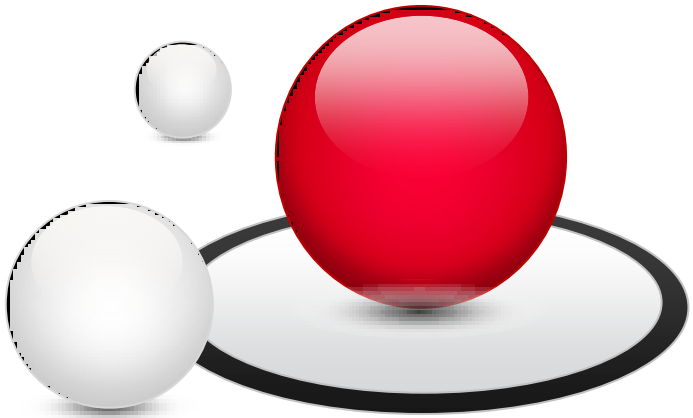
Эшелон
комплексная безопасность

Что значит сертификация по требованиям безопасности информации для компании-разработчика?

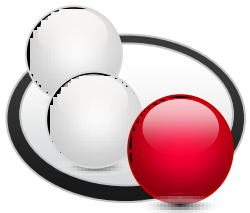


Марков Алексей
Фадин Андрей

НПО «Эшелон».
2012

План выступления

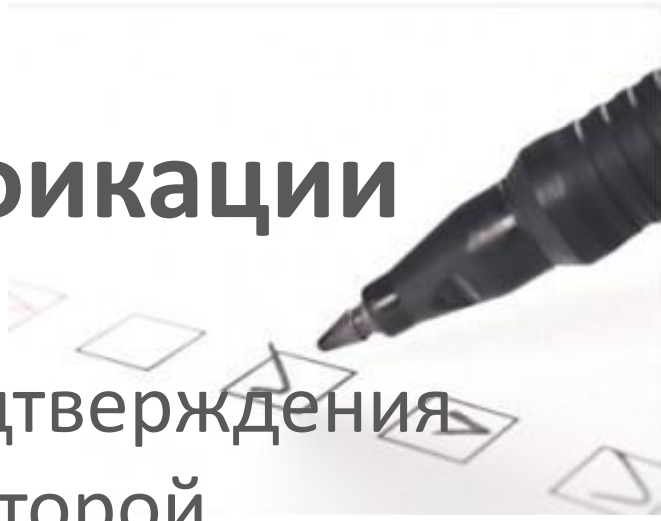
- Системы сертификации средств защиты информации по требованиям безопасности информации
- Особенности сертификационных испытаний



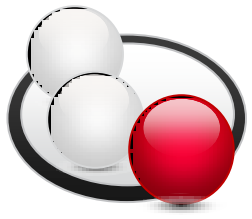
Эшелон
комплексная безопасность

СИСТЕМЫ СЕРТИФИКАЦИИ СЗИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Понятие сертификации



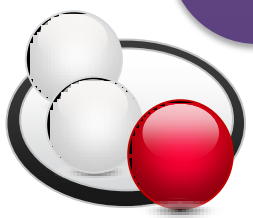
Сертификация – процесс подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме (сертификат), что продукция соответствует установленным требованиям.



Что дает сертификация?

Выход на IT-рынок

- Выполнение требований законодательства
- Дополнительный аудит процессов жизненного цикла, а также самого продукта
- Конкурентное преимущество



Обязательность сертификации по требованиям безопасности

Информационный ресурс	Государственная тайна	Личная, семейная тайна	Другие тайны	Открытая общедоступная информация
Государственный информационный ресурс	Да	Да	Да	Для систем общего пользования и для специфических систем
Негосударственный информационный ресурс	-	Да	Только для специфических систем	Только для специфических систем

