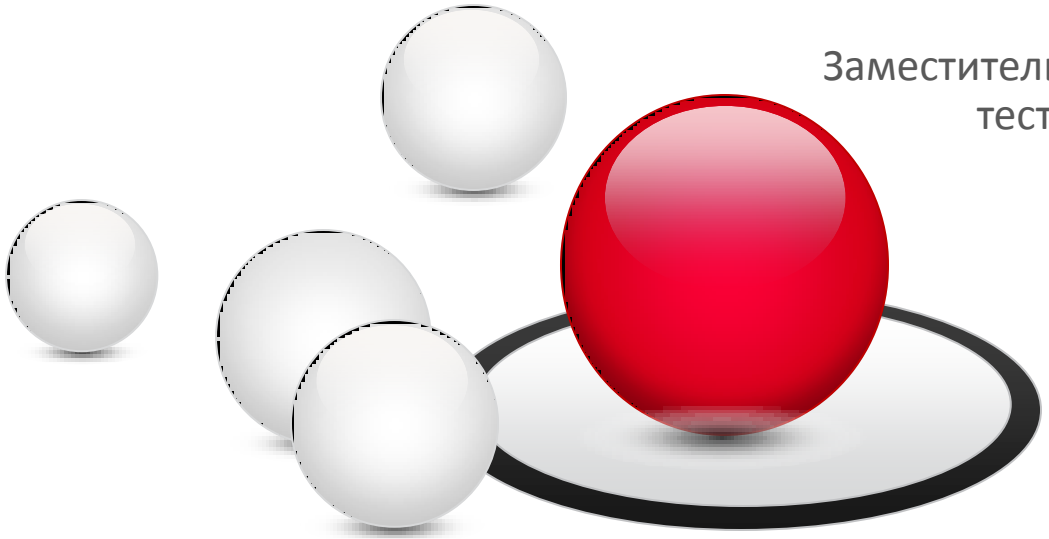
Эшелон
учебный центр

Проведение сертификационных испытаний на отсутствие НДВ. Можно ли найти НДВ?

Вареница Виталий,

Заместитель директора департамента тестирования и сертификации



Что есть?

- Руководящий документ «Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия, 1999)

Что должны искать?

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

Что должны искать?

- **Программные закладки** – ***преднамеренно*** внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению ***конфиденциальности, доступности или целостности*** обрабатываемой информации.

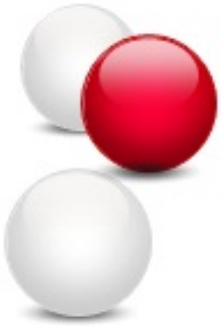
Что предписывает РД

№	Наименование требования	Уровень контроля			
		4	3	2	1
	Требования к документации				
1	**Контроль состава и содержания документации**				
1.1.	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2.	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3.	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4.	Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
1.5.	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
	Требования к содержанию испытаний				
2.	**Контроль исходного состояния ПО**	+	=	=	=
3.	**Статический анализ исходных текстов программ**				
3.1.	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2.	Контроль соответствия исходных текстов ПО его объектному (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 в исходных текстах	-	-	+	+
3.7.	Формирование перечня маршрутов выполнения фкнуциональных объектов	-	+	+	=
3.8.	Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
3.9.	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	-	-	+	=
4.	**Динамический анализ исходных текстов программ**				
4.1.	Контроль выполнения функциональных объектов	-	+	+	=
4.2.	Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=
5.	**Отчетность**	+	+	+	+

Эшелон учебный центр

Что ищут за пределами РФ

- **Уязвимость** - ***дефект ПО***, возникший на этапе его проектирования, реализации или эксплуатации и потенциально ***способный привести к нарушению конфиденциальности, целостности или доступности*** обрабатываемой с его помощью информации.



