Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»
Финансово-экономический колледж

УТВЕРЖДАЮ
Директор
_____ Р. А. Сычев
«03» 07 2023г.

Рабочая программа МДК
Сертификация информационных систем

Специальность
09.02.07
Информационные системы и программирование

Форма обучения	очная
Часов по учебному плану	107
в том числе:	
аудиторные занятия	100
самостоятельная работа	4

Ростов-на-Дону
2023

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		**6 (3.2)**		Итого	
Недель	12		17			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	10	10	26	26	36	36
Практические	18	18	46	46	64	64
Итого ауд.	28	28	72	72	100	100
Контактная работа	28	28	72	72	100	100
Сам. работа	2	2	2	2	4	4
Промежут. аттестация			3	3	3	3
Итого	30	30	77	77	107	107

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование (Приказ Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1547)

Рабочая программа составлена по образовательной программе 09.02.07 Информационные системы и программирование для набора 2022 года

программа среднего профессионального образования

Учебный план утвержден учёным советом вуза от 29.08.2023 протокол № 1

Программу составил(и): Преподаватель, Кадобкин Д.М.

Председатель ЦМК: Горелько Е.А.

Рассмотрено на заседании ЦМК от 30.08.2023 протокол № 1

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Усвоение основных понятий и способов сертификации информационных систем, умение применять законодательство Российской Федерации в области сертификации программных средств информационных технологий, идентифицирование технических проблем, возникающих в процессе эксплуатации баз данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	МДК
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы проектирования баз данных
2.1.2	Архитектура аппаратных средств
2.1.3	Операционные системы и среды
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Учебная практика ПП.07
2.2.2	Производственная практика ПП.07
2.2.3	Квалификационный экзамен ПМ.07

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1 Знать

ПК 7.2. Осуществлять администрирование отдельных компонент серверов.
Тенденции развития банков данных.

Технологию установки и настройки сервера баз данных.

Требования к безопасности сервера базы данных.

ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.
Представление структур данных.

Технологию установки и настройки сервера баз данных.

Требования к безопасности сервера базы данных.

ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции.
Модели данных и их типы.

Основные операции и ограничения.

Уровни качества программной продукции.

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.
Технологию установки и настройки сервера баз данных.

Требования к безопасности сервера базы данных.

Государственные стандарты и требования к обслуживанию баз данных.

3.2 Уметь

ПК 7.2. Осуществлять администрирование отдельных компонент серверов.
Осуществлять основные функции по администрированию баз данных.

Проектировать и создавать базы данных.

ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.
Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в рамках поставленной задачи.

ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции.
Развертывать, обслуживать и поддерживать работу современных баз данных и серверов.

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.
Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.

3.3 Владеть

ПК 7.2.: Осуществлять администрирование отдельных компонент серверов
Навыками участвовать в администрировании отдельных компонент серверов.
ПК 7.3.: Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов
Навыками формировать необходимые для работы информационной системы требования к конфигурации локальных компьютерных сетей.
ПК 7.4.: Осуществлять администрирование баз данных в рамках своей компетенции
Навыками участвовать в соадминистрировании серверов
Навыками проверять наличие сертификатов на информационную систему или бизнес-приложения.
Навыками применять законодательство Российской Федерации в области сертификации программных средств информационных технологий.
ПК 7.5.: Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации
Навыками разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Защита и сохранность информации баз данных					
1.1	Законодательство Российской Федерации в области защиты информации. Требования безопасности к серверам баз данных. Классы защиты. Основные группы методов противодействия угрозам безопасности в корпоративных сетях /Лек/	5	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.2	Основные группы методов противодействия угрозам безопасности в корпоративных сетях. Программно-аппаратные методы защиты процесса обработки и передачи информации. Политика безопасности, настройка политики безопасности. Виды неисправностей систем хранения данных. /Лек/	5	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.3	Практическая работа №1 «Настройка политики безопасности» /Пр/	5	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.4	Резервное копирование: цели, методы, концепции, планирование, роль журнала транзакций. Виды резервных копий /Лек/	5	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.5	Утилиты резервного копирования /Лек/	5	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.6	Практическая работа №2 «Создание резервных копий базы данных» /Пр/	5	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.7	Восстановление базы данных: основные алгоритмы и этапы. Восстановление носителей. Воссоздание утраченных файлов. Полное восстановление. Неполное восстановление /Лек/	5	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.8	Практическая работа №3 «Восстановление базы данных» /Пр/	5	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.9	Самостоятельная работа «Защита и сохранность информации баз данных» /Ср/	5	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.10	Практическая работа №4 «Восстановление носителей информации» /Пр/	6	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.11	Практическая работа №5 «Восстановление удаленных файлов» /Пр/	6	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	

1.12	Мониторинг активности и блокирование /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.13	Автоматизированные средства аудита /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.14	Брандмауэры /Лек/	6	4	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.15	Практическая работа №6 «Мониторинг активности портов» /Пр/	6	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
1.16	Практическая работа №7 «Блокирование портов» /Пр/	6	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
	Раздел 2. Сертификация информационных систем					
2.1	Уровни качества программной продукции /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.2	Требования к конфигурации серверного оборудования и локальных сетей. Оформление требований. Техническое задание. /Лек/	6	4	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.3	Объекты информатизации, требующие обязательной сертификации программных средств и обеспечения /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.4	Сертификаты безопасности: виды, функции, срок действия. Проверка наличия сертификата безопасности /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.5	Системы сертификации. Процедура сертификации. /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.6	Платформы и центры сертификации. Сертификат разработчика. Процесс подписи и проверки кода. /Лек/	6	4	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.7	Практическая работа №8 «Проверка наличия и сроков действия сертификатов» /Пр/	6	8	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.8	Практическая работа №9 «Разработка политики безопасности корпоративной сети» /Пр/	6	8	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.9	Практическая работа №10 «Получение сертификата» /Пр/	6	6	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.10	SSL сертификат: содержание, формирование запроса, проверка данных с помощью сервисов. /Лек/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.11	Современные методы и средства обработки и представления информации в сети /Ср/	6	2	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	
2.12	Экзамен	6	3	ПК 7.2 ПК 7.3 ПК 7.4. ПК 7.5.	Л1.1 Л2.1 Э1 Э2	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация проводится в форме экзамена. Перечень вопросов к экзамену:

1. Законодательство Российской Федерации в области защиты информации.
2. Основные группы методов противодействия угрозам безопасности в корпоративных сетях.
3. Программно-аппаратные методы защиты процесса обработки и передачи информации.
4. Политика безопасности, настройка политики безопасности.
5. Виды неисправностей систем хранения данных.
6. Резервное копирование данных: цели.
7. Резервное копирование данных: методы.
8. Резервное копирование данных: концепции.
9. Резервное копирование данных: планирование.
10. Резервное копирование данных: роль журнала транзакций.
11. Виды резервных копий.
12. Утилиты резервного копирования.
13. Автоматизированные средства аудита.
14. Назначение и применение брандмауэров.
15. Восстановление носителей информации.
16. Воссоздание утраченных файлов.
17. Процедура полного восстановления.
18. Процедура неполного восстановления.
19. Уровни качества программной продукции.
20. Восстановление RAID-массива.
21. Требования к конфигурации серверного оборудования и локальных сетей.
22. Объекты информатизации, требующие обязательной сертификации программных средств и обеспечения.
23. Сертификаты безопасности: виды.
24. Сертификаты безопасности: функции.
25. Сертификаты безопасности: срок действия.
26. Системы сертификации.
27. Процедура сертификации.
28. Платформы и центры сертификации.
29. Сертификат разработчика.
30. SSL сертификат: содержание, формирование запроса, проверка данных с помощью сервисов.
31. Процесс подписи и проверки кода.
32. Процесс аттестации информационной системы.
33. Классификация информационных систем по степени защищенности.
34. Требования безопасности при разработке информационных систем.
35. Методы проверки и контроля за выполнением требований безопасности.
36. Аудит информационных систем: основные этапы и методы.
37. Сертификация и аттестация программного обеспечения.
38. Процедуры эксплуатации сертифицированных информационных систем.
39. Оценка рисков и угроз при сертификации информационных систем.
40. Обеспечение конфиденциальности информации при сертификации.
41. Роли и обязанности участников процесса сертификации информационных систем.
42. Специфика сертификации систем обработки платежей и финансовых данных.
43. Процедура получения разрешительной документации после сертификации.
44. Сертификационный центр и его функции.
45. Управление сертификатами и ключами при сертификации информационных систем.
46. Оценка соответствия сертифицированных информационных систем требованиям стандартов безопасности.
47. Процедуры тестирования и анализа уязвимостей при сертификации информационных систем.
48. Применение международных стандартов при сертификации информационных систем.
49. Сертификация открытых и закрытых информационных систем.
50. Использование результатов сертификации для повышения уровня безопасности информационных систем.

Критерии оценивания:

5 баллов выставляется студентам за полный и правильный ответ на все вопросы билета с логическим обоснованием аргументов, в ответе нет ошибок.

4 балла выставляется студентам, если вопросы билета раскрыты полностью, но обоснования доказательства недостаточны, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

3 балла ставится студентам за правильный ответ на вопросы билета, при этом допущено более одной ошибки по изложению фактов или более двух-трёх недочетов в ответе.

2 балла ставится студентам, если допущены существенные ошибки, показавшие, что обучающийся не обладает обязательными умениями по данной теме в полной мере.

5.2. Фонд оценочных средств для проведения текущего контроля

Представлен в Приложении 1 к рабочей программе МДК

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Количество

Л1.1	А. Г. Сергеев, В. В. Терегеря.	Стандартизация и сертификация: учебник и практикум для среднего профессионального образования.: учебное пособие для СПО: текст электронный	Издательство Юрайт, 2022	https://urait.ru/book/standartizaciya-i-sertifikaciya-489971 неограниченный доступ зарегистрированным пользователям
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Количество
Л2.1	Л. А. Доронина	Организация и технология документационного обеспечения управления: учебник и практикум: текст электронный	Издательство Юрайт, 2022	https://urait.ru/bcode/489555 неограниченный доступ зарегистрированным пользователям
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э1	ЭБС «Научная электронная библиотека eLIBRARY» https://www.elibrary.ru/defaultx.asp?			
Э2	ЭБС «Библиокомплектатор» http://www.bibliocomplectator.ru/			
6.3. Перечень программного обеспечения				
6.3.1	Офисный пакет - LibreOffice			
6.3.2	Интернет-браузер - Chromium			
6.4 Перечень информационных справочных систем				
6.4.1	ИСС «КонсультантПлюс»			
6.4.2	ИСС «Гарант»			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе МДК.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

МДК 07.02 Сертификация информационных систем

1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

УУД, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК 7.2. Осуществлять администрирование отдельных компонент серверов.			
Знать: Тенденции развития банков данных. Технологию установки и настройки сервера баз данных. Требования к безопасности сервера базы данных.	**Получение систематических знаний** о технологиях установки и настройки серверов баз данных и требованиях безопасности	**Уровень знаний** – тенденции развития банков данных. Технология установки и настройки сервера баз данных. Требования к безопасности сервера базы данных.	**Т (1-15), ПЗ (1-10)**
Уметь: Осуществлять основные функции по администрированию баз данных. Проектировать и создавать базы данных.	**Сформировать систематическое умение** по проектированию и созданию баз данных	**Уровень умения** осуществлять основные функции по администрированию баз данных. Проектировать и создавать базы данных.	**Т (1-15), ПЗ (1-10)**
Владеть: Навыками участия в администрировании отдельных компонент серверов.	**Сформировать систематическое владение** администрированием серверов и их компонент	**Уровень владения** - участвовать в администрировании отдельных компонент серверов.	**Т (1-15), ПЗ (1-10)**
ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.			
Знать: Представление структур данных. Технологию установки и настройки сервера баз данных. Требования к безопасности сервера базы данных.	**Получение систематических знаний** по установке и настройке серверов баз данных	**Уровень знаний** Технология установки и настройки сервера баз данных. Требования к безопасности сервера базы данных.	**Т (1-15), ПЗ (1-10)**
Уметь: Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в рамках поставленной задачи.	**Сформировать систематическое умение** по формированию требований в рамках поставленной задачи	**Уровень умения** – формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов в	**Т (1-15), ПЗ (1-10)**