Системы обязательной сертификации по требованиям безопасности информации

ФСБ России

- Средства криптографической защиты
- ИС высших органов исполнительной власти

Минобороны России

- Объекты ВС РФ

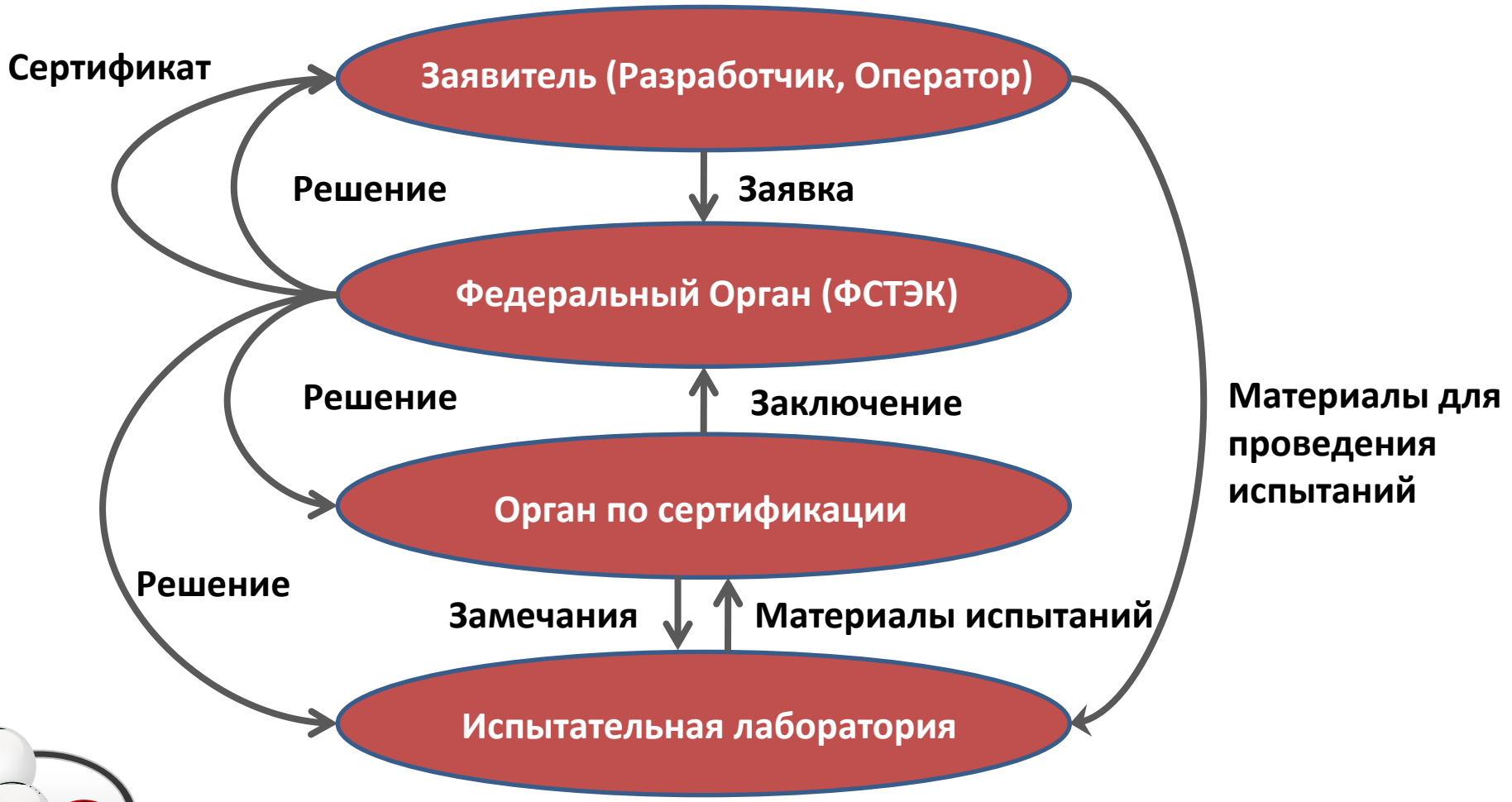
ФСТЭК России (Гостехкомиссия России)

- Средства защиты информации некриптографическими методами

СВР России

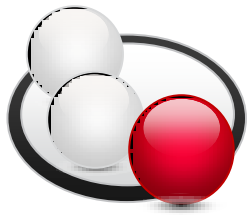
- Объекты в зарубежных представительствах РФ