Классификация уязвимостей ПО

- Позволяющие реализовать сбор или хищение данных.
  - Позволяющие реализовать перехват сетевой информации.
  - Позволяющие реализовать перехват потоков данных (например, с консоли ввода пользователя).
  - Позволяющие превысить полномочия при доступе к информации, хранящейся в базе данных.
- Позволяющие реализовать сокрытие информации.
  - Обеспечивающие выполнение скрытых процессов.
  - Позволяющие реализовать сокрытие данных.

Эшелон
учебный центр

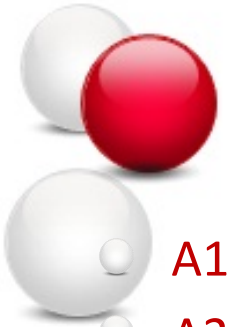
Классификация уязвимостей ПО (2)

- Позволяющие реализовать скрытые каналы передачи информации.
- Позволяющие реализовать управляющее воздействие на информационную систему.
  - Позволяющие реализовать удалённое управление программной системой.
  - Позволяющие реализовать нарушение доступности удалённой системы.

Подходы к выявлению уязвимостей ПО: зарубежный опыт (IBM, Fortify, OWASP, CWE)

- OWASP Top Ten
  - 10 самых больших угроз для веб-приложений
- Fortify Seven Pernicious Kingdoms
  - 7 разрушительных "царств" компании Fortify
- MITRE Common Weaknesses Enumeration
  - всесторонняя классификация изъянов ПО

Эшелон
учебный центр



Десятка OWASP (OWASP Top Ten)

- A1 – Межсайтовый скриптинг (Cross Site Scripting, XSS)
- A2 – Изъяны при внедрении (Injection Flaws)
- A3 – Злонамеренный запуск файла (Malicious File Execution)
- A4 – Небезопасная прямая ссылка на объект (Insecure Direct Object Reference)
- A5 – Подделка HTTP-запросов (Cross Site Request Forgery, CSRF)
- A6 – Утечка информации и неправильная обработка ошибок (Information Leakage and Improper Error Handling)
- A7 – Нарушенная аутентификация и управление сессиями (Broken Authentication and Session Management)
- A8 – Небезопасное криптографическое хранилище (Insecure Cryptographic Storage)
- A9 – Небезопасные коммуникации (Insecure Communications)
- A10 – Ошибка в запрете доступа к URL (Failure to Restrict URL Access)

Эшелон
учебный центр

7 разрушительных царств (Fortify Seven Pernicious Kingdoms)

1. Валидация ввода и представление
2. Эксплуатация API
3. Механизмы безопасности
4. Время и Состояние
5. Обработка ошибок
6. Качество кода
7. Инкапсуляция

*Окружение

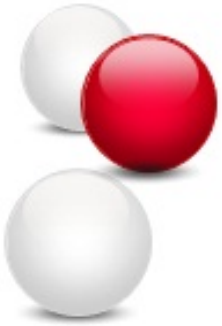
Эшелон учебный центр

Common Weakness Enumeration

http://cwe.mitre.org

- метаязык для описания всех недостатков ПО, схем защиты и атаки
- Структура типа «дерево»
  - Категории
    - Элементы
      - Составные элементы
- Сгруппировано по «отображениям»
  - Research View
  - Development View
  - C/C++ Developer View
  - Java Developer View
  - …

