Классификация автоматизированных информационных систем.
2. Классификация угроз.
3. Нормативная база.
4. Особенности объектов защиты.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 2

Тема № 2. «**Жизненный цикл автоматизированных систем**»

1. Жизненный цикл изделия. Этап эксплуатации, как основная цель.
2. Замысел, степень новизны, жизненный путь, жизненный цикл.
3. Потребность, цель и возможные последствия.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 3

Тема № 3. «**Угрозы безопасности информации в автоматизированных системах**»

1. Категорирование информационных ресурсов.
2. Анализ угроз безопасности информации.
3. Каналы утечки информации АИС.
4. Оценка угроз безопасности АИС.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.
Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 4

Тема № 4. «**Основные меры защиты информации в автоматизированных системах**»

1. Политика безопасности АИС.
2. Методы и средства защиты информации.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.
Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 5

Тема № 5. «**Содержание и порядок эксплуатации АС в защищенном исполнении**»

1. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.
2. Защита входа в систему (идентификация и аутентификация пользователей).
3. Разграничение доступа к устройствам. Управление доступом.
4. Использование принтеров для печати конфиденциальных документов. Контроль печати.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.
Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 6

Тема № 6. «**Защита информации в распределенных автоматизированных системах**»

1. Планирование и реализация систем защиты.
2. Средства разграничения доступа.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.
Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 7

Тема № 7. «**Особенности разработки информационных систем персональных данных**»

1. Определения уровня защищенности информационных систем персональных данных и выбор мер по обеспечению безопасности персональных данных.
2. Оценка угроз безопасности информационных систем персональных данных.
3. Требования по защите персональных данных, в соответствии с уровнем защищенности.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.
Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 8

Тема № 8. «Особенности эксплуатации автоматизированных систем в защищенном исполнении»

1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
2. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
3. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 9

Тема № 9. «Администрирование автоматизированных систем»

1. Задачи и функции администрирования автоматизированных систем.
2. Автоматизация управления сетью. Организация администрирования автоматизированных систем.
3. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем.
4. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 10

Тема № 10. «Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении»

1. Защита носителей информации резервное копирование и восстановлении данных.
2. Сопровождение автоматизированных систем. Управление исками и инцидентами управления безопасностью.
3. Обязанности администратора информационной безопасности автоматизированных систем.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 11

Тема № 11. «Защита от несанкционированного доступа к информации»

1. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.
2. Классификация автоматизированных систем. Требования по защите информации от НСД для АС.
3. Требования защищенности СВТ от НСД к информации.

4. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 12

Тема № 12. **«Система защиты информации от несанкционированного доступа»**

1. Установка и настройка СЗИ от НСД.
2. Защита входа в систему (идентификация и аутентификация пользователей).
3. Разграничение доступа к устройствам.
4. Управление доступом.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 13

Тема № 13. **«Эксплуатация средств защиты информации в компьютерных сетях»**

1. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.
2. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.
3. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении.
4. Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Самостоятельная работа № 14

Тема № 14. **«Документация на защищаемую автоматизированную систему»**

1. Оформление основных эксплуатационных документов на автоматизированную систему.
2. Особенности введения эксплуатационной документации.

Задание

Используя предложенную литературу и интернет источники ответить на вопросы.

Форма сдачи отчетности: письменные ответы на вопросы в тетради.

Примерная тематика курсовой работы

1. Физическое кодирование с использованием манчестерского кода.
2. Логическое кодирование с использованием скремблирования.
3. Подключение клиента к беспроводной сети в инфраструктурном режиме.
4. Оценка беспроводной линии связи.
5. Проектирования беспроводной сети.

