Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.

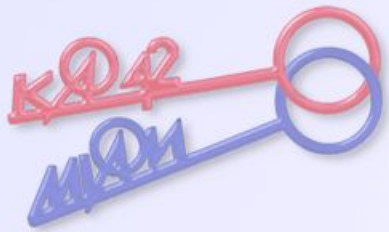
WMI-Analyser

Исполнители: Еремин А., Теплов Д., Колобова А., Кожухова П., Сюзюкина А.
Научный руководитель: Малкин В.А.

Этапы и цели работы

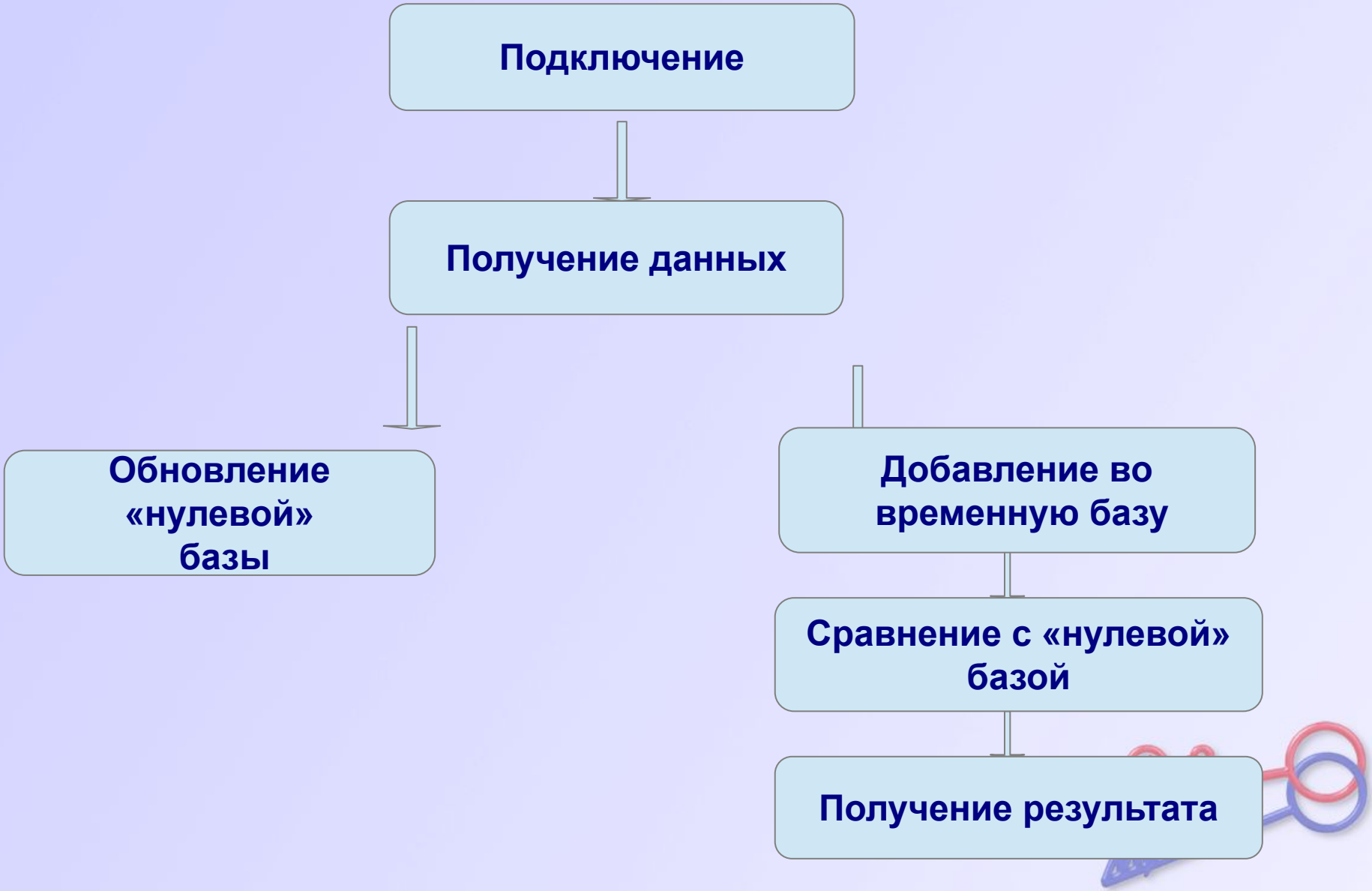
- Основная цель работы — проверка устройств на заражение.

