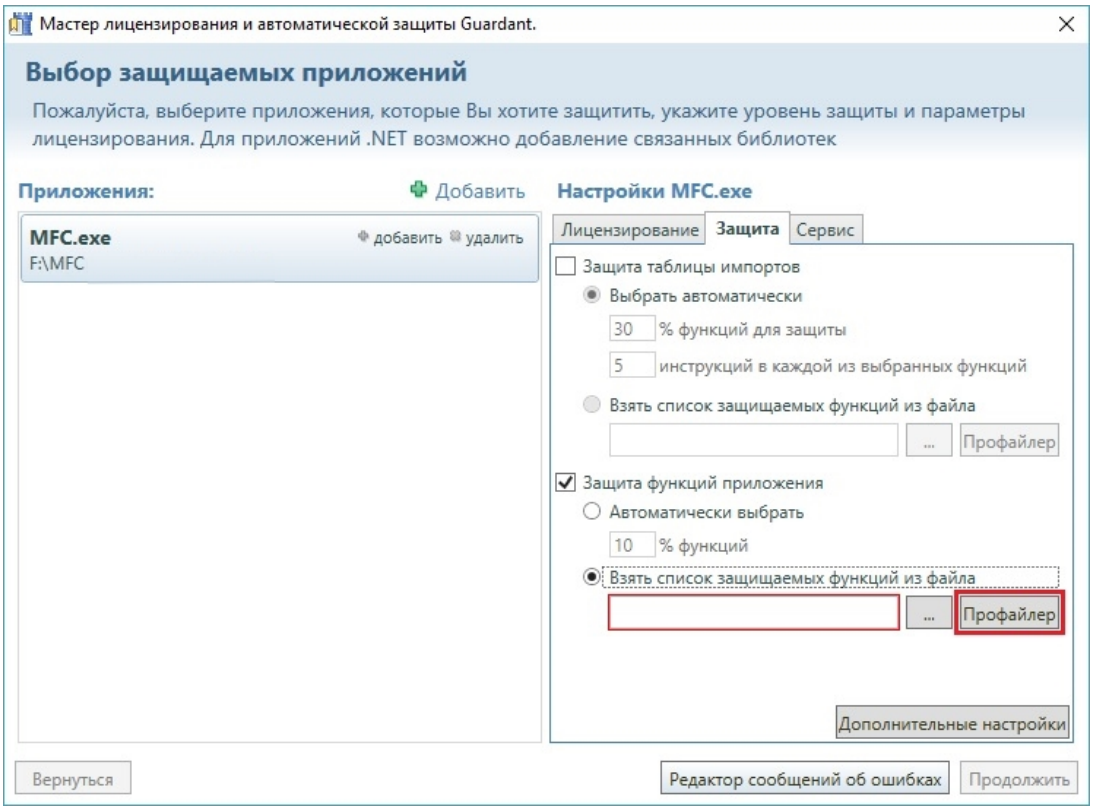
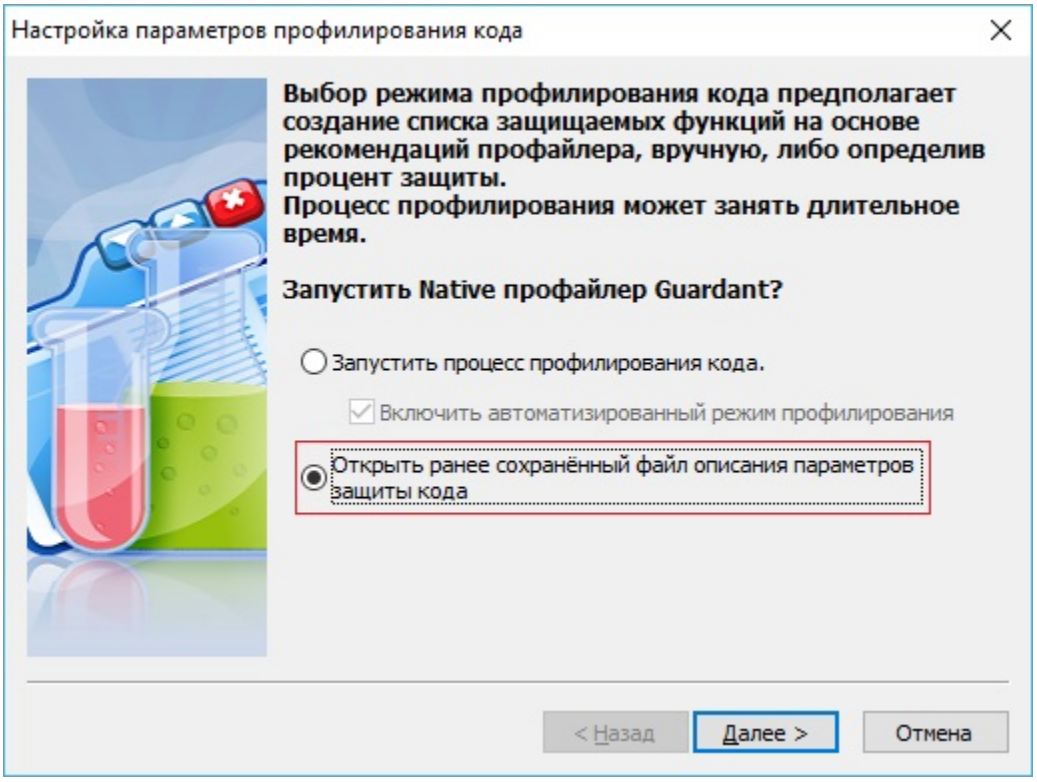
Ручной выбор функций Native-приложений