6. Сбор информации о клиентских устройствах.
7. Планирование производительности и зоны действия беспроводной сети.
8. Предпроектное обследование места установки беспроводной сети.
9. Обеспечение отказоустойчивости в беспроводных сетях.
10. Режимы работы и организация питания точек доступа.
11. Сегментация беспроводной сети.
12. Настройка QoS.
13. Постпроектное обследование и тестирование сети.
14. Создание ACL-списка.
15. Наблюдение за трафиком в сети VLAN.
16. Определение уязвимых мест сети.
17. Реализация функций обеспечения безопасности порта коммутатора.
18. Исследование трафика.
19. Создание структуры сети организации.
20. Определение технических требований.
21. Мониторинг производительности сети.
22. Создание диаграммы логической сети.
23. Подготовка к обследованию объекта.
24. Обследование зоны беспроводной связи.
25. Формулировка общих целей проекта.
26. Разработка требований к сети.
27. Анализ существующей сети.
28. Определение характеристик сетевых приложений.
29. Анализ сетевого трафика.
30. Определение приоритетности трафика.
31. Изучение качества обслуживания сети.
32. Исследование влияния видеотрафика на сеть.
33. Определение потоков трафика, построение диаграмм потоков трафика.
34. Применение проектных ограничений.
35. Определение проектных стратегий для достижения масштабируемости.
36. Определение стратегий повышения доступности.
37. Определение требований к обеспечению безопасности.
38. Разработка ACL-списков для реализации наборов правил межсетевого экрана.
39. Использование CIDR для обеспечения объединения маршрутов.
40. Определение схемы IP-адресации.
41. Определение количества IP-сетей.
42. Создание таблицы для выделения адресов.
43. Составление схемы сети.
44. Анализ плана тестирования и выполнение теста.
45. Создание плана тестирования для сети комплекса зданий.
46. Проектирование виртуальных частных сетей.
47. Безопасная передача данных в беспроводных сетях.

Вопросы к дифференцированному зачету и к экзамену:

1. Понятие автоматизированной (информационной) системы.
2. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС.

3. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность
4. Основные особенности современных проектов АИС. Электронный документооборот.
5. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.
6. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение.
7. Модели жизненного цикла АИС.
8. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении.
9. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.
10. Требования к автоматизированной системе в защищенном исполнении.
11. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.
12. Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз.
13. Методы оценки опасности угроз. Банк данных угроз безопасности информации
14. Понятие уязвимости угрозы. Классификация уязвимостей.
15. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.
16. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним.
17. Идентификация и аутентификация субъектов доступа и объектов доступа.
18. Управление доступом субъектов доступа к объектам доступа.
19. Ограничение программной среды. Защита машинных носителей информации
20. Регистрация событий безопасности
21. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты.
22. Обновление баз данных признаков вредоносных компьютерных программ.
23. Обнаружение (предотвращение) вторжений
24. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.
25. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.
26. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.
27. Резервное копирование и восстановление данных.
28. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.
29. Механизмы и методы защиты информации в распределенных автоматизированных системах.
30. Архитектура механизмов защиты распределенных автоматизированных систем.
31. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем
32. Общие требования по защите персональных данных.
33. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.
34. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.

35. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
36. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
37. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении
38. Анализ журнала аудита ОС на рабочем месте.
39. Построение сводной матрицы угроз автоматизированной (информационной) системы.
40. Анализ политик безопасности информационного объекта.
41. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью.
42. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями.
43. Управление, тестирование и эксплуатация автоматизированных систем.
44. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
45. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.
46. Общие обязанности администратора информационной безопасности автоматизированных систем.
47. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД.
48. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.
49. Классификация автоматизированных систем. Требования по защите информации от НСД для АС.
50. Требования защищенности СВТ от НСД к информации.
51. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.
52. Назначение и основные возможности системы защиты от несанкционированного доступа.
53. Архитектура и средства управления. Общие принципы управления.
54. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.
55. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами.
56. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков.
57. Управление режимом контроля печати конфиденциальных документов.
58. Управление грифами конфиденциальности.
59. Обеспечение целостности информационной системы и информации
60. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.
61. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.
62. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации
63. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
64. Основные эксплуатационные документы защищенных автоматизированных систем.

65. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем.
66. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.
67. Настройка и устранение неисправности программно - аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

Правила выполнения практических работ:

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

1. Прежде, чем приступить к выполнению ПР, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
2. Перед началом каждой работы проверяется готовность обучающегося к ПР.
3. После выполнения ПР студент должен представить отчет о проделанной работе в рабочей тетради или в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.
4. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
5. Оценка за ПР выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

Примерный перечень практических заданий:

Практическая работа №1

Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)

Задание

1. Рассмотреть компоненты информационной системы: база данных (БД); схема базы данных;
2. Система управления базой данных (СУБД); приложения; пользователи; технические средства.
3. Найти информацию, характеризующую назначение и область применения заданного вида информационных систем.
4. Определить, к какому классу относится заданный вид информационных систем (по характеру использования информации, по сфере применения, по способу организации, по уровню и масштабу решаемых задач).
5. Составить общее описание заданного вида информационных систем.
6. Найти описание нескольких (не менее двух) современных информационных систем, относящихся к заданному виду.
7. Сформулировать краткое описание назначения и функциональных возможностей каждой из информационных систем по отдельности. Указать на характеристики и свойства, которые являются общими для всех рассматриваемых ИС.
8. Составить таблицу отличий между информационными системами.
9. Указать на их индивидуальные особенности, различающиеся количественные и качественные характеристики.

10. Разработать пример возможного применения одной из информационных систем в деятельности некоторого объекта автоматизации (предприятия или организации). Вид деятельности объекта автоматизации выбирается самостоятельно.
 11. Составить документ-обоснование для внедрения информационной системы. Описать, чего позволит достичь внедрение информационной системы с точки зрения повышения эффективности работы объекта автоматизации (организации, предприятия).
- Результаты зафиксировать в отчете.

Практическая работа №2

Разработка технического задания на проектирование автоматизированной системы

Задание

Для создания пояснительной записки использовать MS Word, а для создания схем и диаграмм рекомендуется использовать MS Visio.

1. Ознакомиться с примером технического задания для разработки какой-либо автоматизированной системы (АС), изучить основные типовые его разделы, ГОСТ 34.602-89
 2. Необходимо для себя ответить на следующие вопросы:
 - а) на основании каких документов разрабатывается методическое и информационное обеспечение системы (нормативные и другие документы);
 - б) перечень исходных данных: - какие массивы данных используются и в каких форматах; - на каких носителях эти данные будут поставляться в систему;
 - в) перечень выходных данных: - какие массивы данных будут являться результатом работы ПС; - какие документы будут представлены пользователю и в каком виде (указывается вид носителя) и с какой периодичностью; - какие требования по целостности данных и их защите должны быть выполнены в проектируемой системе.
 3. Используя пример и ГОСТ в пояснительной записке технического задания сформировать и описать раздел «Характеристика объекта управления»
 4. Сформировать и описать раздел «Назначение АС»
 5. Сформировать и описать раздел «Основные требования к АС»
 6. Сформировать и описать раздел «Технико-экономические показатели АС»
 7. Сформировать и описать раздел «Состав, содержание и организация работ по созданию АС»
 8. Сформировать и описать раздел «Порядок приемки АС»
- Результаты зафиксировать в отчете

Практическая работа №3

Построение модели угроз

Задание

1. Получить у преподавателя описание.
2. Для данной ИС построить модель угроз и уязвимостей:
 - выделить уязвимости, через которые могут быть реализованы угрозы;
 - определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать причины наличия этих угроз;
 - выделить угрозы, применимые к рассматриваемой ИС;

- определить уязвимости, через которые могут быть реализованы указанные угрозы.

Содержание отчета

1. Формулировка задачи.
2. Описание построенной модели угроз и уязвимостей.

Предметная область.

Тестовая информационная система ЗАО "ТестИС-Строй".

