Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

Докладчик: **ФАУ «ГНИИИ ПТЗИ ФСТЭК России»**
начальник лаборатории
Сердечный Алексей Леонидович

Разработка методики выявления уязвимостей и недекларированных возможностей в программном обеспечении

Эшелон
комплексная безопасность

ИСП РАН

ЦБИ

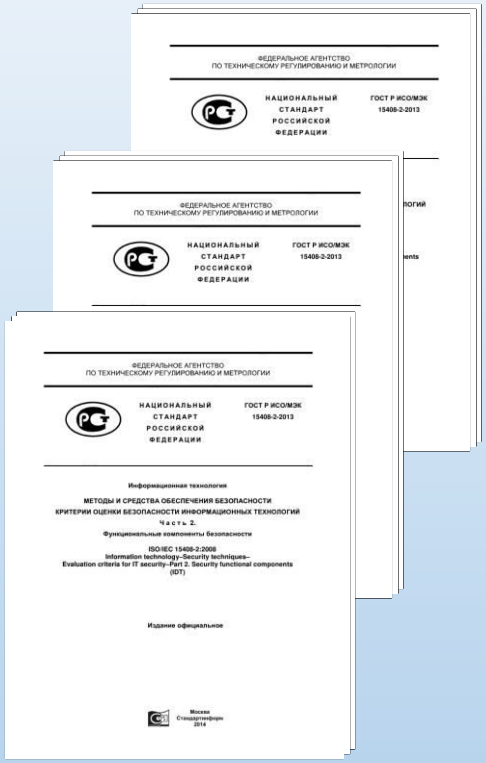
СТАНКО ИНФОРМ ЗАЩИТА

Испытательные лаборатории ФСТЭК России

KASPERSKY lab

POSITIVE TECHNOLOGIES

Структура методики выявления уязвимостей и недекларированных возможностей в программном обеспечении



ГОСТ Р ИСО/МЭК 15408

ГОСТ Р ИСО/МЭК 18045

ГОСТ Р 56939-2016

РД НДВ

1. Общие положения

2. Общие требования к проведению исследований ...

3. Подготовка к проведению исследований ...

4. Проведение исследований ...

5. Оформление результатов исследований ...

Приложение 1. Термины и определения ...

Приложение 2. Методы ...

Приложение 3. Инструментальные средства ...

Приложение 4. Расчёт потенциала нападения ...

