|  |  |
| --- | --- |
| http://www.pl130.ru/doc/index/%D0%9B%D0%BE%D0%B3%D0%BE%D1%82%D0%B8%D0%BF22.jpg | Санкт-Петербургское государственное бюджетное  профессиональное образовательное учреждение  "Колледж электроники и приборостроения" |

отчет

**по практической работе №1**

**по дисциплине «Стандартизация, сертификация и техническое документирование»**

Тема: Использование сервисных программ поддержки интерфейсов. Настройка рабочего стола

|  |  |  |
| --- | --- | --- |
| Студент гр. 13 ИТ |  | Липинский К.С. |
| Преподаватель |  | Петухова М.В. |

Санкт-Петербург

2023

**Цель работы**

Изучить международные и национальные стандарты и спецификации в области информационной безопасности.

**Оборудование**

Персональный компьютер, подключённый к Интернету.

**Ход работы**

* **Задание 1**

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Перечислить стандарты в области ИБ | Перечислить базовые сервисы безопасности для систем | Перечислить механизмы управления доступом |
|  | «Оранжевая книга» | 1. Мандатное управление доступом 2. Обязательная аутентификация 3. Уровни доступа 4. Аудит безопасности 5. Защита данных 6. Физическая безопасность 7. Защита ПО 8. Защита от вредоносного кода | 1. Политики безопасности 2. Дискретное управление доступом 3. Аудит доступа 4. Обязательное управление доступом на основе меток 5. Ролевое управление доступом 6. Мандатное управление доступом |
|  | рекомендации X.800 | 1. Аутентификация 2. Конфиденциальность 3. Целостность 4. Недоступность 5. Учёт и аудит 6. Криптография 7. Контроль доступа 8. Физическая безопасность | 1. Идентификация и аутентификация 2. Авторизация 3. Аудит доступа 4. Контроль доступа на основе ролей 5. Криптографические механизмы |
|  | Стандарт ISO/IEC 15408 | 1. Идентификация и аутентификация 2. Аудит 3. Конфиденциальность 4. Целостность 5. Невозможность отказа в обслуживании 6. Управление доступом 7. Криптография 8. Защита от вредоносного кода | 1. Модели доступа (ACL, AM, MAC, MLS) 2. Мандатный контроль доступа 3. Политики безопасности 4. Механизмы аутентификации 5. Ролевое управление доступом 6. Аудит доступа 7. Контроль доступа на основе контекста |

* **Задание 2**

|  |  |  |
| --- | --- | --- |
| №п/п | Вопросы для ответа | Положения стандарта |
| 1. | Название стандарта | Информационная технология  ОЦЕНКА ПРОГРАММНОЙ ПРОДУКЦИИ  Характеристики качества и руководства по их применению |
| 2. | Кем подготовлен, внесен и принят ГОСТ ИСО/МЭК 9126—2001 | ЕВРАЗИИСКИИ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (ЕАСС) |
| 3. | Идентичен стандарту | ГОСТ Р ИСО/МЭК 9126-93 |
| 4. | Модель процесса оценивания | 1. Установление (определение) требований к качеству 2. Подготовка к оцениванию 3. Процедура оценивания |
| 5. | Требования к качеству | Целью начальной стадии является установление требований в терминах характеристик качества и возможных комплексных показателей (подхарактеристик). Требования выражают потребности внешнего окружения для рассматриваемой программной продукции и должны быть определены до начала разработки. Так как программная продукция разделяется на основные компоненты, требования для продукции в целом могут отличаться от требований для отдельных компонентов. |
| 6. | Выбор метрик качества | Способ, которым определялись характеристики качества, не допускает их непосредственного измерения. Существует потребность в установлении метрик (показателей), которые соотносятся с характеристиками программной продукции. Каждый количественный признак и каждое количественно оцениваемое взаимодействие программного обеспечения с его окружением, которые соотносятся с характеристикой, могут быть приняты в качестве метрики (показателя).  Метрики могут по-разному зависеть от окружения и фаз процесса разработки, в которых они используются. Метрики, используемые в процессе разработки, должны быть соотнесены с соответствующими метриками пользователя, потому что метрики из представления пользователя являются решающими. |
| 7. | Уровни ранжирования | Отличный  Хороший  (Удовлетворительно)  Низкий  (Неудовлетворительно) |
| 8. | Процедура оценивания:  «измерение»  «ранжирование»  «оценка» | Для измерения выбранные метрики применяются к программной продукции. Результатом являются значения в масштабах метрик.  Ранжирование  На этапе ранжирования устанавливается уровень ранжирования для измеренного значения.  Оценка является последним этапом процесса оценивания программного обеспечения, на котором обобщается множество установленных уровней. Результатом является заключение о качестве программной продукции. Затем обобщенное качество сравнивается с другими факторами, такими как время и стоимость. Окончательное решение руководства принимается на основе критерия управляемости. Результатом является решение руководства по приемке или отбраковке, или по выпуску или невыпуску программной продукции. |
| 9. | Комплексные показатели качества | 1. Функциональные возможности 2. Пригодность 3. Правильность 4. Способность к взаимодействию 5. Согласованность 6. Защищённость 7. Надёжность 8. Стабильность 9. Устойчивость к ошибкам |

**Контрольные вопросы**

1. **Чем характеризуется уровень безопасности «А» согласно «Оранжевой книге»?**
2. реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;
3. представлены формальные спецификации верхнего уровня; используются современные методы формальной спецификации и верификации систем;
4. механизм управления конфигурациями распространяется на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;
5. описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.
6. **Чем характеризуется уровень безопасности «С» согласно «Оранжевой книге»?**
7. доверенная база управляет доступом именованных пользователей к именованным объектам;
8. пользователи четко идентифицируют себя;
9. аутентификационная информация пользователей защищена от несанкционированного доступа;
10. доверенная вычислительная база имеет изолированную область для собственного выполнения, защищенную от внешних воздействий;
11. есть в наличии аппаратные или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
12. защитные механизмы протестированы на отсутствие способов обхода или разрушения средств защиты доверенной вычислительной базы;
13. описаны подход к безопасности и его применение при реализации

доверенной вычислительной базы.

1. **На каком уровне может быть реализована аутентификация согласно рекомендациям Х.800?**

На сетевом, транспортном и прикладном уровнях

1. **На каком уровне может быть реализована целостность с восстановлением согласно рекомендациям Х.800?**

На транспортном и прикладном уровнях