1. Анализ известных мер разработки безопасного ПО
2. Определение базового набора требований к разработке безопасного ПО
3. Концептуальная модель выбора мер разработки безопасного ПО
4. Разработка концептуальной модели анализа и синтеза мер разработки безопасного ПО
5. Оценка эффективности: уязвимости ПО, выявляемые при проведении сертификации
6. Разработка программ с помощью объектно-ориентированного программирования C++
7. Разработка программ с помощью объектно-ориентированного программирования Python
8. Разработка программ с помощью объектно-ориентированного программирования Java
9. Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире
10. Международный стандарт ISO 17799
11. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении проектирования архитектуры программы
12. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении конструирования и комплексирования программного обеспечения
13. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении квалификационного тестирования программного обеспечения
14. Регламент отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы
15. Регламент приема и обработки сообщений от пользователей об ошибках ПО и уязвимостях программы.
16. Актуальность вопросов тестирования безопасности и защищённости программных продуктов»
17. Security Development Life Cycle (SDLC)
18. Практика применения SDL
19. Требования к безопасной разработке ПО согласно приказу ФСТЭК №31
20. Классификация угроз для программного обеспечения
21. Модель защиты внутренних сетевых ресурсов на предприятии
22. Исследование проблем безопасности при разработке компьютерных игр
23. Криптографические уязвимости в Web – приложениях