Приложение 5. Классификация уязвимостей ПО

Приложение 6. Классификация НДВ ПО

Особенности методического подхода

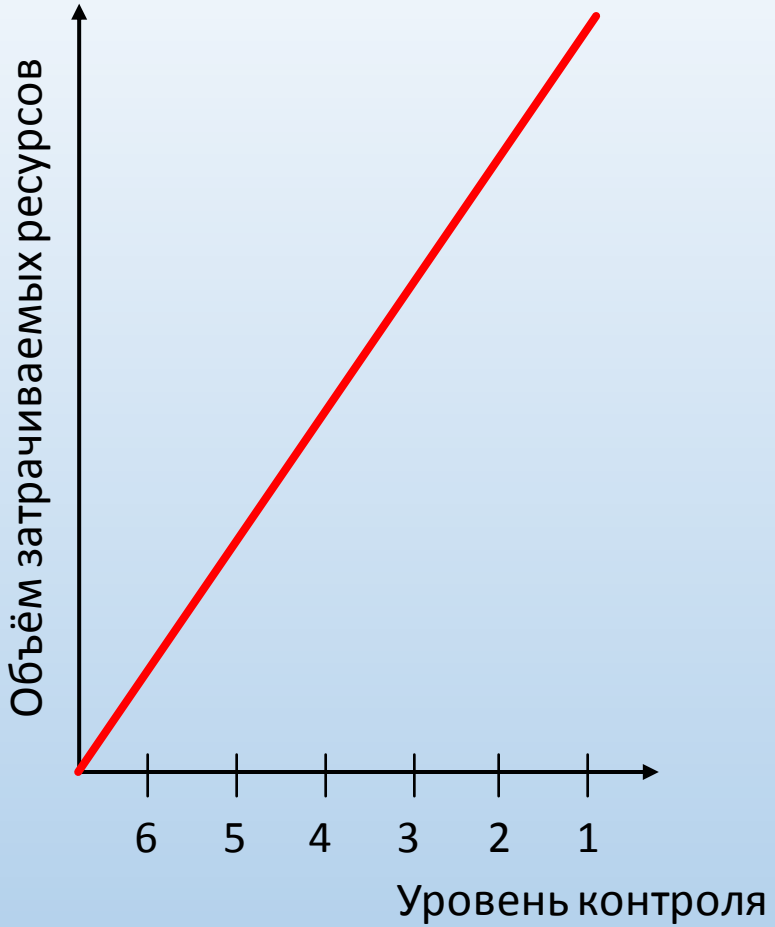
Работа 1

- исходные данные
- требования
- методы
- средства
- результаты
- усиления

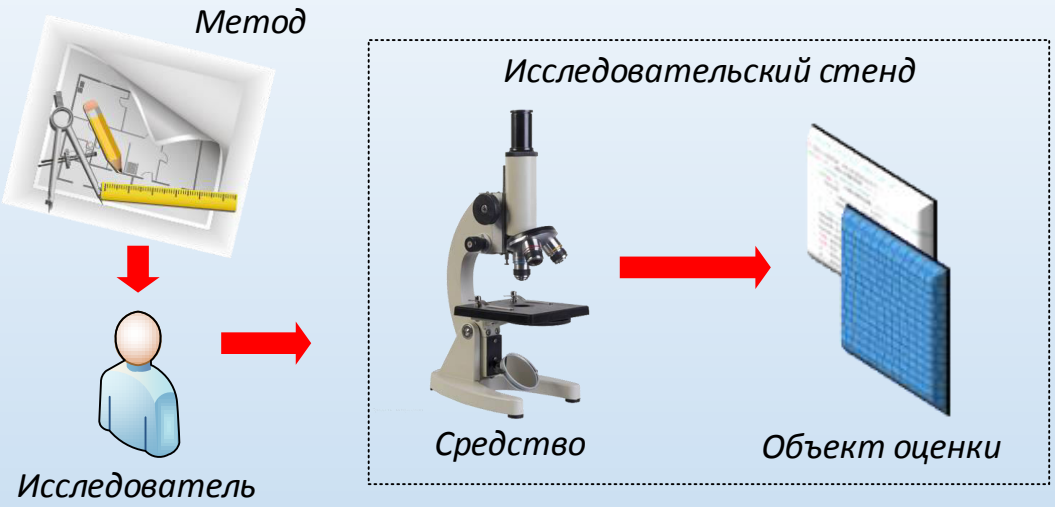
Работа 2

…

Работа N



Методы и инструментальные средства выявления уязвимостей и НДВ



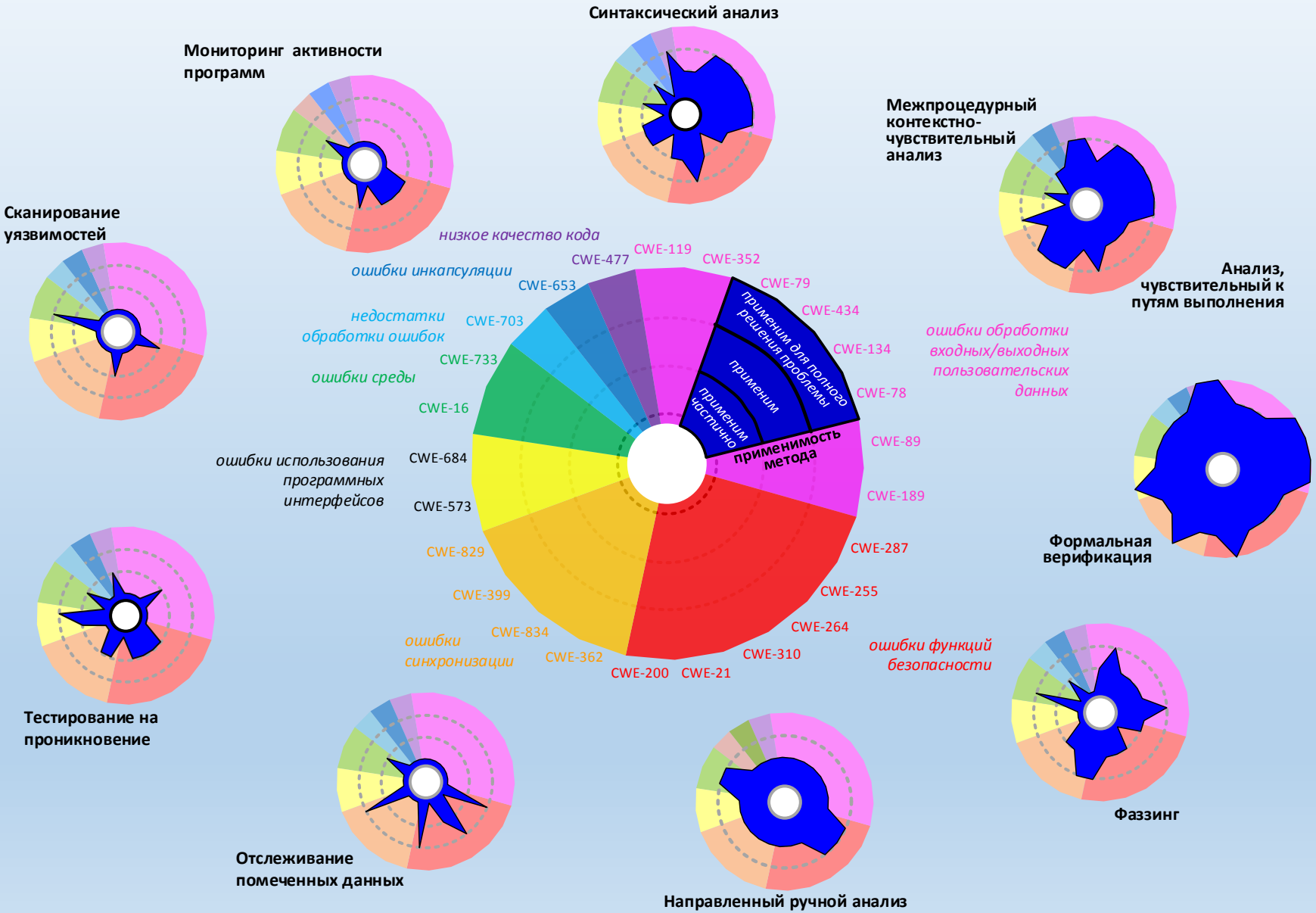
Методы

- Анализ документации
- Анализ, чувствительный к путям выполнения
- Антивирусный контроль
- Аутентификация программного кода
- Межпроцедурный контекстно-чувствительный анализ
- Мониторинг активности программ
- Тестирование на проникновение
- Направленный анализ участков кода
- Отслеживание помеченных данных
- Оценка соответствия исходных кодов программы их исполняемому коду
- Символьное выполнение
- Синтаксический анализ
- Сканирование интерфейсов получения входных данных
- Сканирование уязвимостей
- Сопоставление путей и трасс выполнения программы
- Съём трасс выполнения программы
- Фаззинг
- Формальная верификация

Средства

- Средство антивирусной защиты
- Монитор активности приложений
- Анализатор сетевых протоколов
- Сетевой сканер
- Программа фиксации и контроля целостности информации
