



ТРИБУНА
МОЛОДЫХ УЧЕНЫХ

БИТ

С. В. Гаврилюк

ПРОВЕРКА КОРРЕКТНОСТИ РЕЗУЛЬТАТА ВЫЧИСЛЕНИЙ В ГРИД-СЕТИ

Грид — географически распределенная инфраструктура, объединяющая множество ресурсов разных типов (процессоры, долговременная и оперативная память, хранилища и базы данных, сети), доступ к которым пользователь может получить из любой точки, независимо от места их расположения [1].

В процессе работы вычислительной Грид-сети производится получение результатов вычислений от огромного количества узлов, их объединение и обработка. Если результат вычислений, получаемый от одного из участников Грид-вычислений, будет искажен злоумышленником, то весь комплекс вычислений может оказаться напрасным, что обуславливает важность защиты Грид от искажения результата вычислений.

Для эффективного функционирования Грид-сети важно, чтобы вычислительные узлы с максимальной производительностью корректно производили все необходимые подсчеты.

Злонамеренный пользователь может нарушить работу сети, поэтому необходимо снабдить защитой вычислительные узлы и диспетчер Грид-сети.

Предлагается ввести систему кодирования и сокрытия полученного результата путем периодической генерации алгоритма кодирования результатов и передачи его каждому клиенту сети в виде динамической библиотеки. Генерация библиотеки производится диспетчером. Помимо этого, диспетчер служит для опроса вычислительных узлов на предмет наличия свободных ресурсов и обработки результатов вычисления.

Вычислительная часть принимает динамическую библиотеку, вычисляет результат и передает его в закодированном виде на диспетчер.

Средой передачи данных является Интернет либо локальная сеть, в зависимости от назначений результатов вычислений Грид-сети. Для решений, связанных с глобальными экономическими, медицинскими или общими техническими подсчетами, для передачи данных от диспетчера к вычислительным узлам и наоборот средой передачи данных является глобальная сеть Интернет. Для решений в рамках одной организации достаточно локальной корпоративной сети.

Динамическая библиотека защиты, рассылаемая диспетчером, включает в себя задание, написанное программистами, сопровождающими Грид-сеть, и правила кодирования результата. Она подключается к диспетчеру при необходимости рассылки нового задания вычислительным узлам.

Для защиты предлагается проводить анализ потока управления подпрограммы вычислений с последующим ее разбиением на множество блоков (узлов графа потока управления), применения

запутывающих преобразований к графу потока управления и внедрения специального диспетчера потока управления, проводящего передачу управления от одного блока к другому. Кроме того, в граф потока управления вставляются новые блоки, производящие проверку контрольной суммы исполнимого кода задания и попытки обнаружения и противодействия средствам динамического анализа ПО. Некоторым блокам присваиваются уникальные идентификаторы, включаемые в ходе вычислений в состав результата вычислений в порядке, соответствующем порядку вызова блоков. При этом сокращенное описание графа потока управления с помеченными уникальными идентификаторами блоками сохраняется диспетчером после генерации задания для дальнейшей проверки результата. Функции кодирования результата вызываются не непосредственно, а через делегаты, что значительно усложняет анализ. Поскольку делегат — это ссылка на функцию, то с ними можно работать как с обычными указателями и ссылками.

Последовательность вызова преобразований содержится в специальной таблице делегатов. При вызове каждой функции преобразования таблица делегатов перемешивается. Этими действиями производится изменение графа потока управления программы. Таким образом, задача статического анализа является пр-трудной задачей [2, 3].

Комбинации хранятся на диспетчере после генерации задания. На рис. 1 показан случай, когда вычислительные действия выполняются линейно. На рис. 2 показан случай, когда вычислительные действия разбиваются на блоки с уникальными идентификаторами.