		рамках поставленной задачи.	
Владеть: Навыками формирования необходимых для работы информационной системы требований к конфигурации локальных компьютерных сетей.	**Сформировать систематическое владение** способами формирования требований к конфигурации локальных компьютерных сетей.	**Уровень владения** - формировать необходимые для работы информационной системы требования к конфигурации локальных компьютерных сетей.	**Т (1-15), ПЗ (1-10)**
ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции.			
Знать: Модели данных и их типы. Основные операции и ограничения. Уровни качества программной продукции.	**Получение систематических знаний** по моделям данных и их типам, уровням качества ПО.	**Уровень знаний** - Модели данных и их типы. Основные операции и ограничения. Уровни качества программной продукции.	**Т (1-15), ПЗ (1-10)**
Уметь: Развертывать, обслуживать и поддерживать работу современных баз данных и серверов.	**Сформировать систематическое умение** по развертыванию, обслуживанию и поддержке работы баз данных и серверов.	**Уровень умения** – развертывать, обслуживать и поддерживать работу современных баз данных и серверов.	**Т (1-15), ПЗ (1-10)**
Владеть: Навыками участвовать в соадминистрировании серверов Навыками проверять наличие сертификатов на информационную систему или бизнес-приложения. Навыками применять законодательство Российской Федерации в области сертификации программных средств информационных технологий.	**Сформировать систематическое владение** навыками соадминистрирования серверов	**Уровень владения** - участвовать в соадминистрировании серверов.	**Т (1-15), ПЗ (1-10)**
ПК 7.5. Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.			
Знать: Технологию установки и настройки сервера баз данных. Требования к безопасности сервера базы данных. Государственные стандарты и требования к обслуживанию баз данных.	**Получение систематических знаний** технологий установки и настройки сервера баз данных, требований безопасности	**Уровень знаний** - технология установки и настройки сервера баз данных. Требования к безопасности сервера базы данных.	**Т (1-15), ПЗ (1-10)**

Уметь: Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.	**Сформировать систематическое умение** в технологиях проведения сертификации программного средства, разработке политики безопасности	**Уровень умения** – разрабатывать политику безопасности SQL сервера, базы данных. Владеть технологиями проведения сертификации ПО.	**Т (1-15), ПЗ (1-10)**
Владеть: Навыками разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.	**Сформировать систематическое владение** средствами реализации политике безопасности SQL сервера, базы данных и отдельных объектов базы данных.	**Уровень владения** - разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.	**Т (1-15), ПЗ (1-10)**

Т – тестовые задания, ПЗ –практические задания.

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Практические задания:

1 семестр

№ 1

Тема: «Настройка политики безопасности»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Главная цель мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин «политика безопасности» является не совсем точным переводом английского словосочетания «security policy», однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные «правила безопасности». Мы будем иметь в виду не отдельные правила или их наборы, а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений на верхнем уровне детализации может включать в себя следующие элементы:

· решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;

· формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;

· обеспечение базы для соблюдения законов и правил;

· формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Задание.

Изучить теоретический материал

Контрольные вопросы

1. Какие события безопасности должны фиксироваться в журнале аудита?
2. Какие параметры определяют политику аудита?
3. Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4. Целесообразно ли с точки зрения безопасности компьютерной системы

разрешать анонимный доступ к ее информационным ресурсам?

5. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?

6. Нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

7. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?

8. Из каких этапов состоит построение политики безопасности для компьютерной системы?

9. К чему может привести ошибочное определение политики безопасности (приведите примеры)?

10. Почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

№ 2

Тема: «Создание резервных копий базы данных» «Восстановление базы данных»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Для небольшой базы данных достаточно создать одно табличное пространство SYSTEM; однако, Oracle рекомендует создавать дополнительные табличные пространства для хранения данных и индексов пользователя, сегментов отмены, временных сегментов отдельно от словаря данных. Это обеспечивает вам большую гибкость в выполнении различных задач администрирования и уменьшает конкуренцию при обращении к объектам словаря и схемы.

Администратор может создавать новые табличные пространства, изменять размер файлов данных, добавлять файлы к табличным пространствам, устанавливать и изменять параметры хранения по умолчанию сегментов в табличном пространстве, переводить табличное пространство в состояние «только чтение» или «чтение-запись», делать табличное пространство временным или постоянным или удалить его.

Ход работы

Задание.

1. необходимо создать резервные копии базы данных «MMM» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

2. необходимо провести восстановление базы данных «MMM» из сделанных в задании №1 резервных копий.

2 семестр

№ 3

Тема: «Восстановление носителей информации» «Восстановление удаленных файлов»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

TestDisk — свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или человеческих ошибок (например, потеря MBR).

- Установка <sudo apt-get install testdisk>.
- Запускаем TestDisk <sudotestdisk>.
- Появляется окошко приветствия TestDisk, нам предлагается вести лог

работы (для выполнения данной работы лог не требуется).

- Выбираем нужный диск и нажимаем Enter.
- Предлагается выбрать тип таблицы разделов, обычно TestDisk определяет все правильно, так что нажимаем Enter.
- Выбираем Analise.
- Выбираем QuickSearch.
- Нам выводят таблицу разделов. Выбираем раздел и нажимаем P, чтобы вывести список файлов.
- Выбираем файлы для восстановления и нажимаем C.
- Выбираем папку, куда будут сохранены файлы и нажимаем C.