Эшелон учебный центр

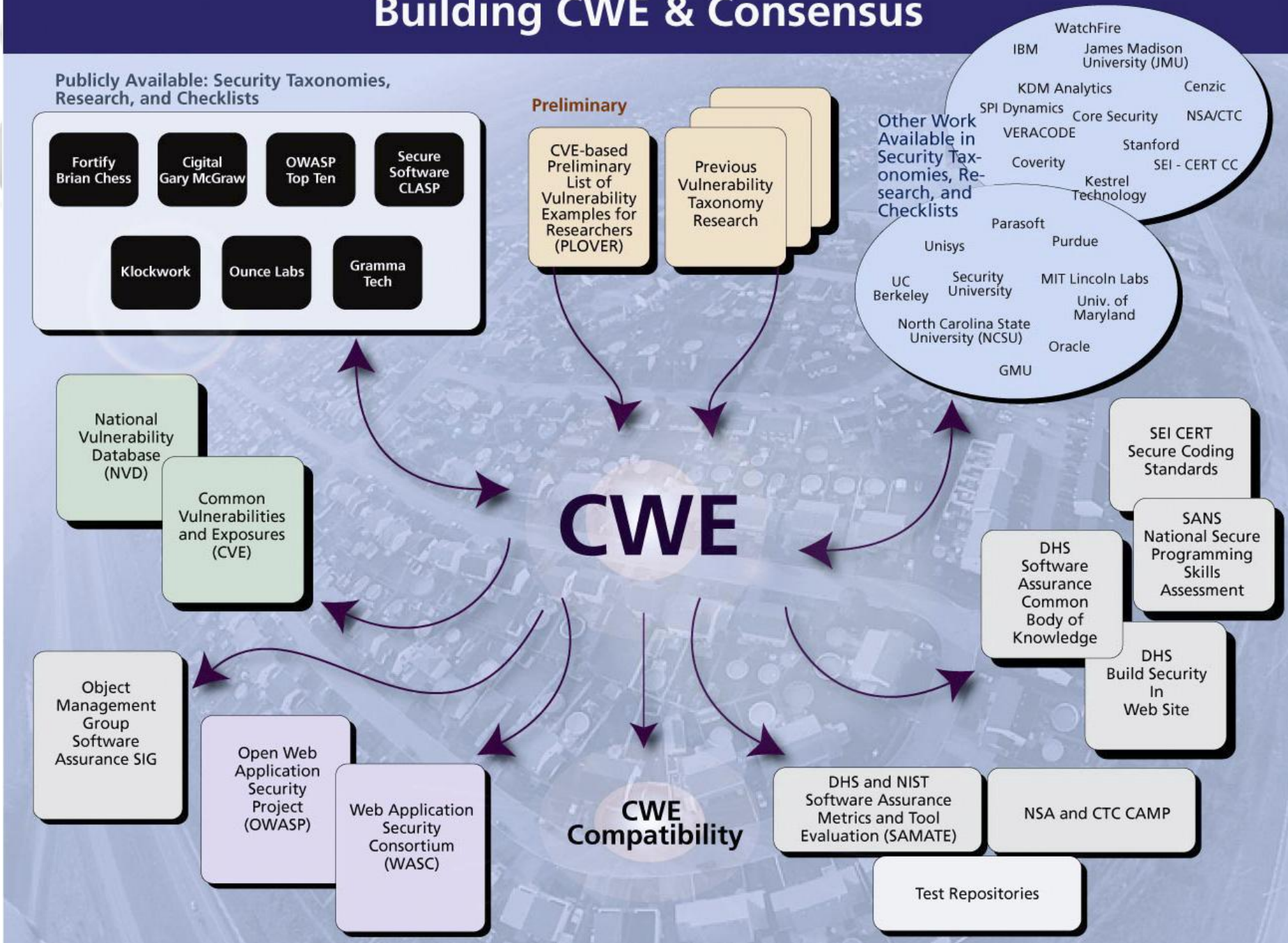


Уязвимости и изъяны

- CVE (Common Vulnerability Enumeration)
- CWE - Common Weakness Enumeration

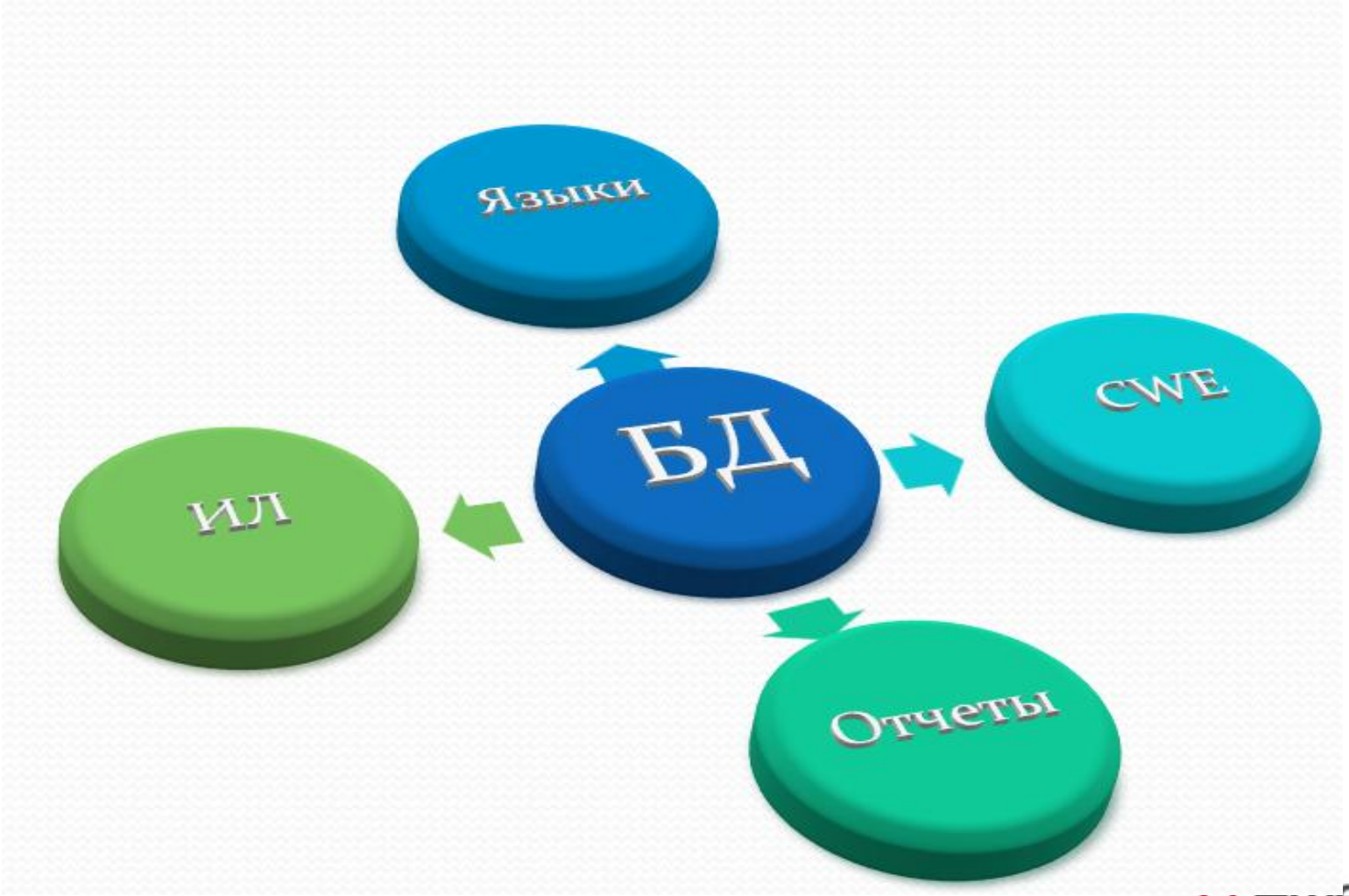
Эшелон
учебный центр

Building CWE & Consensus



АК-ВС

Анализатор кода вычислительных систем (АК-ВС), структура:



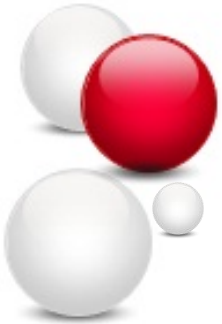
АК-ВС

- **АК-ВС поддерживает работу с языками**
  - C, C++
  - C#
  - Java
- **Построение отчетов АК-ВС**
  - Списка функциональных объектов
  - Списка информационных объектов
  - Списка висячих функциональных объектов
  - Связей ФО по управлению и по информации
  - Построение трасс вызовов (ф-ф, ф-в, в-в)
  - Построение графов вызовов
  - Построение блок-схем
  - Ведение протокола вставки датчиков

АК-ВС

- **Сигнатурный модуль базируется на CWE**
- **База сигнатур для поиска программных закладок и уязвимостей включает конструкции способные привести к:**
  - переполнению буфера;
  - обращениям к файловой системе;
  - манипулированию именами;
  - уязвимости для троянских атак;
  - вводу пароля;
  - возможному превышению полномочий;
  - уязвимости для DOS-атак;
  - низкоуровневой работе с дисками и файловой системой;
  - скрытым каналам передачи информации.