Участники сертификационного процесса



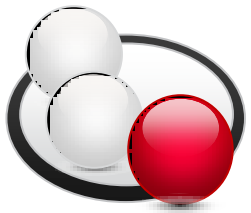
Виды сертификационных испытаний

- ***Структурное тестирование (требуются исходные тексты)***
  - На соответствие уровню контроля отсутствия недекларированных возможностей (программных закладок)
- ***Функциональное тестирование:***
  - На соответствие классу защищенности (определяется требованиями нормативных документов регуляторов)
  - На соответствие конструкторской/эксплуатационной документации (ТУ, формуляр и др.)
  - На соответствие заданию по безопасности (при сертификации по линии ОК) – может быть ссылка на контроль отсутствия НДВ



Схемы сертификации

- Единичный образец
- Партия
- Типовой образец с проверкой производства (серийное производство)



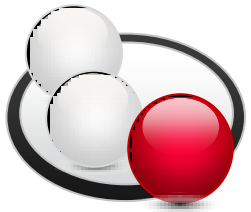
Что на выходе? Содержимое сертификата

Главное:

- Идентификационные характеристики ПО
- На соответствие каким нормативным документам проведено испытание
- Схема сертификации
- Время действия

Что еще?

- Ссылка на документ с контрольными суммами
- Ссылка на документ с ограничениями по использованию
- Порядок маркировки



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2418

Выдан 25 августа 2011 г.
Действителен до 25 августа 2014 г.

Настоящий сертификат удостоверяет, что **операционная система Microsoft Windows 7 OEM в редакции «Профессиональная»**, разработанная компанией Microsoft Corporation, производимая и поставляемая ООО «ГЕЛИОС КОМПЬЮТЕР» и ООО «Сертифицированные информационные системы», является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по **5** классу защищенности и может использоваться при создании автоматизированных систем до класса защищённости **1Г** включительно и при создании информационных систем персональных данных до **2** класса включительно при выполнении ограничений, указанных в приложении к настоящему сертификату.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 24.05.2006 № СЗИ RU.304.Б07.022) – техническое заключение от 24.05.2011, и экспертного заключения от 14.07.2011 органа по сертификации ООО «Научно-испытательный институт систем обеспечения комплексной безопасности» (аттестат аккредитации от 26.11.2008 № СЗИ RU.2262.А99.012).

Заявитель: ООО «ГЕЛИОС КОМПЬЮТЕР»
Адрес: 111250, Солдатская ул., д. 6, г. Москва
Телефон: (495) 969-2400

Заявитель: ООО «Сертифицированные информационные системы»
Адрес: 115201, г. Москва, 2-й Котляковский переулок, д. 1, стр. 3
Телефон: (495) 229-5607

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанного в настоящем сертификате руководящего документа осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
25 августа 2011 г.

Эшелон
комплексная безопасность

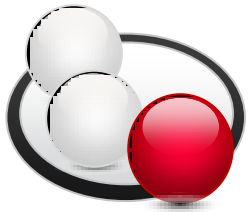
ОСОБЕННОСТИ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

ПОРЯДОК СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

- Отбор образца
- Проведение испытаний:
  - Структурное тестирование (пример: НДВ)
  - Функциональное тестирование (пример: НСД)
- Оформление материалов
- Согласование и экспертиза в органе по сертификации

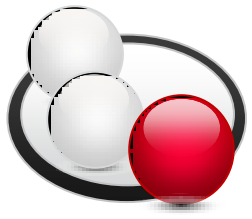
Отбор образца. Основные артефакты

- Документация
- Дистрибутив
- Исходные тексты



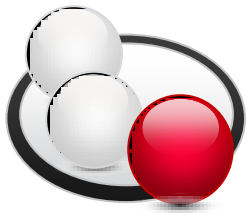
Отбор образца: подводные камни

- Конфиденциальность передаваемых материалов
  - Внутренние регламенты компаний-разработчиков
    - Соглашение о неразглашении (NDA)
    - Внутренний аудит итоговых материалов испытательной лаборатории и их фильтрация (пример: исключение фрагментов исходных текстов)
  - Требования законодательства (пример: trade compliance)
- Полнота предоставленных материалов
  - Примеры: отсутствие программных компонентов, отдельных типов документов и др.
- Соответствие материалов требованиям испытательной лаборатории и органа по сертификации
  - Примеры: иностранный язык в документации, её несоответствие ГОСТам, недостаточно подробный лог сборки и пр.