Можно выбрать функции для защиты вручную. Это рекомендуется делать, если защищенное приложение демонстрирует невысокую производительность (по сравнению с исходной), и разработчик хорошо знаком с внутренней структурой приложения, а значит, сможет указать автозащите, какие функции лучше не защищать.

При выборе данного метода запускается процесс статического анализа кода.

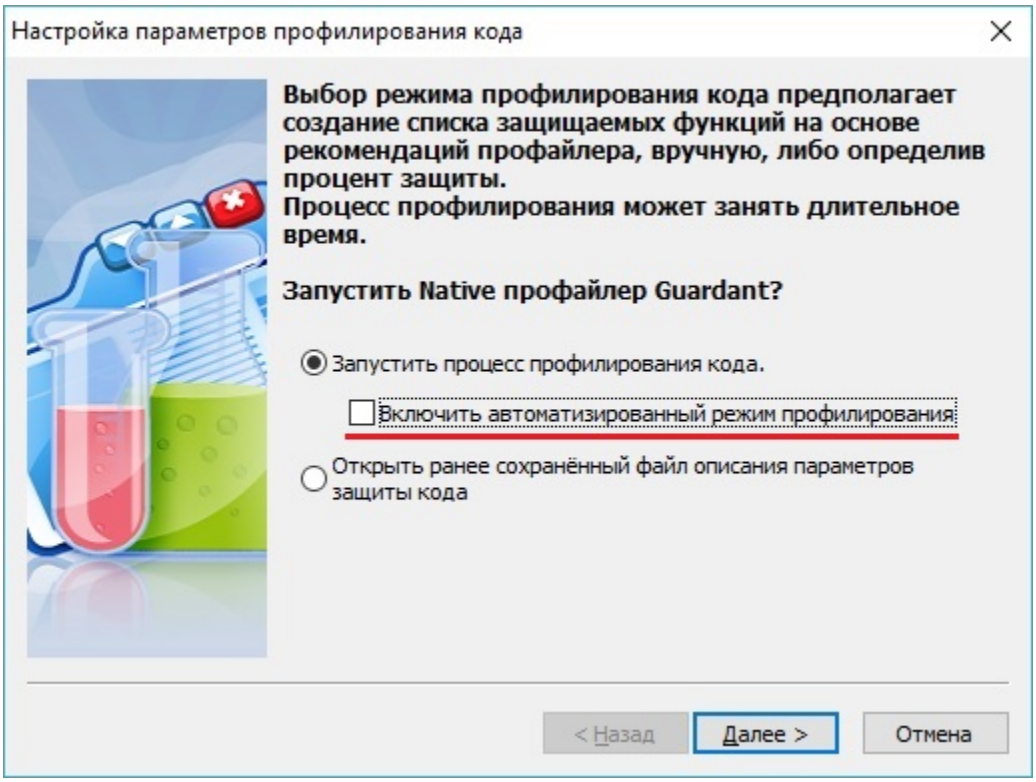
Если статический анализ уже проводился, и нужно лишь подкорректировать выбор защищаемых функций,то следует в интерфейсе утилиты мастера лицензирования нажать кнопку **Профайлер** в разделе **Защита функций приложения** и выбрать вариант **Открыть ранее сохраненный файл описания параметров защиты кода** (*.prc).