Основной вид деятельности ЗАО "ТестИС-Строй" – продажа строительных товаров на рынке "BusinessstoClient". Поставщиками являются частные лица и организации среднего и малого бизнеса. ЗАО "ТестИС-Строй" имеет четыре точки продаж, расположенные в пределах города. Каждая из этих точек – магазин площадью от 300 до 2000 м². В каждом магазине работает до 100 сотрудников.

ЗАО "ТестИС-Строй" имеет центральный офис в центре города, где располагается дата-центр, включающий центральную базу данных товаров и серверы баз данных бухгалтерии, отдела кадров и т. д. В центральном офисе и на каждой из точек продаж развернуты локальные вычислительные сети (ЛВС).

Каждая из ЛВС точек продаж связана с центральным офисом посредством сети Интернет. В точках продаж функционируют 1-2 сервера, обеспечивающих синхронизацию с центральной базой данных, и до 20 рабочих станций: компьютеры директора магазина, секретаря, терминалы в торговых залах.

В дата-центре установлены Web-сайт электронного магазина и почтовый сервер.

К терминалам торговых залов исключена возможность подключения внешних носителей. В датацентре все серверы размещены в несгораемых сейфах, доступ в помещение контролируется физически (охраняемое помещение). В торговых точках все серверы находятся в кабинетах, закрываемых на ключ. На всех компьютерах, кроме терминалов в торговых залах, установлено антивирусное ПО.

На серверах дата-центра установлен межсетевой экран. На сервере базы данных бухгалтерии дополнительно установлена система обнаружения вторжений.

Для подключения к дата-центру используется защищенное VPN-соединение. Для подключения к центральной базе товаров предусмотрен резервный канал. Загрузка терминалов торговых залов обеспечивается только после введения пароля в BIOS.

Примерные задачи по дисциплине:

1. Разработать модель разрешительной системы ролевого управления доступом в автоматизированной системе, с учетом:
 - групп пользователей (не более 5 ролей);
 - выполняемых функций группами пользователей;
 - наименования информационного ресурса;
 - меток конфиденциальности информационного ресурса;
 - мест хранения информационного ресурса (каталог HDD);
 - прав на доступ к информации (R - чтение, W - запись, D - удаление, N переименование, E - исполнение, M - модификация, A - полный доступ).
2. Разработать частную модель угроз безопасности распределенной информационной системы персональных данных (ИС ПДн) с подключением к сети международного информационного обмена по следующим исходным данным:
 - локальная ИС ПДн, развернута в пределах нескольких близко расположенных зданий;
 - имеет многоточечный выход в сеть общего пользования;
 - позволяет запись, удаление, сортировку ПДн;

- имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн;
 - используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн;
 - данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;
 - предоставляются сторонним пользователям ИС ПДн без предварительной обработки только часть ПДн.
3. Определить базовый уровень защищенности ИС ПДн по следующим исходным данным:
- обработка ПДн сотрудников организации;
 - категории биометрических и иных персональных данных;
 - объем обработки менее 100000 субъектов персональных данных;
 - возможны угрозы 2 типа.
4. Определить состав и содержание организационных и технических мер по защите ИС ПДн в соответствии с уровнем защищенности, руководствуясь последовательностью действий:
- определить базовый набор мер для третьего уровня защищенности ПДн;
 - адаптировать базовый набор мер, с учетом характеристик распределенной информационной системы;
 - подготовить предложения для уточнения адаптированного базового набора мер для различных вариантов ИС ПДн.
- Подобрать необходимый для заданного уровня защищенности ПДн состав средств защиты информации.
5. Разработать структуру технического задания на создание автоматизированной системы в защищенном исполнении. Составить технический паспорт на автоматизированную систему в защищенном исполнении, включающий:
- общие сведения об автоматизированной системе;
 - состав оборудования автоматизированной системы (состав основных и вспомогательных средств и систем);
 - состав средств защиты информации.
 -

