УДК 004.75:004.056

С.Я. Гильгурт, канд.техн.наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев
А.Н. Давиденко, канд.техн.наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев
В.В. Душеба, канд.техн.наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев

АНАЛИЗ ВОПРОСОВ КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В РАСПРЕДЕЛНННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

In the article, based on analysis of current normative and scientific information protection state, a demand list that must be done to development the concept of creating a continuity test system in the Grid environment is formed.

Введение. Ввиду сложности современных объектов моделирования и чрезвычайной трудоемкости проведения соответствующих научных исследований, резко возрастают требования к скорости и надежности обработки больших объемов информации. Решение данных проблем возможно на базе использования достижений в развитии прогрессивных информационных технологий и вычислительной техники. Поэтому обоснованным шагом является применение современных грид-технологий для организации параллельных распределенных вычислений с целью повышения эффективности научных исследований, требующих большого количества расчетов.

Важность результатов решения задач предъявляет особые требования к обеспечению защиты информации в грид-среде. Гарантированное сохранение структуры и содержания, как исполняемых файлов, так и файлов данных в процессе их передачи и хранения обеспечивается системой контроля целостности информации. Контроль целостности файловых объектов в распределенных высокопроизводительных системах является сложной и самостоятельной задачей защиты информации.

Основная часть. Под целостностью информации подразумевается ее свойство сохранять свою структуру и/или содержание в процессе передачи и хранения [1]. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайное или преднамеренное искажение или разрушение.

Контроль целостности секретной пользовательской или системной информации реализуется путем применения программ, выполняющих функции по генерации контрольных сумм и их проверке; обычно используются бесключевые хэш-функции или имитовставки. Контроль целостности защищаемой информации предполагает систематичность ее проведения [2]. Например, либо администратор безопасности должен инициировать ее с помощью организационных мер, либо в прикладное или системное программное обеспечение (ПО) должны быть встроены функции контроля целостности, которые автоматически вызываются непосредственно перед началом работы с защищаемой информацией.

Анализ последних достижений и публикаций по указанной теме показывает, что использующиеся в современных грид-сетях механизмы безопасности ориентированы преимущественно на защиту от внешних по отношению к грид-инфраструктуре субъектов. В то же время вопросы контроля целостности системного, промежуточного и прикладного программного обеспечения грид-узлов, а также программ и данных грид-пользователей остаются открытыми.

Таким образом, возникает необходимость в расширении штатных возможностей информационной безопасности грид-инфраструктуры, в частности, во введении дополнительных функций контроля целостности информации и программных средств, использующихся в грид-узлах.

Целью настоящей работы является разработка в первом приближении концепции, которая может послужить основой для создания системы контроля целостности в грид-среде (СКЦГС). Для проверки концепции планируется разработка и исследование пробной версии системы на базе грид-узла ИПМЭ им. Г.Е. Пухова НАНУ.

Для осуществления контроля целостности необходимо вводить избыточность либо в процесс обработки информации (например, аутентификация), либо в саму информацию (например, электронная подпись) либо в архитектуру системы (дублирование критичных блоков).

Понятие целостности, как и состав функциональных услуг для ее реализации, эволюционировали по мере развития теории защиты информации что, в различной трактовке, нашло отражение в ряде нормативных документов информационной безопасности. К таким документам можно отнести следующую последовательность стандартов: «Критерии безопасности компьютерных систем министерства обороны США» («Оранжевая книга»), Руководящие документы Гостехкомиссии России, «Европейские критерии безопасности информационных технологий, «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» и «Единые критерии безопасности информационных технологий» [3, 4].

Применительно к Украине наиболее значимый нормативный документ технической защиты информации (НД ТЗИ) – «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа» [5]. Данный документ совместно с НД ТЗИ 1.1-003-99 «Терминология в области защиты информации в компьютерных системах от несанкционированного доступа» [6] рассматривает два понятия: *целостность информации* и *целостность системы*.

Целостность информации (information integrity) – свойство информации, состоящее в том, что информация не может быть модифицирована неавторизированным пользователем и/или процессом.

Целостность системы (system integrity) – свойство системы, состоящее в том, что ни один ее компонент не может быть удален, модифицирован или добавлен с нарушением политики безопасности.

НД ТЗИ 2.5-004-99 рассматривает четыре функциональных услуги, связанные с целостностью информации:

- доверительная целостность;
- административная целостность;
- откат;
- целостность при обмене,

а также одну услугу, связанную с целостностью системы:

- целостность комплекса средств защиты.

Последняя функциональная услуга является обязательной для всех систем защиты.

В скрытом виде требования по целостности также присутствуют в критериях гарантий. Например, требования к среде разработки состоят в том, что должна использоваться система мер технической, физической, организационной и кадровой безопасности, направленная на защиту всех средств и материалов, используемых при генерации комплекса средств защиты от несанкционированной модификации или разрушения.

Таким образом, создание концепции, которая может послужить основой для создания системы контроля целостности в грид-среде, является важной и нетривиальной научно-технической задачей. Ее решение должно: опираться на основные положения НД ТЗИ 2.5-004-99; использовать имеющийся опыт создания систем контроля целостности; учитывать новые требования, возникшие в связи с появлением грид-технологий.