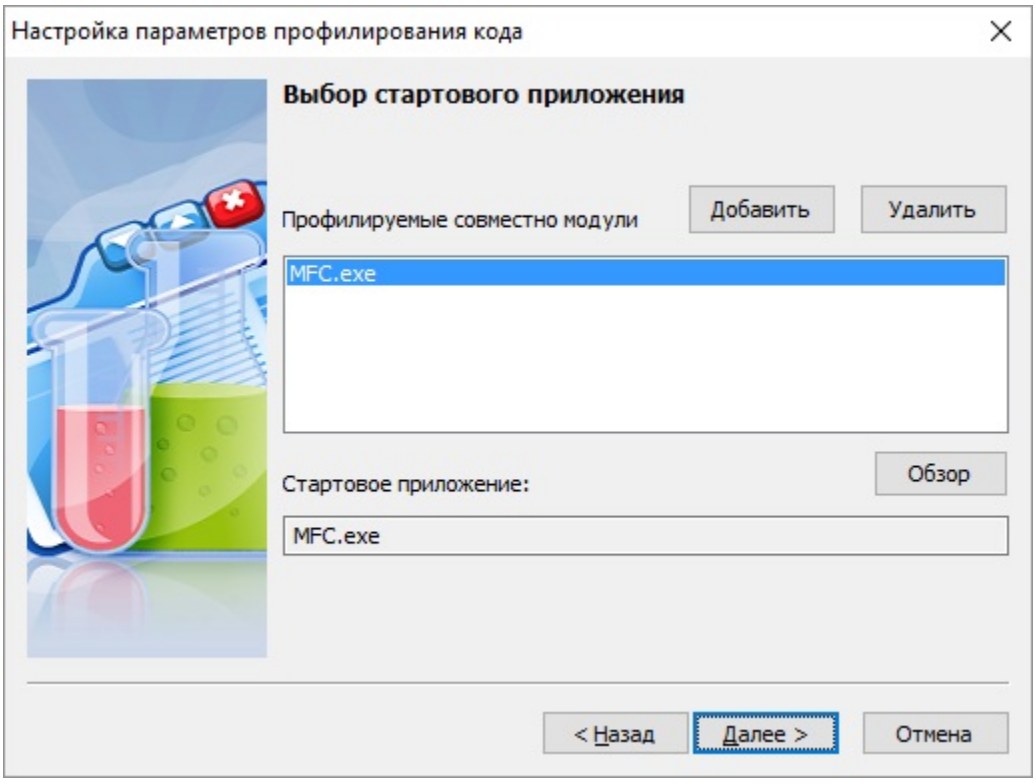




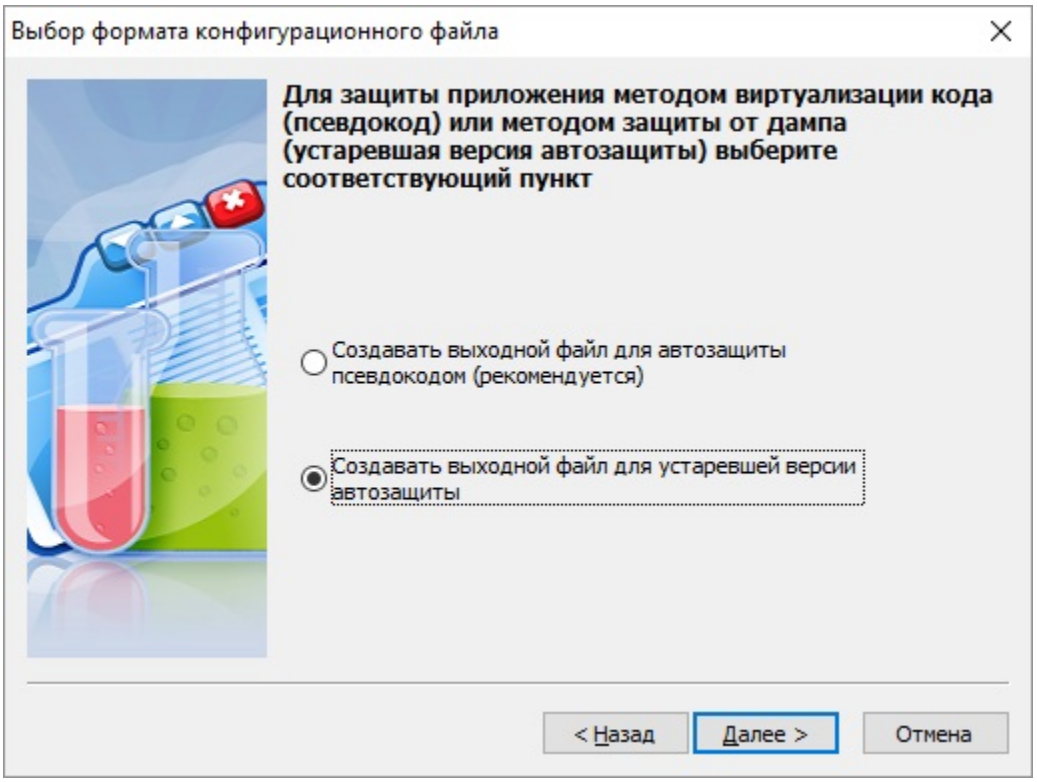
Важно!
При повторной компиляции приложения, и, соответственно, перегенерации **MAP-файла,** существующий файл описания защиты кода становится недействительным, и необходимо повторное проведение статического анализа и повторный выбор функций!