PhotoRec - это утилита, входящая в состав пакета TestDisk. Предназначена для восстановления испорченных файлов с карт памяти цифровых фотоаппаратов (CompactFlash, SecureDigital, SmartMedia, MemoryStick, Microdrive, MMC), USB flash-дисков, жестких дисков и CD/DVD. Восстанавливает файлы большинства распространенных графических форматов, включая JPEG, аудио-файлы, включая MP3, файлы документов в форматах winPDF и HTML, а также архивы, включая ZIP. Может работать с файловыми системами ext2, ext3, ext4 FAT, NTFS и HFS+, причем способна восстановить графические файлы даже в том случае, когда файловая система повреждена или отформатирована.

- Установка <sudo apt-get install testdisk>.
- Запускаем PhotoRec <sudophotorec>.
- Выбираем нужный диск и нажимаем Enter.
- В нижнем меню можно выбрать FileOpt, чтобы выбрать типы файлов для восстановления (по умолчанию выбраны все).
- Чтобы начать восстановление нажмите Enter, выбрав Search.
- У нас выбрана система ext4, поэтому выбираем первый вариант [ext2/ext3].
- Если выбрать пункт FREE, то поиск будет произведен в пустом пространстве и в этом случае будут восстановлены только удаленные файлы, а если выбрать WHOLE, то поиск будет произведен на всем диске.
- Теперь нужно указать директорию, куда будем сохранять нужные нам файлы. Выбираем нужную папку и нажимаем C.
- Выбираем файлы для восстановления и нажимаем C.

Extundelete – утилита, позволяющая восстанавливать файлы, которые были удалены с разделов ext3/ext4.

- Установка: <sudo apt-get install extundelete>.
- Как только вы поняли, что удалили нужные файлы, необходимо отмонтировать раздел: <umount /dev/<partition>>
- Зайдите в каталог, в который будут восстанавливаться удаленные данные. Он должен быть расположен на разделе отличном от того, на котором хранились восстанавливаемые данные: cd /<путь_к_каталогу_куда_восстанавливать_данные>
- Запустите extundelete, указав раздел, с которого будет происходить восстановление и файл, который необходимо восстановить: sudoextundelete /dev/<partition> –restore-file

/<путь к файлу>/<имя_файла>

- Можно так же восстанавливать содержимое каталогов: sudoextundelete /dev/<partition>

–restore-directory /<путь_к_директории>

Foremost - консольная программа, позволяющая искать файлы на дисках или их образах по hex-данным, характерным заголовкам и окончаниям. Программа проверяет файлы на предмет совпадения заранее определённых hex-кодов (сигнатур), соответствующих наиболее

распространённым форматам файлов. После чего экстрагирует их из диска/образа и складывает в каталог, вместе с подробным отчётом о том, чего, сколько и откуда было восстановлено. Типы файлов, которые foremost может сразу восстановить: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp. Есть возможность добавлять свои форматы (в конфигурационном файле /etc/foremost.conf), о которых программа не знает.

- Установка: <sudo apt-get install foremost>
- Примериспользованиядлявосстановленияизображенийсдиска /dev/sdb вкаталог ~/out_dir

: <sudo foremost -t jpg,gif,png,bmp -i /dev/sdb -o ~/out_dir>

Задание.

Добавьте в виртуальную машину виртуальный жесткий диск.

Запустите виртуальную машину с Linux.

Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами.

Отформатируйте созданные разделы в файловую систему ext4.

Установите TestDisk.

Удалите MBR (или таблицу разделов) с помощью команды DD.

Восстановите MBR (или таблицу разделов) с помощью TestDisk. Смонтируйте восстановленные разделы и создайте там произвольные файлы. Удалите созданные файлы.

С помощью TestDisk восстановите данные.

Создайте произвольный каталог и запишите туда данные каталога /var/log/ .

Удалите данные с созданного каталога.

С помощью PhotoRec восстановите данные.

Создайте произвольный каталог и запишите туда данные каталога /etc/ .

С помощью Extundelete или Foremost восстановите данные.

Контрольные вопросы

1. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?
2. Какие файловые системы поддерживает PhotoRec?
3. Какие форматы поддерживает PhotoRec?
4. Как Foremost восстанавливает файлы?
5. Можно ли восстановить данные с файловой системы NTFS, используя extundelete?
6. Все ли данные скопированные с каталога /var/log/ восстановились?
7. Все ли данные скопированные с каталога /etc/ восстановились?

№ 4

Тема: «Мониторинг активности портов»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

На этапе мониторинга выполняется процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Ход работы

Задание.

1. Опишите процедуру активности портов.

№ 5

Тема: «Блокирование портов»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Понятие порта в компьютере многозначно.

Самое общее определение: порт - это соединение (физическое или логическое), через которое принимаются и отправляются данные. Обмен данными между любыми устройствами возможен только при наличии утвержденного стандарта на интерфейс.

В состав аппаратного обеспечения порта входит специализированный разъём, предназначенный для подключения оборудования определённого типа. Часто этот специализированный разъем и называют портом, например USB-порт, но есть разъемы, которые портами называть не принято, например, RJ11. Как правило, каждый порт имеет обозначение, которое размещается рядом с разъемом.

Основные порты, используемые в компьютерах, ноутбуках:

- USB-порт;
- IEEE 1394 (FireWire) ;
- Порт eSATA и комбинированный порт USB/eSATA;
- Сетевой порт Ethernet;
- Порт SCSI;
- Последовательный порт RS-232;
- Порты для подключения внешних мониторов VGA, DVI, S-Video, HDMI, DisplayPort;
- Порт для док-станции и порт репликатор;
- Порты для модулей расширения PCMCIA, ExpressCard. USB - UniversalSerialBus -

универсальная последовательная шина.