Подходы по обеспечению доступа испытательной лаборатории к материалам образца

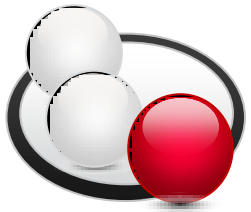
1. Полное проведение сертификации на территории испытательной лаборатории в РФ.
2. Доступ к материалам образца на территории российской компании (филиала иностранной компании).
3. Доступ к материалам образца на территории иностранной компании.



Проведение испытаний: контроль отсутствия НДВ

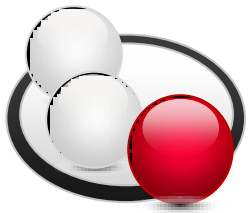
- Недекларированные возможности (НДВ) - функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Руководящий документ Гостехкомисии РФ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»



Контроль отсутствия НДВ

1. Контроль состава и содержания документации
2. Контроль исходного состояния ПО
3. Статический анализ исходных текстов программ
4. Динамический анализ исходных текстов программ
5. Отчетность

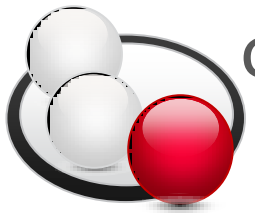


Контроль состава и содержания документации

Выполняемые проверки	Уровень контроля			
	4	3	2	1
1.Контроль состава и содержания документации				
Спецификация (ГОСТ 19.202-78)	+	=	=	=
Описание программы (ГОСТ 19.402-78)	+	=	=	=
Описание применения (ГОСТ 19.502-78)	+	=	=	=
Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
Исходные тексты программ (ГОСТ 19.401-78)	+	=	=	=

Контроль состава и содержания документации

- Основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО)
- Основные сведения о назначении компонентов, входящих в состав ПО, параметрах обрабатываемых наборов данных (подсхемах баз данных), формируемых кодах возврата, описание используемых переменных, алгоритмов функционирования.

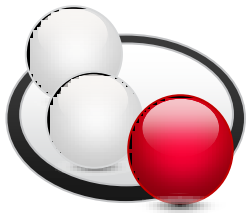


Контроль исходного состояния

Выполняемые проверки	Уровень контроля			
	4	3	2	1
2.Контроль исходного состояния	+	=	=	=

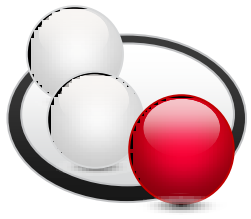
Контроль исходного состояния ПО

- Дистрибутив
- Исполняемые модули ПО
- Исходные тексты
  - Заимствованные компоненты
  - «Мертвый код»
- Информация по сторонним компонентам
  - Наименование
  - Разработчик
  - Назначение
  - Список модулей



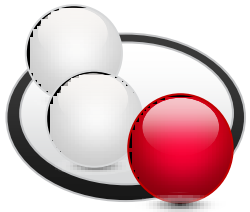
Требования к сборке ПО

- Сборочный стенд
  - Обеспечение полного цикла компиляции и сборки
  - Обеспечение сетевой изоляции сборочного стенда
  - Возможности по установке дополнительных средств аудита
- Документация на сборочный стенд
  - Аппаратная конфигурация стенда
  - Программная конфигурация инструментов сборки (компиляторы, линковщики, обфускаторы, оптимизаторы, IDE, CVS, системы управления сборкой)