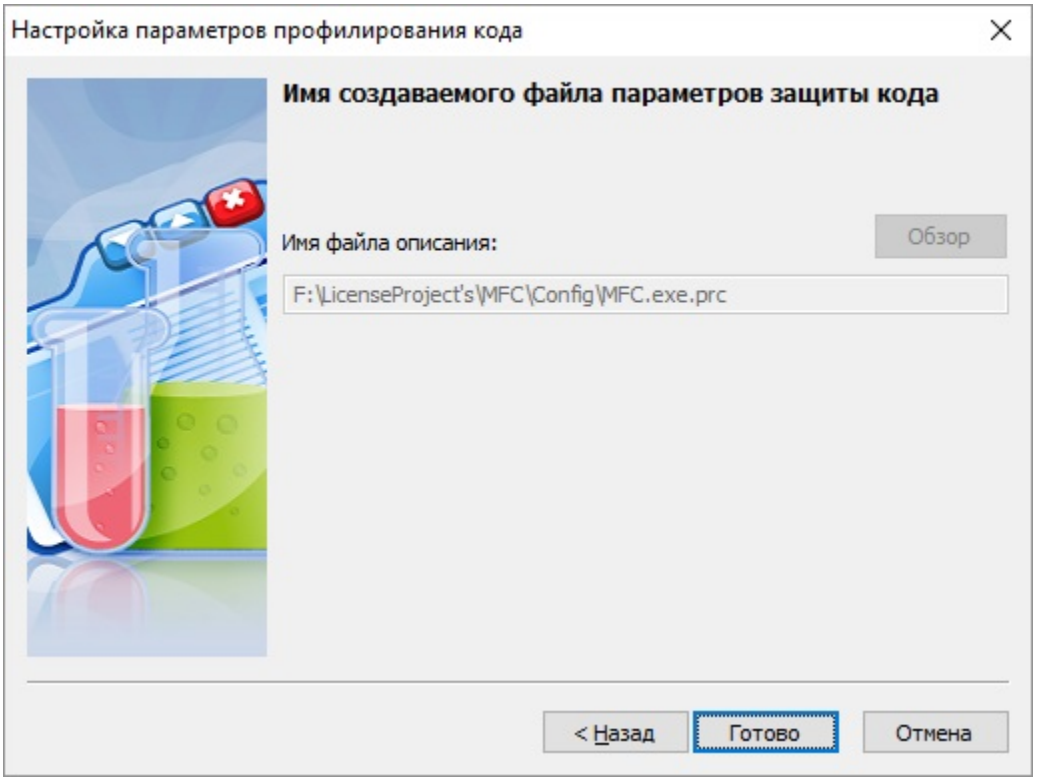
Если же процесс статического анализа проводится впервые (или защищаемый файл изменился), то необходимо выбрать пункт **Запустить процесс профилирования кода** и отключить опцию выбора автоматического режима, предварительно убедившись, что в одной папке с защищаемым файлом находится соответствующий ему **MAP-файл:**