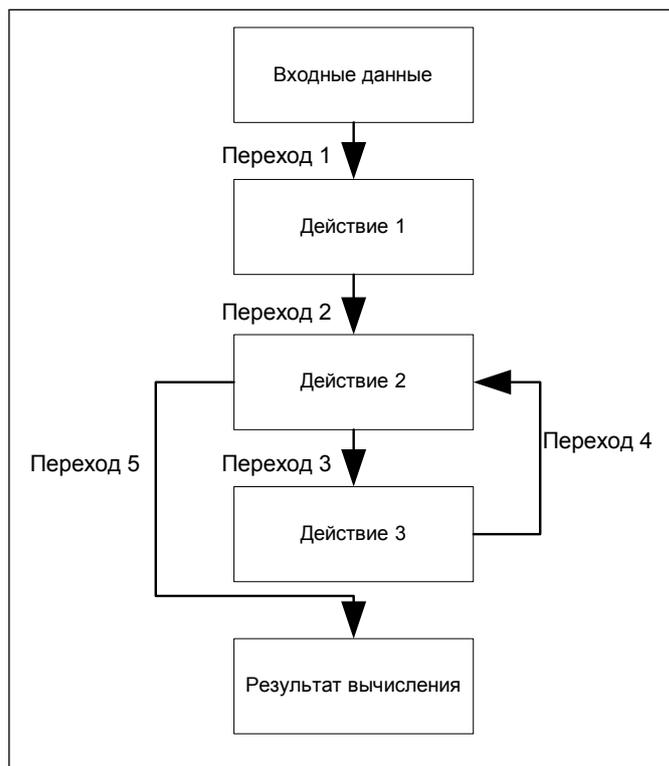


Рис. 1. Линейное исполнение блоков

При генерации каждого задания сервер создает и компилирует динамическую библиотеку. Она содержит в себе алгоритм кодирования результатов вычислений, само вычислительное задание и диспетчер потока управления с таблицей делегатов. Диспетчер Грид передает вычислительным узлам эту библиотеку.



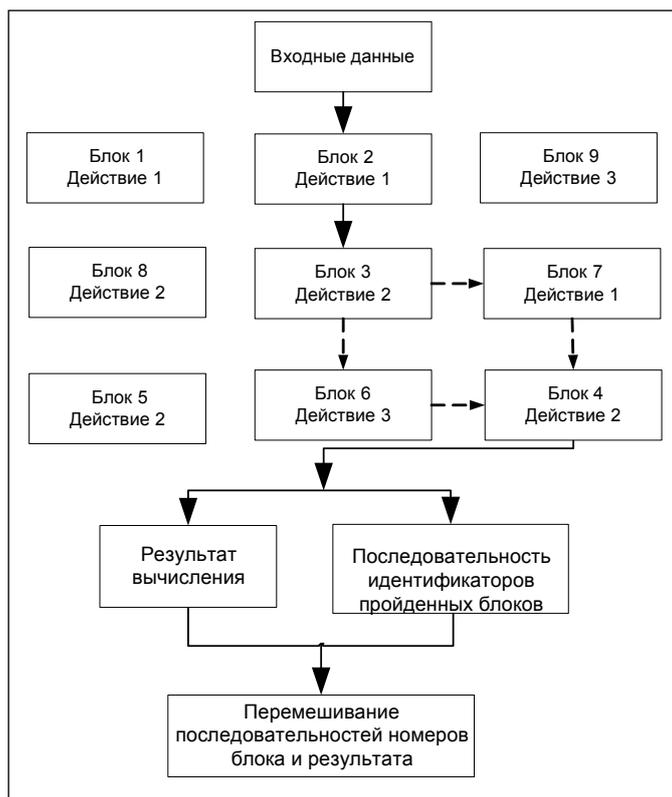


Рис. 2. Разбиение вычисления на блоки

В итоге выполнения вычислительного задания диспетчеру Грид передается сообщение, содержащее результат и последовательность идентификаторов блоков, которые были использованы при вычислении, закодированный с использованием полученного алгоритма кодирования. Диспетчер производит проверку допустимости последовательности выполнения блоков. В случае успешного прохождения проверки результат считается верным.

Был разработан и реализован на языке С# демонстрационный прототип программного обеспечения для вычислительного узла и диспетчера Грид. Программа генерирует задание и алгоритм кодирования результата и сохраняет их в виде текстового файла с исходным кодом динамически подключаемой библиотеки на языке С#. Затем вызывается компилятор, который собирает динамическую библиотеку, и производится ее рассылка вычислительным узлам, где эта библиотека исполняется. Результаты отправляются диспетчеру Грид, где они декодируются.

Далее диспетчер производит анализ последовательности уникальных идентификаторов блоков при помощи таблицы допустимых переходов между блоками. Если хотя бы один из переходов между блоками невозможен, результат считается искаженным и соответствующее задание заново генерируется и отправляется на другой вычислительный узел.

СПИСОК ЛИТЕРАТУРЫ:

1. Фостер Я. Что такое Грид. URL: <http://www.gridclub.ru/library/publication.2004-11-29.5830756248>.
2. Анализ и трансформация программ. URL: http://window.edu.ru/window_catalog/pdf2txt?p_id=27128&p_page=2.
3. Чернов А. В. Интегрированная среда для исследования «обфускации» программ. URL: <http://www.ict.nsc.ru/ws/Lyap2001/2350/>.