Виды исследуемых сборок программных проектов

- Официальный дистрибутив (RTM, COTS)
- Контрольная сборка (lab build)
- Исследовательские сборки
  - По исходному коду с датчиками динамического анализа
  - По исходному коду с датчиками использования файлов
  - С контролем обращений к ресурсам
  - В отладочном режиме



3.Статический анализ исходных текстов программ

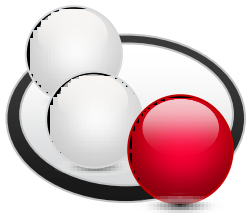
Выполняемые проверки	Уровень контроля			
	4	3	2	1
3. Статический анализ исходных текстов программ				
3.1.Контроль отсутствия избыточности исходных текстов	+	+	+	=
3.2.Контроль соответствия исходных текстов загрузочному коду	+	=	=	+
3.3.Контроль связей функциональных объектов по управлению	-	+	=	=
3.4.Контроль связей функциональных объектов по информации	-	+	=	=
3.5.Контроль информационных объектов	-	+	=	+
3.6.Контроль наличия заданных конструкций	-	-	+	+
3.7.Формирование перечня маршрутов выполнения ФО	-	+	+	=
3.8.Анализ критических маршрутов выполнения ФО	-	-	+	=
3.9.Анализ алгоритма работы на основе блок-схем, построенных по исходным текстам контролируемого ПО	-	-	+	=

Статический анализ

- объекты исследования
  - исходные тексты ПО
  - исполняемый код ПО
  - артефакты производства ПО (отладочная информация, логи сборки, вывод при работы внешних средств)
  - параметры программного проекта (проектные файлы, манифесты)
- особенности подхода
  - не требует запуска ПО
  - ограниченный набор проверяемых свойств ПО (проблема «останова», теорема Райса)
  - сложность анализа нелинейно возрастает с ростом объема анализируемого ПО

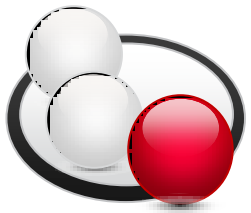
Контроль полноты и отсутствия избыточности исходных текстов

- Полнота исходных текстов
  - Заимствованные компоненты
  - Предкомпилированные компоненты
- Избыточность исходных текстов
  - «Мертвый код»
  - Устаревшие компоненты (бинарные модули)



Виды контроля соответствия исходных текстов ПО его объектному (загрузочному) коду в процессе сборки приложения

- Основной: сертификация контрольной сборки
- Сертификация RTM-релиза при установлении эквивалентности с контрольной сборкой



Виды контроля соответствия исходных текстов ПО его объектному (загрузочному) коду в процессе сборки приложения

Структурный (статический) анализ исходных текстов программ

Выполняемые проверки	Уровень контроля			
	4	3	2	1
3. Статический анализ исходных текстов программ				
3.1.Контроль отсутствия избыточности исходных текстов	+	+	+	=
3.2.Контроль соответствия исходных текстов загрузочному коду	+	=	=	+
3.3.Контроль связей функциональных объектов по управлению	-	+	=	=
3.4.Контроль связей функциональных объектов по информации	-	+	=	=
3.5.Контроль информационных объектов	-	+	=	+
3.6.Контроль наличия заданных конструкций	-	-	+	+
3.7.Формирование перечня маршрутов выполнения ФО	-	+	+	=
3.8.Анализ критических маршрутов выполнения ФО	-	-	+	=
3.9.Анализ алгоритма работы на основе блок-схем, построенных по исходным текстам контролируемого ПО	-	-	+	=

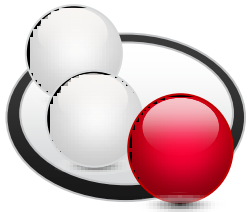
Контроль наличия заданных конструкций в исходных текстах