USB-порты являются своего рода стандартом для подключения внешних устройств, к которому стремятся все производители этих устройств. К портам USB подключаются: мыши, клавиатуры, принтеры, сканеры, модемы, кардридеры, флэш-накопители, фотоаппараты, сотовые телефоны, плееры, жёсткие диски, оптические дисководы и др. IEEE 1394 - высокоскоростной последовательный порт для цифровых видеоустройств.

Компания Apple продвигает стандарт IEEE 1394 под маркой FireWire, компания Sony – под маркой i.LINK. IEEE 1394 применяется для подключения видеокамер, цифровых фотоаппаратов и других мультимедийных устройств, а также принтеров, сканеров, внешних жестких дисков. Основные преимущества по сравнению с USB 2.0 - более высокая скорость передачи, большая стабильность, большая длина кабеля до оконечного устройства.

eSATA - ExternalSerial ATA (AdvancedTechnologyAttachment - присоединение по передовой технологии) – последовательный интерфейс для подключения внешних устройств, поддерживающий режим «горячей замены». Стандарт eSATA предусматривает подключение внешних жестких дисков, оптических дисков, RAID-массивов. Скорость передачи данных гораздо выше, чем у USB 2.0 или IEEE 1394.

Недостатки eSATA:

- максимальная длина кабеля не превышает 2 метров;
- жёсткие диски, подключаемые через eSATA, потребуют дополнительного

источника питания - это могут быть как разъёмы USB или 1394, так и розетка.

Порт Ethernet предназначен для подключения ноутбука к компьютерной сети с помощью сетевого кабеля через разъем RJ45 (RJ-45). Технология Ethernet описывается стандартами IEEE группы 802.3. Существует несколько стандартов технологии Ethernet. Стандарты различаются скоростью передачи данных и передающей средой. В ноутбуках обычно устанавливают порт Ethernet 10/100/1000, который поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T для расстояний до 100 м.

Стандарт 10BASE-T позволяет передавать данные со скоростью 10 Мбит/с. Для передачи используется 4 провода кабеля витой пары категории 3 или категории 5. По стандарту 100BASE-TX скорость передачи данных составляет 100 Мбит/с. Стандарт применяется для построения сетей топологии «звезда». Задействована витая пара категории 5, поддерживается дуплексная передача данных. Стандарт 1000BASE-T - гигабитный (Gigabit, Geth) Ethernet позволяет передавать данные со скоростью до 1 Гбит/с. Стандарт предусматривает использование витой пары категорий 5е. RS-232 (англ. RecommendedStandard) - стандарт последовательной асинхронной передачи двоичных данных между двумя устройствами на расстоянии до 15 метров.

Порт RS-232 в последнее время не часто встречается в бизнес-ноутбуках, но может быть полезен в промышленных ноутбуках. Он используется для реализации систем сбора данных в реальном времени, подключения научного оборудования, управления другими устройствами. Для подключения оборудования, работающего по стандарту RS-232, ноутбуки оснащаются 9-штырьковым разъёмом DB-9 (D-sub).

VGA (англ. Video Graphics Array) - аналоговый интерфейс, предназначенный для подключения внешнего дисплея или проектора через 15-контактный разъём DB-15F (D-sub). DVI (англ. Digital Visual Interface - цифровой видеоинтерфейс) - стандарт на интерфейс и соответствующий разъём, предназначенный для передачи видеоизображения на цифровые устройства отображения, такие как жидкокристаллические мониторы и проекторы. Имеются три версии DVI:

- DVI-A - только аналоговая передача.
- DVI-I - аналоговая и цифровая передача.
- DVID - только цифровая передача. Аналоговый порт S-Video служит для подключения ноутбука к телевизору.

HDMI (англ. High-Definition MultimediaI nterface - мультимедиа интерфейс высокой чёткости) - интерфейс, позволяющий передавать цифровые видеоданные высокого разрешения и многоканальные цифровые аудиосигналы с защитой от копирования. Разъем HDMI в ноутбуке используется для подключения к жидкокристаллическому телевизору или проектору. Основное различие между HDMI и DVI состоит в том, что разъём HDMI меньше по размеру, а также поддерживает передачу многоканальных цифровых аудиосигналов. Display Port – современный интерфейс, предназначенный для подключения к компьютеру аудио и видеоаппаратуры.

Display Port имеет пропускную способность вдвое большую, чем DVI, низкое напряжение питания и низкие посторонние наводки. В настоящее время существуют два типа разъёмов: полноразмерный Display Port и уменьшенный MiniDisplay Port, разработанный компанией Apple. Размеры разъёма MiniDisplayPort в 10 раз меньше, чем у стандартного разъёма DVI. Технология, реализованная в DisplayPort, позволяет передавать одновременно как графические, так и аудио сигналы. Основное отличие от HDMI — более широкий канал для передачи и большая скорость передачи данных.

Док-станция (dockstation) - это специальная "подставка под ноутбук", предназначенная для подключения к ноутбуку набора различных портов, разъемов и интерфейсов. Док-станция обычно устанавливается на стационарном рабочем месте, к ней можно подключить монитор, мышь, клавиатуру, сетевой кабель, принтер. В ней может находиться встроенный блок питания,

дисковод CD/DVD. Ноутбук устанавливается на док-станцию, и через специальный разъем все его интерфейсы соединяются с интерфейсами док-станции, облегчая тем самым подключение ноутбука к внешним устройствам. Док-станция не только существенно расширяет набор интерфейсов, но и делает более удобным переход из офисного режима использования ноутбука в мобильный. При использовании док-станции нет необходимости каждый день, уходя домой, терять время на то, чтобы отсоединить ноутбук от сети и периферии. Всё, что нужно сделать, – извлечь его из док-станции. Сам же разъём для подключения док-станции, как обычно, находится на днище ноутбука и в тех случаях, когда необходимости в нём нет, закрывается небольшой шторкой, предохраняющей от засорения. Док станции выпускаются, как фирмами изготовителями ноутбуков, так и сторонними разработчиками. Как правило, у каждого производителя есть собственный вариант разъёма для подключения док станции.