Далее нужно выбрать **Создавать выходной файл для устаревшей версии автозащиты**.

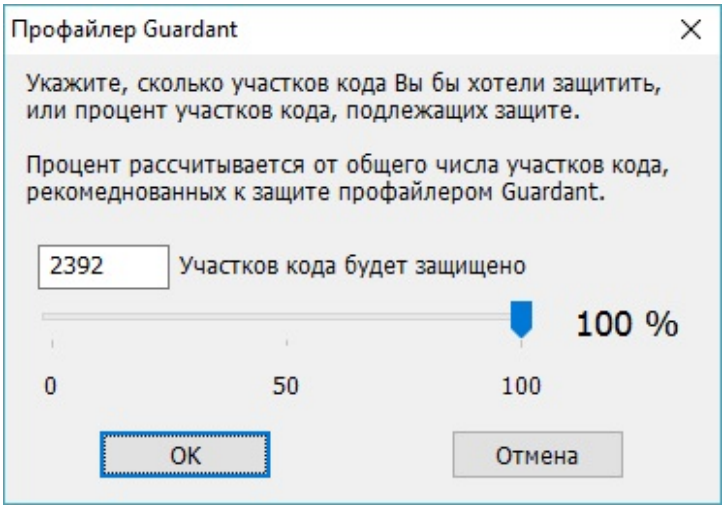




Когда профилирование запускается из среды мастера лицензирования, то изменение параметров в данном диалоговом окне будет недоступно. В случае, если мастер лицензирования не используется, то имя файла описания изменить нельзя – оно жестко привязано к проекту лицензии.