- Статический анализатор кода
- hex-редактор
- Профилировщик
- Эмулятор
- Сканер уязвимостей
- Фаззер
- Анализатор трасс

Характеристика целевых методов вяления уязвимостей

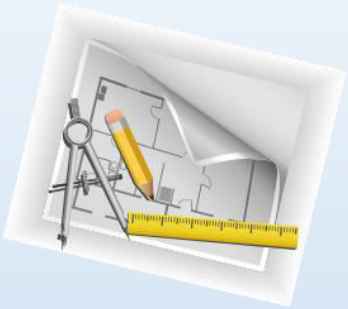


Примеры инструментальных средств

Инструментальные средства

Средство антивирусной защиты	Антивирус Касперского, Dr.Web, ...
Монитор активности приложений	Process Monitor, ...
Анализатор сетевых протоколов	Wireshark, ...
Сетевой сканер	Nmap, ...
Программа фиксации и контроля целостности информации	ФИКС, ...
Статический анализатор кода	Svace, PVS-Studio, SPModeler, ...
hex-редактор	010 Editor, ...
Профилировщик	Valgrind, CodeAnalyst, Vtune, ...
Эмулятор	QEMU, ...
Сканер уязвимостей	Xspider, ...
Фаззер	ISP-fuzzer, AFL, Peach, ...
Анализатор трасс	Avalanche-Anxiety, BitBlaze, ...

Работы по выявлению уязвимостей и НДВ



Этап 1. Подготовка к проведению исследований

- Анализ документации и других источников, содержащих сведения об объекте оценки
- Подготовка исследовательского стенда

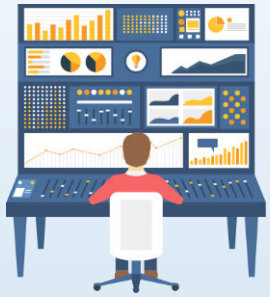
Этап 2. Проведение исследований

- Экспертный анализ объекта оценки
- Статический анализ объекта оценки
- Динамический анализ объекта оценки
- Ручной анализ объекта оценки

