

АНО СПО «КИТП»

Методические указания
по организации практических занятий
по дисциплине «Стандартизация, сертификация и техническое
документирование»

Специальность
09.02.07 Информационные системы и программирование

2023

АНО СПО «КИТП»

Методические рекомендации по учебной дисциплине «Стандартизация, сертификация и техническое документирование» разработаны с учетом ФГОСЗ среднего профессионального образования специальности 09.02.07 Информационные системы и программирование, предназначены для студентов и преподавателей колледжа.

Методические указания определяют этапы выполнения работы на практическом занятии, содержат рекомендации по выполнению индивидуальных заданий, а также список рекомендуемой литературы.

Составитель (автор): _____ преподаватель колледжа

Рассмотрены на заседании предметной (цикловой) комиссии специальности 09.02.07 Информационные системы и программирование

Протокол № от «30» июня 2023 г

Председатель ПЦК специальности _____
личная подпись инициалы, фамилия

и одобрены решением учебно-методического совета колледжа.

Протокол № ____ от «____» _____ 2023 г

Председатель учебно-методического совета колледжа

личная подпись

инициалы, фамилия

Рекомендованы к практическому применению в образовательном процессе.

ПРАКТИЧЕСКАЯ РАБОТА № 1 СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЦЕЛЬ РАБОТЫ: изучить международные и национальные стандарты и спецификации в области информационной безопасности.

Для проведения практической работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Практическая работа содержит отчет.

Отчет должен содержать:

- название и цель работы;
- формулировки практических упражнений;
- заполненные таблицы;
- вывод к практической работе;
- ответы на контрольные вопросы.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ 1: ознакомиться со стандартами и спецификациями в области информационной безопасности:

Руководящие документы Гостехкомиссии России;

- а) Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»;
- б) рекомендации X.800;
- в) «Оранжевая книга».

ПРАКТИЧЕСКОЕ ЗАДАНИЕ 2: заполнить таблицу 1 согласно распределению функций безопасности по уровням эталонной семиуровневой модели OSI.

Таблица 1 Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функция безопасности	Уровень						
	1	2	3	4	5	6	7
Аутентификация							
Управление доступом							
Конфиденциальность соединения							
Конфиденциальность вне соединения							
Избирательная конфиденциальность							
Конфиденциальность трафика							
Целостность с восстановлением							
Целостность без восстановления							
Избирательная целостность							
Целостность вне соединения							
Неотказуемость							

В клетках таблицы можно расположить следующие символы:
«+» данный уровень может предоставить функцию безопасности;

«-» данный уровень не подходит для предоставления функции безопасности.

Таблицу сохранить в отчёте.

Практическое задание 3: заполнить таблицу 2 согласно рекомендациям X.800.

Таблица 2 Взаимосвязь функций и механизмов

Функция	Механизм							
	шифрование	электронная подпись	управление доступом	целостность	аутентификация	дополнение трафика	управление маршрутизацией	ногаризация
Аутентификация партнёров								
Аутентификация источника								
Управление доступом								
Конфиденциальность								
Избирательная конфиденциальность								
Конфиденциальность трафика								
Целостность соединения								
Целостность вне соединения								
Неотказуемость								

В клетках таблицы можно расположить следующие символы:

«+» механизм пригоден для реализации данной функцию безопасности;

«-» механизм не предназначен для реализации данной функции безопасности.

Таблицу сохранить в отчёте.

Практическое задание 4: заполнить таблицу 3 согласно руководящим документам Гостехкомиссии России.