- Синтаксический
- Семантический

Выполняемые проверки	Уровень контроля			
	4	3	2	1
3. Статический анализ исходных текстов				
3.1.Контроль отсутствия избыточности исходных текстов	+	+	+	=
3.2.Контроль соответствия исходных текстов загрузочному коду	+	=	=	+
3.3.Контроль связей функциональных объектов по управлению	-	+	=	=
3.4.Контроль связей функциональных объектов по информации	-	+	=	=
3.5.Контроль информационных объектов	-	+	=	+
3.6.Контроль наличия заданных конструкций	-	-	+	+
3.7.Формирование перечня маршрутов выполнения ФО	-	+	+	=
3.8.Анализ критических маршрутов выполнения ФО	-	-	+	=
3.9.Анализ алгоритма работы на основе блок-схем, построенных по исходным текстам контролируемого ПО	-	-	+	=

Потенциально опасные конструкции

- Программные закладки
  - Логические бомбы
  - Backdoor/trapdoor (пароли по умолчанию)
  - Скрытые каналы
- Дефекты кода
  - SQL-инъекция
  - Переполнения буфера
  - Злоупотребления API

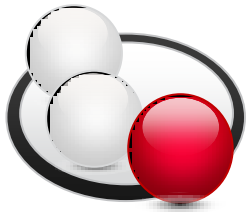


Задачи, представления кода и методы статического анализа

Представление кода/ Решаемые задачи	Декомпозиция и анализ структуры программы	Проверка стиля, подсчет метрик	Проверка свойств программы	Поиск багов/дефектов по шаблону
Исходные тексты программного обеспечения	Контроль зависимостей на уровне компонентов и отдельных файлов проекта	Подсчет базовых метрик (LOC и т.п.)	Свойста по недоступны	Поиск сигнатур по регулярным выражениям (реализации на основе grep, sed)
Абстрактное синтаксическое дерево (AST)	Лексический и синтаксический анализ	Лексический и синтаксический анализ	Лексический и синтаксический анализ	Лексический и синтаксический анализ, Поиск сигнатур по AST
Абстрактный семантический граф (ASG): Поток управления (control flow)	Определение связей объектов в иерархии	Подсчет метрик связности	Анализ потока выполнения (control flow)	Поиск сигнатур последовательностей инструкций
ASG: Поток данных (data flow)	Определение зависимостей по данным	Подсчет метрик связности	Абстрактная интерпретация (abstract interpretation): Интервальный анализ Анализ указателей Анализ зависимостей по данным	Анализ потока данных (data flow) Поиск внутрипроцедурных сигнатур последовательностей инструкций с учетом передаваемых значений

Задачи, представления и методы статического анализа

Представление кода/ Решаемые задачи	Декомпозиция и анализ структуры программы	Проверка стиля, подсчет метрик	Проверка свойств программы	Поиск багов/дефектов по шаблону
ASG: Межпроцедурный анализ (interprocedural analysis)	Не требуется	Подсчет метрик связности	Анализ на основе систем уравнений	Поиск сигнатур с учетом связей между процедурами
ASG: Семантические описания конструкций (например вызовов внешних API)	Не требуется	Подсчет метрик связности с учетом семантики	Абрстрактная интерпретация Ресурный анализ Темпоральная логика	Поиск сигнатур на основе семантической базы конструкций Темпоральная логика
ASG: Формальные методы верификации	Не требуется	Не требуется	Дедуктивная верификация	Не требуется

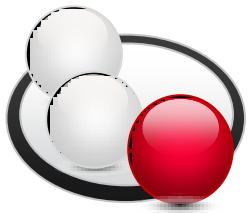


Динамический анализ исходных текстов программ

Выполняемые проверки	Уровень контроля			
	4	3	2	1
4 Динамический анализ исходных текстов программ				
4.1.Контроль выполнения функциональных объектов	-	+	+	=
4.2.Сопоставление фактических маршрутов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=

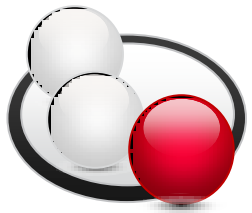
Динамический анализ исходных текстов программ

1. Вставка датчиков в исходные тексты продукта
2. Полная пересборка исходных текстов продукта со вставленными датчиками
3. Функциональное тестирование собранного дистрибутива, сбор лога отработки датчиков
4. Сопоставление трасс из лога отработки датчиков с данными статического анализа