Этап 3. Оформление результатов исследований

- Разработка методик испытаний
- Разработка протокола исследований

Предварительный анализа объекта оценки



Документация на объект оценки

Сведения об объекте оценки

Дистрибутив объекта оценки

Образ встраиваемого программного обеспечения

Этап 1. Подготовка к проведению исследований

Анализ документации и иных сведений об объекте оценки

Подготовка исследовательского стенда

Потенциально опасные функциональные возможности

Представление об объекте оценки

Исследовательский стенд

Экспертный анализ объекта оценки

Подготовка к проведению исследований

Документация на объект оценки

Исполняемый код

Исходный код

Представление об объекте оценки

Экспертный анализ объекта оценки

Анализ архитектуры объекта оценки

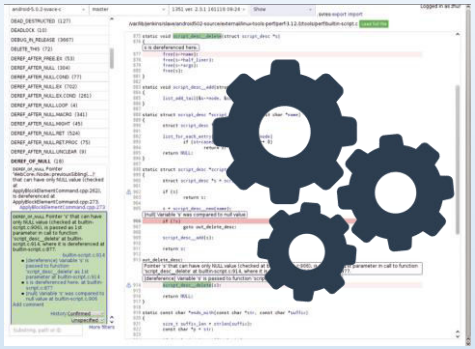
Идентификация потенциальных уязвимостей объекта оценки

Тестирование на проникновение объекта оценки

Сведения о функциональных возможностях объекта оценки

Перечень уязвимостей и НДВ объекта оценки

Статический анализ объекта оценки



Исходный код

Документация на объект оценки

Статический анализ объекта оценки

Синтаксический анализ исходного кода объекта оценки

Анализ исходного кода объекта оценки, чувствительный к контексту и путям выполнения

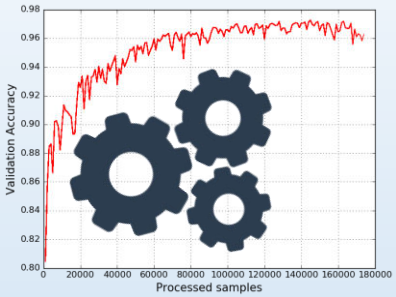
Формальная верификация исходного кода объекта оценки

Перечень уязвимостей и НДВ объекта оценки

Код, написанный с использованием языков программирования, не поддерживаемых статическим анализатором

Сведения о связях между информационными и функциональными объектами

Динамический анализ объекта оценки



Экспертный анализ объекта оценки

Статический анализ объекта оценки

Исполняемый код

Исходный код

Документация на объект оценки

Сведения о функциональных возможностях объекта оценки

Сведения о связях между информационными и функциональными объектами

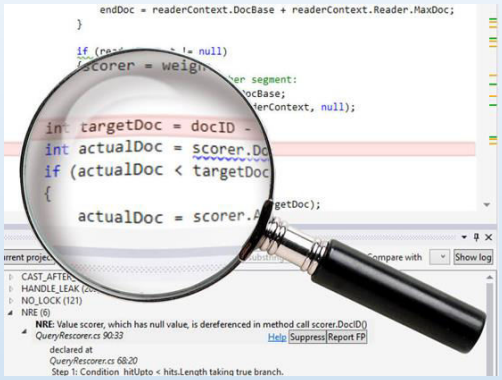
Динамический анализ объекта оценки

Фаззинг-тестирование объекта оценки

Анализ трасс выполнения объекта оценки

Перечень уязвимостей и НДВ объекта оценки

Ручной анализ объекта оценки



Статический анализа объекта оценки

Динамический анализ объекта оценки

Документация на объект оценки

Код, незадействованный в ходе статического и динамического анализа

Исходный код

Код, написанный с использованием языков программирования, не поддерживаемых статическим анализатором

Ручной анализ объекта оценки

Перечень уязвимостей и НДВ объекта оценки

Оформление результатов исследований

Этап 1

Этап 2

Документация на объект оценки

Результаты выполнения работ

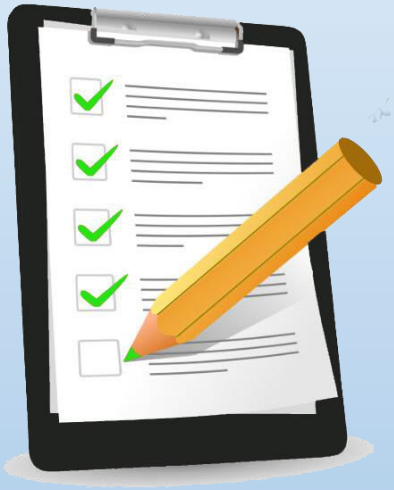
Этап 3. Оформление результатов исследований