Таблица 3 Требования к защищенности автоматизированных систем

АНО СПО «КИТП»

Подсистема и требования	Класс								
	ЗБ	ЗА	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом.									
1.1. Идентификация. Проверка подлинности и контроль доступа субъектов в систему:									
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ									
к программам									
к томам, каталогам, файлам, записям, полям записей									
1.2. Управление потоками информации									
2. Подсистема регистрации и учета.									
2.1.Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети)									
выдачи печатных (графических) выходных документов									
запуска/завершения программ и процессов (заданий, задач)									

5

Подсистема и требования	Класс								
	ЗБ	ЗА	2Б	2А	1Д	1Г	1В	1Б	1А
доступа программ к терминалам ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, каталогам, файлам, записям, полям записей									
изменения полномочий субъектов доступа создаваемых защищаемых объектов доступа									
2.2. Учет носителей информации									
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей									
2.4. Сигнализация попыток нарушения защиты									
3. Криптографическая подсистема.									
3.1. Шифрование конфиденциальной информации									
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) "на разных ключах									
3.3. Использование аттестованных (сертифицированных) криптографических средств									
4. Подсистема обеспечения целостности.									
4.1. Обеспечение целостности программных средств и обрабатываемой информации									
4.2. Физическая охрана средств вычислительной техники и носителей информации									
4.3. Наличие администратора (службы) защиты информации в АС									
4.4. Периодическое тестирование СЗИ НСД									
4.5. Наличие средств восстановления СЗИ НСД									
4.6. Использование сертифицированных средств защиты									

В клетках таблицы можно расположить следующие символы:

«+» – требование к данному классу присутствует;

«-» – требование к данному классу отсутствует.

Таблицу сохранить в отчёте.

Выводы

Контрольные вопросы

- 1 Чем характеризуется уровень безопасности «А» согласно «Оранжевой книге»?
- 2 Чем характеризуется уровень безопасности «С» согласно «Оранжевой книге»?
- 3 На каком уровне может быть реализована аутентификация согласно рекомендациям X.800?
- 4 На каком уровне может быть реализована целостность с восстановлением согласно рекомендациям X.800?

ПРАКТИЧЕСКАЯ РАБОТА №2. СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА

ЦЕЛЬ РАБОТЫ: ознакомиться с системами менеджмента качества, стандартами в области системы менеджмента качества.

Для проведения практической работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Практическая работа содержит отчет.

Отчет должен содержать:

- название и цель работы;
- формулировки практических упражнений;
- вывод к практической работе;
- ответы на контрольные вопросы.

Практическое задание

1 Закодировать в соответствии с ТН ВЭД следующую продукцию:

- а) микроконтроллер;
- б) процессор ПК;
- в) блок питания для ПК;
- г) монитор.

2 Используя указатель государственных стандартов, определить стандарты на указанную продукцию.

3 Установить требования к данным видам продукции.

4 Провести анализ типовых схем сертификации для данной продукции.

5 Разработать план по подготовке к сертификации данной продукции.

Выводы

Контрольные вопросы

- 1 Что включает в себя менеджмент качества?
- 2 Охарактеризуйте управление качеством, как составной части менеджмента качества.
- 3 На что направлено планирование качества, как составной части менеджмента качества?
- 4 Что используется в контроле качества, как составной части менеджмента качества?
- 5 Перечислите основные типы показателей качества.

ПРАКТИЧЕСКАЯ РАБОТА №3. НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЦЕЛЬ РАБОТЫ: ознакомиться с нормативно-правовыми документами и стандартами в области защиты информации и информационной безопасности.

Для проведения практической работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Практическая работа содержит отчет.

Отчет должен содержать:

- название и цель работы;
- формулировки практических упражнений;
- заполнение таблицы;
- вывод к практической работе;
- ответы на контрольные вопросы.

Практическое задание

1 Провести сравнение стандартов: «Руководящие документы ГТК» и «Единые критерии безопасности информационных технологий».

2 Ознакомиться с нормативно-правовыми документами и стандартами в области криптографии и шифрования.

3 Заполнить в таблице 4 «Криптографическое закрытие информации» столбец «Способ реализации», указав способ реализации: аппаратный, программный или аппаратно-программный.

