УДК 65.012.8

ПРОБЛЕМЫ КОНТРОЛЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА НАЛИЧИЕ ИЛИ ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ С ПОМОЩЬЮ АППАРАТА СЕТЕЙ ПЕТРИ

К. П. Грищенко, В. А. Чулюков

Воронежский государственный педагогический университет

Проблема обнаружения недекларированных возможностей (НДВ) решается несколькими методами, но существуют единые правила, основанные на анализе как закрытого, так и открытого программного кода.

Любой вариант исполнения программы представляет собой маршрут, начинающийся в одном из операторов, который содержит вход в процедуру, и заканчивается выходом из процедуры. В корректно составленной программе через каждый оператор должен проходить хотя бы один маршрут исполнения тела процедуры. Возможны три случая нарушения условия принадлежности оператора хотя бы к одному маршруту:

– некоторый оператор вообще не достигается ни по одному из маршрутов, идущих от входов процедуры;

– из некоторого оператора или их совокупности не существует ни одного пути, ведущего хотя бы к одному выходу из процедуры (образуются тупиковые пути или зацикливание);

– блокирование исключительных ситуаций.

Наличие лишних операторов в программе можно обнаружить путем анализа связей по управлению между функциональными объектами с рассмотрением всевозможных маршрутов выполнения функциональных объектов. Наличие тупиков приводит к тому, что возможны либо непредусмотренные остановы, либо

зацикливания. Тупики в ряде случаев можно обнаружить при выполнении программы. Поиск признаков, характеризующих взаимосвязанные изменения в структуре, логике и вычислениях программ, которыми сопровождается реализация НДВ – главная задача анализа. Эффективным можно назвать тот метод, который позволяет учесть особенности предмета анализа, тем самым повысить вероятность нахождения НДВ.

Для проверки программного обеспечения на наличие ошибок и уязвимостей предлагается использовать аппарат сетей Петри.

Под анализом программного обеспечения понимается:

– поиск ошибок в программном обеспечении;

– нахождение и оптимизация критических (наиболее часто используемых) участков кода;

– испытания на отсутствие НДВ.

Перед проведением анализа и после с файлов исходных текстов программного обеспечения снимаются контрольные суммы по различным алгоритмам хеширования. Но, ввиду того, что между снятием контрольных сумм исходные тексты форматируются и незначительно видоизменяются, контрольные суммы также изменяются, следовательно, использование классического хеширования файлов нецелесообразно.

Перед анализом программного обеспечения, а также во время и после его проведения необходимо использовать специальные механизмы, реализующие идентификацию анализируемых исходных текстов или самих программных модулей. Для этого применяются различные способы идентификации и контроля целостности, например, способ применения контрольных сумм, работающий по следующему алгоритму:

– генерация ключа хеширования;

– на основе сгенерированного ключа формирование контрольного хеш-кода файлов исходных текстов путем хеширования по криптографическому алгоритму;

– при проведении идентификации и контроле хеширования проводят повторное хеширование файлов исходных текстов, сравнение полученного хеш-кода с полученным хеш-кодом, формирование результата проверки.

Существенным недостатком данного способа является неидентичность хеш-кода файлов, содержащих исходные тексты программного обеспечения и хеш-кода тех же файлов после форматирования, не изменяющего структуру алгоритма. Причина наличия такого недостатка заключается в том, что хешированию подвергаются файлы исходных текстов программного обеспечения целиком (побайтно). Следовательно, целесообразно рассмотреть способ обеспечения неизменности хэш-кода исходных текстов программного обеспечения вне зависимости от форматирования, который заключается в получении контрольного образа файла исходного текста на основе аппарата сетей Петри.

Способ можно описать алгоритмом:

1. Генерация ключа хеширования;

2. Построение сети Петри по правилам, описанным в [1] для файлов, содержащих исходные тексты программного обеспечения.

3. Сохранение сети Петри.

4. Формирование контрольного хеш-кода файла сети Петри путем хеширования по криптографическому алгоритму.

5. Повторное построение сети Петри для исследуемых файлов.

6. Хеширование файла сети Петри.

7. Сравнение сформированного результата повторного хеширования файла сети Петри хеш-кода с контрольным хеш-кодом.

8. Формирование результата анализа.

Способ получения контрольного образа файлов исходных текстов на основе аппарата сетей Петри может быть реализован с помощью электронно-вычислительной машины или вычислительного устройства, показанного в патенте [2].

Таким образом, использование предлагаемого способа контроля целостности исходных текстов программного обеспечения путем получения контрольного образа файлов исходных текстов на основе аппарата сетей Петри позволяет обеспечить неизменность хеш-кода исходных текстов программного обеспечения вне зависимости от произведенного форматирования, так как хеш-код снимается не с файлов, содержащих исходные тексты, а с файла сети Петри этих исходных текстов.

Использование данного способа контроля целостности приводит к существенному уменьшению влияния субъективных факторов, таких как стиль форматирования.

Литература

1. *Котов В.Е.* Сети Петри. – М.: Наука. Гл. ред. физ.-мат. лит., 1984. 160 с.

2. *Бурушкин А.А., Минаков В.А., Мирошников В.В., Грищенко К. П.* Система контроля отсутствия недекларированных возможностей в программном обеспечении. Патент №2419135. – Федеральное государственное учреждение “Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» – М.: Федеральная служба по интеллектуальной собственности, патентам и товарным знакам, 2011.