Порт-репликатор (Portreplicator), как и док-станция, служит для подключения к ноутбуку различных портов, разъемов и интерфейсов, но возможности его меньше. Порт-репликатор позволяет иметь всегда готовое подключение к большому монитору, клавиатуре, принтеру, внешнему факс-модему, мыши, мощным стерео-колонкам и др. что сохраняет разъемы этих подключений на более длительный срок от возможных поломок и сокращает время подключения. Порт-репликаторы выпускаются, как фирмами производителями ноутбуков (некоторые даже идут в комплекте с ноутбуком) или же сторонними производителями – универсальные порт-репликаторы. Производители обычно имеют собственные варианты разъёмов для подключения порт-репликатора.

PCMCIA (PersonalComputerMemoryCardInternationalAssociation)- спецификация на модули расширения, разработанная ассоциацией PCMCIA. Карты расширения, изготовленные в соответствии с этой спецификацией обычно называются PC-карты (PC Card). Основные типы карт расширения: Type I, Type II и Type III. Все карты расширения имеют размер 85,6 мм в длину и 54 мм в ширину. Карты Type I имеют 16-разрядный интерфейс и используются для расширения памяти. Толщина карты Type I- 3,3 мм. Разъем имеет один ряд контактов. Карты Type II оснащаются либо 16- , либо 32-разрядным интерфейсом. Толщина карты- 5 мм. Они поддерживают устройства вводавывода, что позволяет использовать их для подключения периферийных устройств. Разъём имеет два ряда контактов. Карты Type III поддерживают 16- или 32-разрядный интерфейс. Они имеют толщину 10,5 мм, что позволяет устанавливать на карту стандартные разъёмы внешних интерфейсов и избавиться таким образом от дополнительных кабелей. Разъем имеет четыре ряда контактов. Разъем PCMCIA представляет собой щель шириной 54 мм, которая закрыта либо откидной шторкой, либо пластиковой заглушкой. Разъем (слот) PCMCIA (вверху) и заглушка, внизу - кардридер Большинство ноутбуков оснащается лишь одним разъемом PCMCIA типа II. А современные ноутбуки уже обходятся и вовсе без этих разъемов.

Порт ExpressCard Стандарт ExpressCard для карт расширения был разработан ассоциацией PCMCIA на смену стандарту PC Card. Новый стандарт был создан на базе новой скоростной последовательной шины PCI Express. Стандарт ExpressCard не только более производительный, чем PC Card, но и более универсальный. Через ExpressCard можно подключаться к шине USB. Карты ExpressCard бывают двух типов, отличающихся по ширине: 34 мм и 54 мм. Соответственно и разъемы бывают двух типов ExpressCard/34 и ExpressCard/54. При этом карты 34 мм можно устанавливать как в разъем ExpressCard/34, так и в разъем ExpressCard/54. Через разъемы ExpressCard подключают ТВ-тюнеры, звуковые карты, карты Wi-Fi, флеш-накопители (они часто подключаются через USB-составляющую интерфейса ExpressCard), модемы для работы в сотовых сетях и др. Разъем RJ11(RJ-11 Registeredjack) – разъем модема ноутбука. Используется для подключения к Интернету через модем по телефонной линии.

Ход работы

Задание. Организовать запрет доступа к USB сменным носителям при помощи групповых политик (GPO).

№ 6

Тема: «Проверка наличия и сроков действия сертификатов»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Цифровой сертификат – электронный документ, выданный и заверенный Удостоверяющим центром.

Цифровой сертификат - это небольшой файл, содержащий в себе следующую информацию:

1. имя и идентификатор владельца сертификата;
2. открытый ключ подписи (шифрования);
3. имя, идентификатор и цифровую подпись Удостоверяющего центра;
4. серийный номер, версию и срок действия сертификата.

Инфраструктура открытых ключей (англ. *PKI - Public Key Infrastructure*) — набор средств (технических, материальных, людских и т. д.), распределенных служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей.

В основе PKI лежат несколько основных принципов:

1. закрытый ключ известен только его владельцу;
2. удостоверяющий центр создает сертификат открытого ключа, таким образом удостоверяя этот ключ;
3. никто не доверяет друг другу, но все доверяют удостоверяющему центру;
4. удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Ход работы

Задание. С помощью консоли работы с личными сертификатами пользователя ознакомьтесь с возможностями манипулирования уже полученными сертификатами.

Познакомьтесь с возможностями получения сертификатов через Web от автономного центра сертификации, а также с методами работы с корпоративным центром выдачи сертификатов.

№ 7

Тема: «Разработка политики безопасности корпоративной сети»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Политика информационной безопасности — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации.

На основе политики информационной безопасности строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение информационных систем в различных ситуациях. Для конкретной информационной системы политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т. д.

Политика информационной безопасности компании должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

Для того, чтобы политика информационной безопасности была эффективно реализована на практике, необходимо, чтобы она была:

- непротиворечивой – разные документы не должны по-разному описывать подходы к одному и тому же процессу обработки информации
- не запрещала необходимые действия – в таком случае неизбежные массовые нарушения приведут к дискредитации политики информационной безопасности среди пользователей
- не налагала невыполнимых обязанностей и требований.

В организации должно быть назначено лицо, ответственное за политику безопасности, отвечающее за её эффективную реализацию и регулярный пересмотр.

Ход работы

Задание.1. Выбрать вариант (вид организации, для которой будет разрабатываться политика ИБ)

1. Скачать образец политики ИБ.
2. На основе образца разработать политику ИБ, учитывая специфику деятельности выбранной организации.
3. Разработанную политику ИБ вложить в качестве ответа на данное задание. Варианты

1) Образовательная организация
2) Агентство недвижимости
3) Администрация города
4) Городская поликлиника
5) Компания по разработке ПО
6) Интернет-провайдер
7) Отделение налоговой службы
8) Городской архив
9) Центр оказания государственных услуг
10) Страховая компания

№ 8

Тема: «Получение сертификата»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Компьютер – это устройство, которое используется во всех сферах жизнедеятельности человека. Передача и хранение информации, ведение бухгалтерии, диагностика в сфере медицины – далеко не полный перечень функций, выполняемых данным оборудованием. Однако успешное функционирование компьютера зависит от качества программного обеспечения. Системой стандартизации к информационным продуктам предъявляется ряд требований.