- Соединение и настройка множества компьютеров по локальной сети
- Работа с базами данных
- Использование WMI-запросов
- Тестирование работы приложения

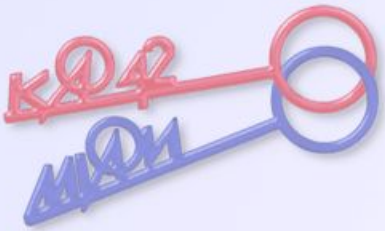


Структура приложения

Схема работы приложения

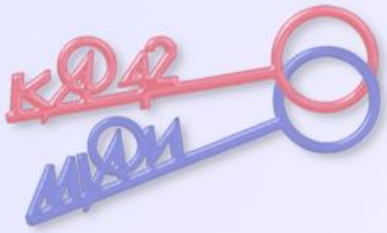


Вирусы, которые могут быть выявлены с помощью приложения:



Тестирование общей архитектуры

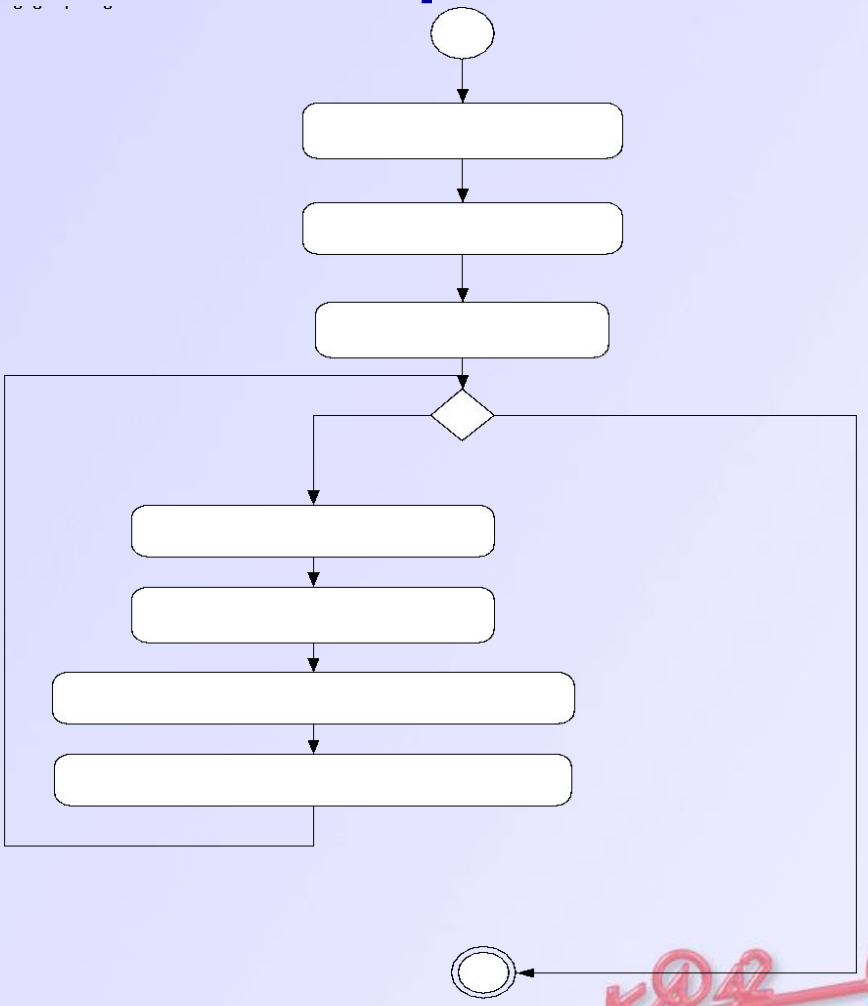
Вид Тестирования	Система с установленным средством	Система, работающая напрямую на аппаратном обеспечении
Врем. характеристики		
Мин. время, такт	300	224
Макс. время, такт	6500	2324
Среднее время, такт	318	267
Потери	~25%	—



Модуль защиты элементов пространства ядра

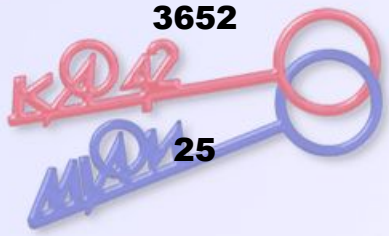
Преимущества:

- Разделяемый доступ к физической памяти
- Дополнительный уровень защиты за счет контроля физ. памяти



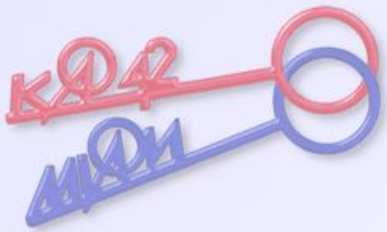
Временное тестирование модуля

Вид тестирования	Защищаемые страницы		Незащищаемые страницы	
Врем. характеристики	Чтение	Исполнение	Чтение	Исполнение
Мин. время, такт	52	40	32	24
Макс. время, такт	2674	3634	68	3652
Среднее время, такт	82	68	40	25
Потери				



Анализ результатов тестирования

- Большая потеря производительности при краевом тестировании >60%
- Потеря производительности не является критической, т.к. ОС в данном режиме не работает



Результаты работы

- Произведен анализ существующих средств создания ДВС
- Спроектировано средство обеспечение ДВС, превосходящие существующие аналоги
- Реализована и протестирована часть модулей составляющих средство обеспечения ДВС