На сегодняшний день разработано большое число систем контроля целостности, как коммерческих, так и свободно распространяемых, различающихся операционными средами, архитектурой (автономные либо клиент-серверные), функциональным составом и предоставляемыми возможностями. Причем, контроль целостности файловых объектов представляет собой самостоятельную задачу защиты информации. Основу механизмов контроля целостности файловых объектов представляет проверка соответствия контролируемого объекта эталонному образцу. Для контроля могут использоваться контрольные суммы, а также ряд иных признаков, таких как дата последней модификации объекта и т.п. В случае необходимости соблюдения строгого соответствия контролируемого объекта эталонному состоянию, данные механизмы могут осуществлять автоматическое либо автоматизированное (под управлением пользователя или администратора безопасности) восстановление несанкционированно измененного файлового объекта из резервной копии.

Основным вопросом при реализации механизмов контроля целостности файловых объектов является выбор принципов и механизмов запуска процедуры контроля. Синхронный запуск, т.е. запуск контроля по расписанию, следует рассматривать лишь в качестве дополнительного механизма, поскольку без существенного снижения производительности системы он должен производиться достаточно редко.

Контролируемые файловые объекты могут быть классифицированы в соответствии с функциональным назначением:

- исполняемые файлы (программы);
- файлы данных [7].

Существующие системы контроля целостности (СКЦ) – integrity checkers – являются важным компонентом средств информационной безопасности и относятся к категории систем обнаружения последствий совершенных атак. Контроль целостности файлов (называемый также целевым анализом – target-based), использует пассивные, не оказывающие заметного влияния на работу, методы проверки объектов системы и их атрибутов, таких как исполняемые программные модули, динамические библиотеки, драйверы, конфигурационные файлы, базы данных, записи системного реестра [8].

Системы целевого анализа работают по замкнутому циклу, обрабатывают файлы, системные объекты и их атрибуты – вычисляют контрольные суммы, бесключевые хэш-функции либо имитовставки, которые затем сравнивают с эталонными значениями, найденными заранее, что позволяет выявлять изменения. В случае обнаружения нарушения целостности генерируется соответствующее сообщение, а также фиксируется время выявления изменения.

Необходимость поиска новых подходов при реализации функциональных услуг безопасности, обеспечивающих целостность информации в грид-среде, обусловлена, ее специфическими особенностями. С точки зрения авторов к таким особенностям можно отнести:

- разнородность системного, вспомогательного, промежуточного (middleware), инструментального и прикладного ПО;
- необходимость контролировать целостность помимо системной информации на кластерах грид-узлов также программ и данных пользователей;
- проблема разделения административных полномочий и сфер влияния, конфликт интересов участников вычислительного процесса;
- необходимость оперативного предоставления пользователю грид-инфраструктуры информации о целостности ресурсов, на которых будет решаться его задача.

На основе выше изложенного сформирован перечень заданий, который должен быть выполнен для успешного решения поставленной задачи. Перечень включат следующие пункты:

1. Анализ текущего состояния дел по проблеме контроля целостности в существующих грид-системах. Формулировка требований, предъявляемых к СКЦГС.

2. Анализ специфических особенностей грид-среды, отличающих ее от традиционных компьютерных систем в плане решения задачи контроля целостности информации. Анализ существующих технических решений по

системам контроля целостности, а также их компонентов на предмет применимости в СКЦГС.

3. Анализ системного программного обеспечения типового грид-узла, а также механизмов исполнения заданий пользователя в грид-среде с целью выделения и классификации объектов, целостность которых подлежит контролю.

4. Разработка структуры и состава СКЦГС, определение функциональности ее компонентов. Анализ возможностей использования штатных средств защиты информации существующих грид-систем для реализации функциональности СКЦГС. Решение вопросов интеграции сервисов СКЦГС в действующую грид-инфраструктуру Украины.

5. Выбор оптимальных технических решений. Адаптация существующих систем контроля целостности, проектирование и разработка оригинальных компонентов СКЦГС.

Выводы. Разработка концепции, которая может послужить основой для создания системы контроля целостности в грид-среде является важной и нетривиальной научно-технической задачей.

Данная концепция должна опираться на основные положения НД ТЗИ 2.5-004-99, использовать имеющийся опыт создания систем контроля целостности и учитывать новые требования, возникшие в связи с появлением грид-технологий.

Для реализации концепции создания СКЦГС необходимо выполнить сформированный авторами перечень заданий.

1. *Соколов А.В.* Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – ДМК Пресс, 2002. – 656 с.
2. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – М.: ДМК, 2000. – 448 с.
3. *Зегжда Д.П.* Основы безопасности информационных систем / Д.П. Зегжда, А.М Ивашко. – М.: Горячая Линия - Телеком, 2000. – 452 с.
4. *Давиденко А.Н.* Анализ критериев безопасной обработки информации в КС / А.Н. Давиденко // Моделювання та інформаційні технології : зб. наук. пр. – К.: ІПМЕ НАНУ, 1999. – Вип. 3. – С. 155-160.
5. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа : НД ТЗИ 2.5-004-99. – К.: ДСТСЗИ СБ Украины, 1999. – 53 с.
6. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа: НД ТЗИ 1.1-003-99. – К.: ДСТСЗИ СБ Украины, 1999. – 24 с.
7. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384с.
8. *Лукацкий А.В.* Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2001. – 624 с.

Поступила 24.02.2011р.