Сертификация программного обеспечения – это процедура, направленная на подтверждение соответствия данного компонента нормам и стандартам, действующим на территории России.

Поскольку основной контролирующей системой в нашей стране является Госстандарт, процедура проверки для такой продукции проводится именно в этой структуре. В соответствии с положениями правительственного Постановления № 982 от 1 декабря 2009 года, сертификат на данный продукт не является обязательным. Несмотря на это, многие изготовители и продавцы

такой продукции считают необходимым получить документальное подтверждение соответствия в Госстандарте на основе добровольного желания.

Сертификация проводится на основе требований ГОСТ 19781-90. Добровольная процедура контроля повышает конкурентоспособность товаров, поскольку вызывает доверие со стороны потребителей. Она осуществляется в органах по сертификации, имеющих аккредитацию Госстандарта. С целью получения разрешительного документа производителю или продавцу необходимо подать заявку, предоставить документы и саму программу для исследования. После детального изучения материалов специалисты принимают решение об их соответствии нормативам данной системы. политику безопасности, отвечающее за её эффективную реализацию и регулярный пересмотр.

Ход работы

Задание. Опишите процедуру получения сертификата на программное обеспечение

№ 9

Тема: «Жизненный цикл программного средства. Качество программного средства»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Под моделью ЖЦ ПО понимается структура, определяющая последовательность выполнения и взаимосвязи процессов, действий, задач на протяжении ЖЦ. Модель ЖЦ зависит от специфики, масштаба и сложности проекта и специфики условий, в которых система создается и функционирует. Международный стандарт ISO/IEC 12207: 1995 описывает структуру процессов ЖЦ ПО.

Наибольшее распространение получили следующие две модели ЖЦ ПО: каскадная и спиральная.

Задание

Разработайте проект своего программного обеспечения (для чего предназначено ПО, какими средствами разработано, на кого направлено, какие функции и операции выполняет, его название и т.д.).

Выберите модель жизненного цикла программного обеспечения для своего проекта. Определите процессы для первой стадии (формирование требований к ПО).

Сделайте выводы по проделанной работе.

Контрольные вопросы

1. Что такое модель жизненного цикла программного обеспечения?
2. Типы моделей жизненного цикла ПО.
3. Преимущества каскадного подхода.
4. Особенности спиральной модели.
5. Стадии программного обеспечения.

№10

Тема: «ГОСТы ЕСПД и их применение»

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Единая система программной документации (ЕСПД) — комплекс государственных стандартов Российской Федерации, устанавливающих взаимосвязанные правила разработки, оформления и обращения программ и программной документации.

В стандартах ЕСПД устанавливают требования, регламентирующие разработку, сопровождение, изготовление и эксплуатацию программ, что обеспечивает возможность:

унификации программных изделий для взаимного обмена программами и применения ранее разработанных программ в новых разработках;

снижения трудоемкости и повышения эффективности разработки, сопровождения, изготовления и эксплуатации программных изделий;

автоматизации изготовления и хранения программной документации.

Сопровождение программы включает анализ функционирования, развитие и совершенствование программы, а также внесение изменений в неё с целью устранения ошибок.

Поскольку ЕСПД представляет собой набор ГОСТов, в настоящее время её применение на территории РФ носит только рекомендательный характер, то есть ЕСПД применяется на добровольной основе (если иное не предусмотрено договором, контрактом, отдельными законами, решением суда и т. п.)

Ход работы

Задание 1. Прочитайте документ ЕСПД, выделите цель введения данных стандартов.

Выпишите основные разделы.

Задание 2. Определите области применения ЕСПД, пользователей ЕСПД.

Задание 3. Прочитайте ГОСТ 19.504-79, определите его область применения, цели введения данного стандарта.

Критерии оценивания:

- 5 баллов выставляется, если правильные ответы даны на 85-100% практических заданий
- 4 балла выставляется студенту, если правильные ответы даны на 65-84% практических заданий
- 3 балла выставляется студенту, если правильные ответы даны на 50-64% практических заданий
- 2 балла выставляется студенту, если правильные ответы даны на менее 50% практических заданий.

Тестовые задания:

1. Соотнести понятия и их определения

1.Программы	1) это данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализацииопределенного алгоритма
2.Программное средство	2) объект, состоящий из программ, процедур, правил и документов,относящихся к функционированию системы обработки информации
3.Программный продукт	3) это программное средство, предназначенное для поставки, передачи,продажи пользователю
4.ЖЦ ПП	4) это совокупность процессов, работ и задач, включающая в себя разработку, эксплуатацию и сопровождение ПС или системы, охватывающаяжизнь ПС или системы от 6 установления требований к ним до прекращенияих использования.

2. Выберете недостающее слово:

«Существует ряд национальных, государственных и международных__, посвященных вопросам стандартизации, оценки качества и сертификации программных средств и систем качества предприятия.»

1. Стандартов
2. Государственных услуг
3. Программных средств
4. Этапов ЖЦ

3. Впишите недостающее слово:

___– это совокупность свойств программного средства, обуславливающая его пригодность удовлетворять заданные или подразумеваемые потребности в соответствии с егоназначением.

4. Качество ПС отражается тремя группами показателей, характеризующими:

1. внутреннее, внешнее, качество при использовании
2. требуемое, обусловленное, реальное
3. номинальное, идеальное, реальное
4. определенное, достигнутое, недостигнутое

5. На чем основано определение ошибки?

1. на эталонном состоянии объекта
2. на случайном обнаружении ошибки
3. на поисковой деятельности
4. на явлении «back door»

6. Какие факторы влияют на степень качества программного средства?