Эшелон
учебный центр



АК-ВС

АК-ВС позволяет отслеживать:

- ассемблерные вставки;
- операции с датой/временем;
- сетевое взаимодействие;
- отладочную информацию;
- работу с временными характеристиками;
- параметры командной строки;
- операции с параметрами безопасности среды;
- скрытые сообщения;
- точки ввода/вывода данных;
- операции, связанные с обработкой прерываний;
- обращение к криптографическим примитивам;
- вызов внешних процедур;
- обращение к файловым системам.

Эшелон
учебный центр

АК-ВС

Сигнатурный модуль АК-ВС

- Ориентирован на выявление потенциально опасных конструкций в коде, которые могут привести к нарушению безопасности системы
- Поддерживается международными объединениями (OWASP)
- Поддерживает международный стандарт (MITRE – CWE)
- Все выявленные НДВ, программные закладки, ошибки проектирования и некорректности кодирования, влияющие на безопасность, были выявлены с помощью сигнатурного метода

Эшелон
учебный центр

АК-ВС

- **АК-ВС может применяться:**
  - Для сертификационных испытаний на отсутствие НДВ
  - При проведении аудита кода по требованиям безопасности
  - При разработке программного обеспечения

АК-ВС

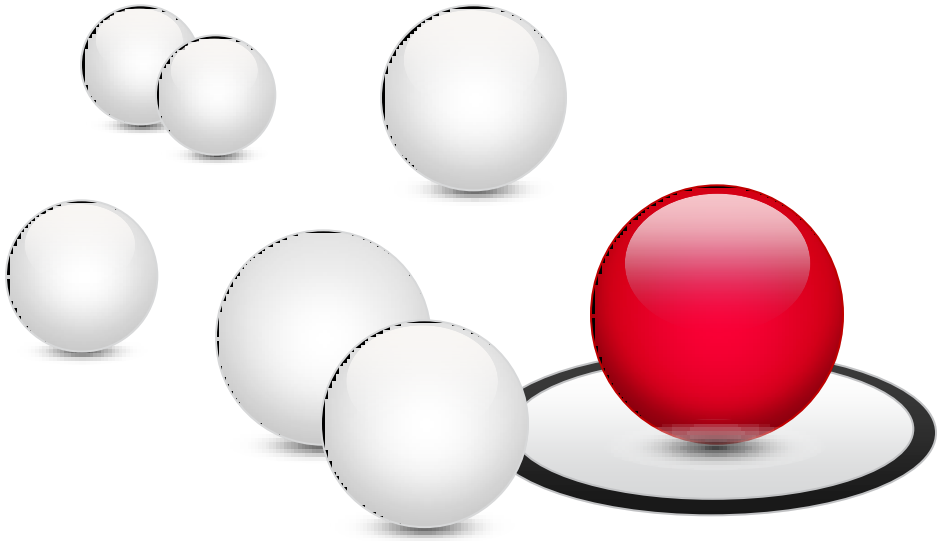
- АК-ВС имеет сертификаты **МО РФ** и **ФСТЭК** России

Эшелон
учебный центр

КУРС ОБУЧАЮЩИЙ РАБОТЕ С АК-ВС

Эшелон
учебный центр

Эшелон
учебный центр



Вареница Виталий

Заместитель директора департамента тестирования и сертификации

ЗАО “НПО“Эшелон”

E-mail: www@cnpo.ru

Тел.: +7(495) 645-38-09