Таблица 4 Криптографическое закрытие информации

Вид преобразований	Способ преобразования	Разновидность способа	Способ реализации	
Шифрование	Замена (подстановка)	Простая (одноалфавитная)		
		Многоалфавитная одноконтурная обыкновенная		
		Многоалфавитная одноконтурная монофоническая		
		Многоалфавитная многоконтурная		
	Перестановка	Простая		
		Усложненная по таблице		
		Усложненная по маршрутам		
	Аналитическое преобразование	По правилам алгебры матриц		
		По особым зависимостям		
	Гаммирование		С конечной короткой гаммой	
			С конечной длинной гаммой	
			С бесконечной гаммой	
	Комбинированные	Замена+перестановка		

		Замена+гаммирование	
		Перестановка+	
		гаммирование	
		Гаммирование+гаммирование	
Кодирование	Смысловое	По специальным таблицам	
		(словарям)	
	Символьное	По кодовому алфавиту	
Другие виды	Рассечение-	Смысловое	
	разнесение		
		Механическое	
	Сжатие-		
	расширение		

Таблицу сохранить в отчёте.

4 Сравнить алгоритмы шифрования: хэширования, цифровой подписи по размеру ключа, размеру файла, скорости работы.

5 Определите время перебора всех паролей, состоящих из 6 цифр при скорости перебора 10 паролей в секунду.

6 Определите минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет при скорости перебора 10 паролей в секунду.

Выводы

Контрольные вопросы

1 Охарактеризуйте симметричные алгоритмы шифрования.

2 В чём отличие потоковых и блочных шифров.

3 Перечислите требования к выбору и использованию паролей.

4 Перечислите и охарактеризуйте основные типы политики безопасности.

ПРАКТИЧЕСКАЯ РАБОТА №4. ОСНОВНЫЕ ВИДЫ ТЕХНИЧЕСКОЙ И ТЕХНОЛОГИЧЕСКОЙ ДОКУМЕНТАЦИИ

Цель работы: ознакомиться с основными видами технической и технологической документации.

Для проведения практической работы используется следующее обеспечение: персональный компьютер, подключённый к Интернету.

Практическая работа содержит отчет.

Отчет должен содержать:

Отчет должен содержать:

-название и цель работы;

-формулировки практических упражнений;

- вывод к практической работе;

-ответы на контрольные вопросы.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ

- 1 Ознакомиться с теоретическими материалами по разделам «Классификаторы» и «Национальная система стандартизации РФ».
- 2 Освоить способ идентификации новых разработок согласно ГОСТ 2.201
- 3 Ознакомиться с классами 06, 27, 44, 62,69,70 классификатора ЕСКД.
- 4 Используя Общероссийский классификатор изделий и конструкторских документов, в соответствии с ГОСТ 2.201 присвоить обозначение изделиям:
 - а) «Анализаторы радиоспектрометрические с измерением амплитуды СВЧ колебаний»;
 - б) «Устройства логического управления с линейно-рассосредоточенными параметрами»;
 - в) «Многофункциональная система регулирования параметров технологических процессов программно-логического управления»;
 - г) «Средство телемеханики программного управления по радиоканалу».
- 5 Выделить в полученном обозначении выбранный по ОК ЕСКД код классификационной характеристики, используя соответствующую часть классификатора ЕСКД. Проанализировать и расписать ее структуру для исследуемого объекта с указанием выявленных существенных признаков классификации (класс, подкласс, группа, подгруппа, вид).
- 6 Приведите классификацию и обозначение технологических документов.
- 7 Привести характеристики стадий разработки технологической документации.

Выводы

Контрольные вопросы

- 1 Какой орган допускает ОК к использованию на территории РФ?
- 2 Как взаимосвязаны ОК ЕСКД и ГОСТ 2.201?
- 3 Какую информацию заключают в себе части обозначения изделия, разделенные точками в соответствии со структурой обозначения изделия, приведенной в ГОСТ 2.201?
- 4 Этапы технологического процесса сборки изделия.

Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Каждому обучающемуся обеспечен доступ к следующим электронным библиотечным системам и профессиональным базам данных:

- ЭБС «Университетская библиотека онлайн».

Электронная библиотека ежегодно обновляется и пополняется.