1. качество технологий проектирования
2. качество разработки ПС
3. качество сопровождения
4. качество документирования

7. Вставьте пропущенное слово

__-средства поддерживают коллективную разработку сложных проектов, используются на этапе системного анализа, разработки технического задания и спецификаций, проектирования концептуальной и логической структур ПС и баз данных (БД), поддерживают автоматическую кодогенерацию и позволяют значительно снижать уровень системных, алгоритмических и программных ошибок при разработке ПО.

8. Вставьте пропущенное слово

_____является основным методом измерения качества, определения корректности, реальной надежности и безопасности функционирования программ на всех этапах ЖЦ ПС.

9. Выделите особенности процесса тестирования программ по отношению к тестированиюаппаратуры:

1. отсутствие эталонной программы, которой должны точно соответствовать все результаты тестирования
2. принципиальная невозможность использования полных тестовых наборов для

исчерпывающей проверки функционирования сложных ПС

3. относительно невысокая степень формализации критериев качества результатов тестирования и достигаемых при этом корректности и надежности функционирования испытуемых ПС

4. все ответы верны

10. Вставьте пропущенное слово:

Целью_____ПС является удостоверение их качества, надежности и безопасности применения

11. Результатом системного проектирования являются:

1. системный проект
2. техническое задание
3. договор на продолжение проектирования
4. выявление системных ошибок

12. Какими бывают первичные ошибки:

1. технологические ошибки
2. программные ошибки
3. алгоритмические ошибки
4. системные ошибки

13. Снижение трудоемкости, длительности проектов ПС, повышение качества разрабатываемых ПС, разработке, эксплуатации и сопровождении, обеспечение возможности расширять программное средство по набору прикладных функций и масштабировать в зависимости от размерности решаемых задач и другое являются:

1. целями применения стандартов
2. методами применения стандартов
3. поводами применения стандартов
4. заменой применения стандартов

14. Совокупность нескольких базовых стандартов и/или других нормативных документов с четко определенными и гармонизированными подмножествами обязательных и дополнительных возможностей, предназначенная для реализации заданной функции или группы функций – это:

1. профиль стандартов
2. группа стандартов
3. классификация стандартов
4. множества стандартов

15. Совокупность организационных структур, методик, технологий и ресурсов, необходимыхдля осуществления общего руководства качеством – это:

1. система качества
2. стандартизация
3. сертификация
4. метрология

Критерии оценивания:

- 5 баллов выставляется, если правильные ответы даны на 85-100% тестовых заданий
- 4 балла выставляется студенту, если правильные ответы даны на 65-84% тестовых заданий

- 3 балла выставляется студенту, если правильные ответы даны на 50-64% тестовых заданий
- 2 балла выставляется студенту, если правильные ответы даны на менее 50% тестовых заданий

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций состоит из текущего контроля.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации и учитываются при оценивании знаний, умений, навыков и (или) опыта деятельности.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

МДК 07.02 Сертификация информационных систем

Методические указания для студентов по освоению МДК являются частью рабочей программы МДК (РПД) (приложением к рабочей программе).

РПД − рабочая программа, утвержденная директором колледжа для изучения МДК. Она определяет цели и задачи МДК, формируемые в ходе ее изучения компетенции и их компоненты, содержание изучаемого материала, виды занятий и объем выделяемого учебного времени, а также порядок изучения и преподавания МДК.

Для самостоятельной учебной работы студента важное значение имеют разделы «Структура и содержание дисциплины (модуля)» и «Учебно-методическое и информационное обеспечение дисциплины (модуля)». В первом указываются разделы и темы изучаемой МДК, а также виды занятий и планируемый объем (в академических часах), во втором − рекомендуемая литература и перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Для подготовки к текущему контролю студенты могут воспользоваться оценочными средствами, представленными в Приложении 1 к рабочей программе МДК.

1. Описание последовательности действий студента

Приступая к изучению МДК необходимо в первую очередь ознакомиться с содержанием РПД, где в разделе «Структура и содержание дисциплины (модуля)» приведено общее распределение часов аудиторных занятий и самостоятельной работы по темам МДК.

Залогом успешного освоения МДК является регулярное посещение занятий и выполнение предусмотренных программой заданий. Пропуск одного, а тем более нескольких занятий может осложнить освоение разделов курса.

Лекции имеют целью дать систематизированные основы научных знаний по содержанию МДК. При изучении и проработке теоретического материала необходимо:

− повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

− при самостоятельном изучении теоретической темы подготовить конспект, используя рекомендованные в РПД литературные источники и электронные образовательные ресурсы.

Практические занятия проводятся с целью углубления и закрепления знаний, полученных на лекциях и в процессе самостоятельной работы с учебной литературой.

Обучающиеся выполняют одно или несколько практических заданий под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.

При подготовке к практическому занятию необходимо изучить или повторить лекционный материал по соответствующей теме.

2. Самостоятельная работа студента

Самостоятельная работа студента – самостоятельная учебная деятельность студента, организуемая колледжем и осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем.

Цели самостоятельной работы:

– систематизация и закрепление полученных теоретических знаний и практических умений студентов;

– углубление и расширение теоретических знаний;

– формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– воспитание самостоятельности, как личностного качества будущего специалиста.

Самостоятельная работа студента по МДК выполняется:

– самостоятельно вне расписания учебных занятий;

– с использованием современных образовательных технологий;

– работа со специальной литературой для подготовки к тестовым, практическим и лабораторным заданиям.

3. Рекомендации по работе с литературой и источниками

Работу с литературой следует начинать с анализа РПД, содержащей список основной и дополнительной литературы, а также знакомства с учебно-методическими разработками.

В случае возникновения затруднений в понимании учебного материала следует обратиться к другим источникам, где изложение может оказаться более доступным.

Работа с литературой не только полезна как средство более глубокого изучения МДК, но и является неотъемлемой частью профессиональной деятельности будущего выпускника.