Тест

1. Основы информационных систем как объекта защиты.
Выберите правильную последовательность уровней защиты информационной системы:
- а) пользовательский -сетевой -локальный -технологический –физический;
 - б) пользовательский -технологический -физический-сетевой –локальный;
 - в) локальный -технологический -физический -пользовательский –сетевой.
2. Для чего создаются информационные системы
- а) получения определенных информационных услуг;
 - б) обработки информации;
 - в) все ответы правильные.
3. Какие трудности возникают в информационных системах при конфиденциальности
- а) сведения о технических каналах утечки информации являются закрытыми;
 - б) на пути пользовательской криптографии стоят многочисленные технические проблемы;
 - в) все ответы правильные.
4. Основными источниками внутренних отказов информационных систем являются:
- а) ошибки при конфигурировании системы;

- б) отказы программного или аппаратного обеспечения;
 - в) выход системы из штатного режима эксплуатации.
5. Утечкой информации в информационной системе называется ситуация, характеризующаяся:
- а) потерей данных в системе 1580436089;
 - б) изменением формы информации;
 - в) изменением содержания информации.
6. Угроза информационной системе (компьютерной сети) – это:
- а) вероятное событие;
 - б) детерминированное (всегда определенное) событие;
 - в) событие, происходящее периодически.
8. Политика безопасности в информационной системе (сети) – это комплекс:
- а) руководств, требований обеспечения необходимого уровня безопасности;
 - б) инструкций, алгоритмов поведения пользователя в сети;
 - в) нормы информационного права, соблюдаемые в сети.
9. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:
- а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды;
 - б) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации способна противостоять только информационным угрозам, как внешним так и внутренним способна противостоять только внешним информационным угрозам.
10. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:
- а) Оранжевая книга;
 - б) Закон «Об информации, информационных технологиях и о защите информации»;
 - в) рекомендации X.800.
11. Базовые модели жизненного цикла: (выбрать все верные)
- а) каскадная модель;
 - б) поэтапная модель;
 - в) логическая модель;
 - г) спиральная модель;
 - д) интеллектуальная модель.
12. Непрерывный процесс, который начинается с момента принятия решения о необходимости создания ИС и заканчивается в момент ее полного изъятия из эксплуатации это:
- а) разработка;
 - б) жизненный цикл;
 - в) конфигурация;
 - г) управление проектами.
13. Что входит в структуру ЖЦ по стандарту ISO/IEC:
- а) организационные процессы;
 - б) основные процессы ЖЦ;
 - в) дополнительные процессы;
 - г) ветвящиеся процессы.

14. Структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ это:
- а) Проект;
 - б) модель ЖЦ;
 - в) инструкция;
 - г) 1580436089.
15. Технологии, базирующиеся на методологиях подготовки информационных систем и соответствующих комплексах интегрированных инструментальных средств, а также ориентированные на поддержку полного жизненного цикла АС или его основных этапов это:
- а) папо-технологии;
 - б) CASE-технологии;
 - в) инновационные технологии;
 - г) информационные технологии.
16. В стандарте ISO 12207 описаны _____ основных процессов жизненного цикла программного обеспечения
- а) три;
 - б) четыре;
 - в) пять;
 - г) шесть.
17. ISO 12207 – базовый стандарт процессов жизненного цикла
- а) программного обеспечения;
 - б) информационных систем;
 - в) баз данных;
 - г) компьютерных систем.
18. Согласно ISO 12207, процессы, протекающие во время жизненного цикла программного обеспечения, должны быть совместимы с процессами, протекающими во время жизненного цикла
- а) автоматизированной системы;
 - б) информационной системы;
 - в) компьютерной системы;
 - г) системы обработки и передачи данных.
19. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является
- а) приобретение;
 - б) решение проблем;
 - в) обеспечение качества;
 - г) аттестация.
20. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является
- а) процесс поставки;
 - б) документирования;
 - в) аудит;
 - г) управление конфигурацией.
21. Источник угрозы информационной безопасности для автоматизированных систем – это:
- а) потенциальный злоумышленник;
 - б) злоумышленник;