Разработка методик испытаний

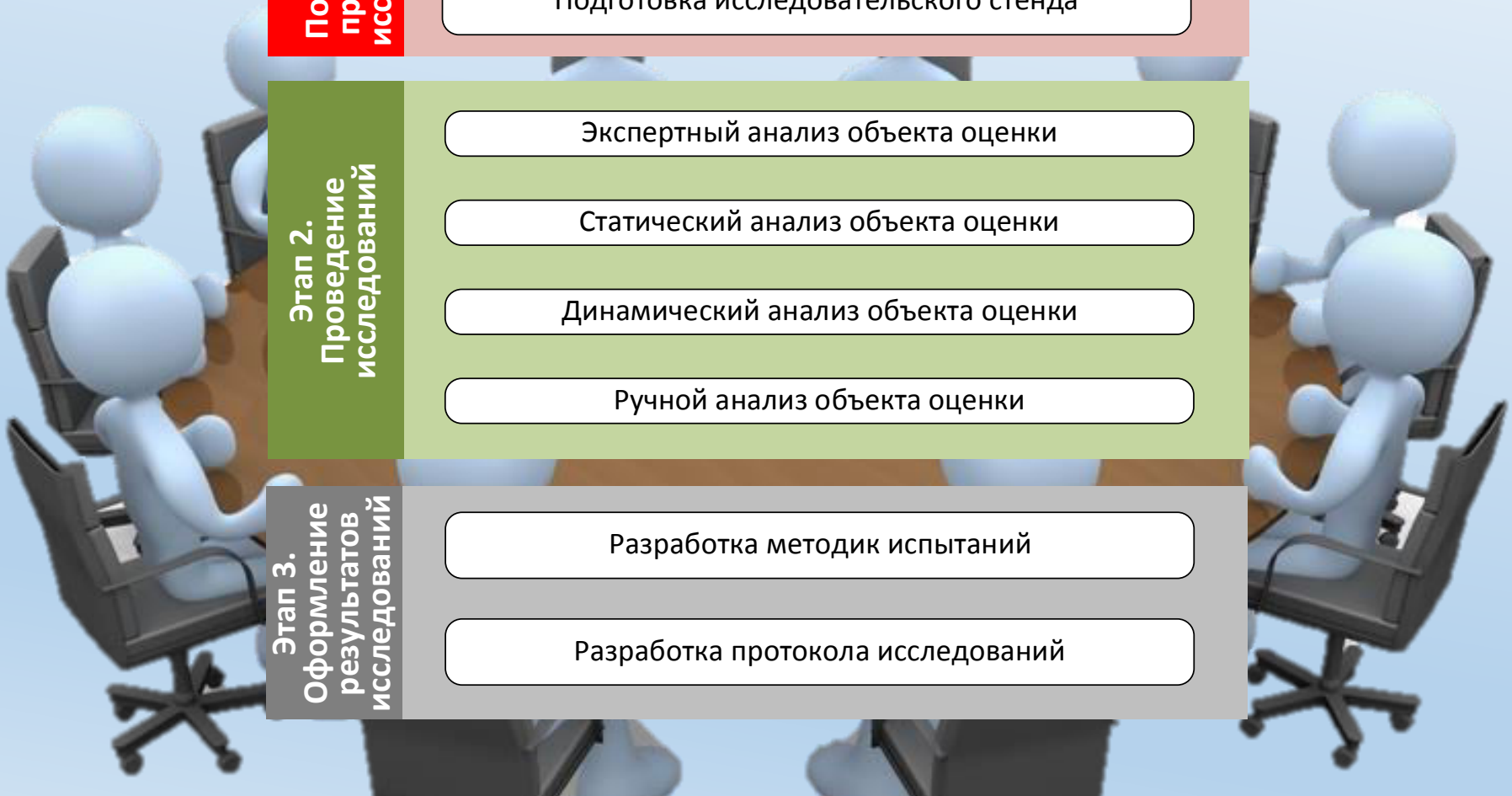
Разработка протокола исследований

Методики испытаний

Протокол исследований



Спасибо за внимание!



Этап 1. Подготовка к проведению исследований

- Анализ документации и других источников, содержащих сведения об объекте оценки
- Подготовка исследовательского стенда

Этап 2. Проведение исследований

- Экспертный анализ объекта оценки
- Статический анализ объекта оценки
- Динамический анализ объекта оценки
- Ручной анализ объекта оценки

Этап 3. Оформление результатов исследований

- Разработка методик испытаний
- Разработка протокола исследований