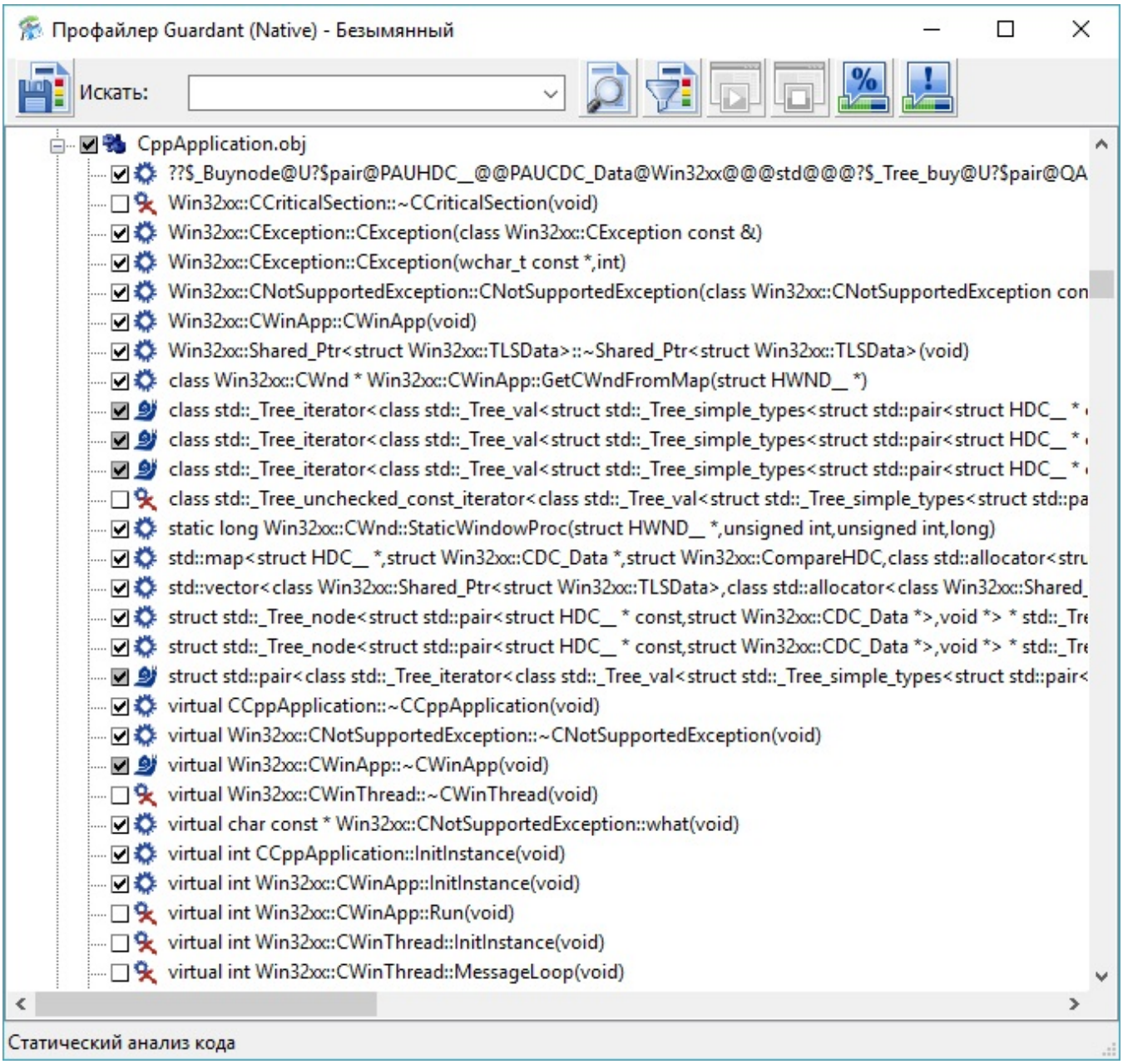
По нажатию на кнопку **Готово** начинается процесс анализа и дизассемблирования защищаемого приложения. После этого в отдельном окне выводятся все базовые блоки, которые можно защитить.

Здесь можно указать первоначальныйпроцент защищаемых базовых блоков. Чем меньше процент, тем быстрее будет работать защищенное приложение, но тем меньше оно будет защищено.



Примечание!
При помощи **RIP CODE** виртуализируется не тело функции целиком, а только определенные наборы инструкций. Каждый такой набор называется базовым блоком. В защищаемой функции может быть от одного базового блока до нескольких тысяч, в зависимости от ее размера. Если базовых блоков в функции не найдено, защите она не подлежит.

По нажатию на **OK** происходит переход в основное окно работы профайлера, методика работы с которым описана в следующем разделе.



Профайлер Native также можно запустить из меню утилиты **Guardant Интегратор** или при помощи исполняемого файла **NativeProfilerGUI.exe**. В этих случаях графический интерфейс утилиты профилирования может незначительно отличаться.