- в) нет правильного ответа.
22. Угрозы ИБ в автоматизированных системах можно классифицировать по нескольким критериям:
- а) по спектру ИБ;
 - б) по способу осуществления;
 - в) по компонентам АИС.
23. По каким компонентам классифицируются угрозы доступности в автоматизированных системах:
- а) 1580436089;
 - б) отказ пользователей;
 - в) отказ поддерживающей инфраструктуры;
 - г) ошибка в программе.
24. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
- а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности;
 - б) обрабатывать большой объем программной информации;
 - в) нет правильного ответа.
25. Вид источника угрозы ИБ, характер возникновения которого обусловлен действиями субъекта:
- а) техногенный источник;
 - б) антропогенный источник;
 - в) стихийный источник.
26. Степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников):
- а) готовность источника;
 - б) фатальность;
 - в) возможность возникновения источника.
27. Естественные угрозы безопасности информации в АИС вызваны:
- а) ошибками при действиях персонала;
 - б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - в) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
 - г) корыстными устремлениями злоумышленников.
28. Угрозы ИБ, реализация которых не влечет за собой изменение структуры данных (копирование):
- а) естественные угрозы;
 - б) пассивные угрозы;
 - в) активные угрозы;
 - г) искусственные угрозы.
29. По каким критериям нельзя классифицировать угрозы:
- а) по расположению источника угроз;
 - б) по аспекту информационной безопасности, против которого угрозы направлены в первую очередь;
 - в) по способу предотвращения;
 - г) по компонентам информационных систем, на которые угрозы нацелены.

30. Наиболее распространены угрозы информационной безопасности корпоративной системы:
- покупка нелегального ПО;
 - ошибки эксплуатации и неумышленного изменения режима работы системы;
 - сознательного внедрения сетевых вирусов.
31. Защита информации от несанкционированного доступа - это деятельность по предотвращению:
- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками;
 - получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации;
 - несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
32. Какая из приведенных техник является самой важной при выборе конкретных защитных мер
- анализ рисков;
 - анализ затрат / выгоды;
 - результаты ALE.
33. Какие меры по защите информации в автоматизированных системах дают наибольший эффект
- организационные;
 - технические (аппаратные);
 - программные;
 - все в совокупности;
 - правильных ответов нет.
34. Требования к программному обеспечению АСЗИ включают в себя требования: (выбрать все верные)
- к алгоритму принятия решения;
 - к системе классификации;
 - к системе команд;
 - к алгоритму обработки событий;
 - к сертификации программного обеспечения;
 - к системе диагностики программного обеспечения;
 - к оптимизации кода программного обеспечения и средству разработки.

Рекомендуемая литература

- Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 333 с. — URL : <https://urait.ru/bcode/491456>
- Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М.

- В. Дибров. — Москва : Издательство Юрайт, 2022. — 351 с. — URL : <https://urait.ru/bcode/491951>
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — URL : <https://urait.ru/bcode/476997>
 4. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2022. — 363 с. — URL : <https://urait.ru/bcode/495353>

Дополнительная литература:

1. Дибров М.В. Компьютерные сети и телекоммуникации. Маршрутизация в IP – сетях. В 2ч. Часть 1: учебник и практикум для СПО М.: Издательство Юрайт, 2020
2. Карпов В.Е., Коньков К.А. Основы операционных систем. Практикум Интуит НОУ, 2020
3. Коньков К.А., Карпов В.Е. Основы операционных систем. Интуит НОУ, 2016
4. Коньков К.А. Основы организации операционных систем Microsoft Windows Интуит НОУ, 2016
5. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации М.: Издательский центр «Академия», 2020.
6. Кузнецов С.Д. Введение в реляционные базы данных. Москва: Интуит НОУ, 2020.
7. Назаров С.В., Широков А.И. Современные операционные системы Интуит НОУ, 2019
8. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft Интуит НОУ, 2016

Интернет-ресурсы:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность <http://www.itsec.ru> –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
11. Федеральный портал «Российское образование www.edu.ru