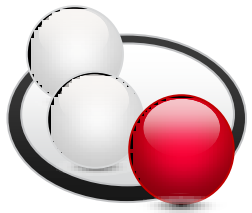
Спорные аспекты

- Документация
  - формализация требований для сопоставления с данными анализа кода
- Отчеты
  - Контроль связей функциональных объектов по управлению, по информации. Контроль информационных объектов.
  - Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО



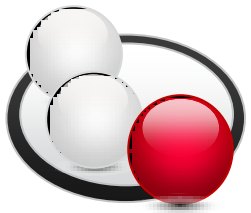
Спорные аспекты

- Формирование перечня маршрутов выполнения функциональных объектов, определение понятия «маршрут»;
- Контроль выполнения функциональных объектов
- Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа



Обоснованные требования

- Контроль полноты и отсутствия избыточности исходных текстов
- Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду
- Контроль наличия заданных конструкций в исходных текстах



Недостатки РД по НДВ:

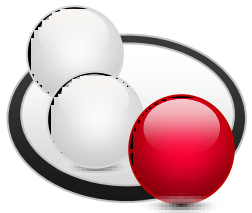
- в документе есть ссылка на базу уязвимостей, но отсутствуют требования к ее содержанию и их описаниям
- большинство методов, используемых в документе «пришли» из теории надежности, в контексте анализа современных программных систем они часто трудновыполнимы из-за высокой сложности
- статистика проведения аудитов исходных текстов показывает, что подавляющее большинство уязвимостей найдены с помощью сигнатурного поиска, а не структурного анализа
- недостаточно четкие определения (маршрут, ветвь)
- отсутствие единого стандарта по вычислению и сравнению контрольных сумм, не используются ЭЦП
- В документе не регламентированы крайне важные параметры:
  - необходимый уровень покрытия при динамическом анализе
  - используемую базу уязвимостей
  - допустимую меру избыточности кода

Положительные моменты РД по НДВ

- Контроль и дополнительный аудит ряда процессов жизненного цикла в первую очередь связанных со сборкой и деплойментом продукта
- Выполнение некоторых практик SDL Process:
  - Явное:
    - SDL Practice #8: Use Approved Tools
    - SDL Practice #10: Perform Static Analysis
    - SDL Practice #11: Perform Dynamic Analysis
    - SDL Practice #16: Release/Archive
  - Неявное:
    - SDL Practice #7: Threat Modeling
    - SDL Practice #12: Fuzz Testing

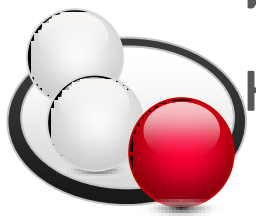
Перспективы развития нормативной базы

- Документация
  - формализация требований для сопоставления с данными анализа кода
- Статический анализ
  - Сигнатурный анализ
    - национальный репозиторий дефектов кода
    - требования к базе сигнатур
  - Проверка свойств на модели
- Динамический анализ
  - Требования к покрытию
  - Подход включающий и контроль выполнения ФО, и фазинг входных данных



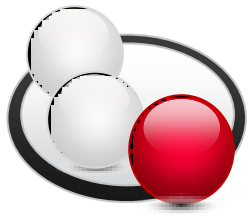
Заключение

- В последние годы произошел стремительный рост иностранных сертификаций
- Несмотря на определенные ограничения нормативной базы и устаревание ряда требований, практика показала практическую возможность успешного проведения сертификационных испытаний даже таких крупных продуктов как операционные системы



Источники

1. Нормативные и методические документы по технической защите информации. Специальные нормативные документы: официальный сайт ФСТЭК России. – URL: http://www.fstec.ru/_razd/_karto.htm
2. Выявление уязвимостей в программном коде / Марков А.С., Миронов С.В., Цирлов В.Л. // Открытые системы. СУБД. 2005. № 12. С.64-69.
3. Сертификация программ: мифы и реальность / Марков А.С., Цирлов В.Л. // Открытые системы. СУБД. 2011. № 6. С.26-29.



Спасибо за внимание!

Контакты докладчиков:

mail@cnpo.ru