УДК 681.3

АДАПТИВНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Луцкий Г. М., д. т. н., проф., Мухин В. Е., к. т. н., доц.
Национальный технический университет Украины
«Киевский политехнический институт»
Украина, Киев, пр. Победы, 37
E-mail: mukhin@comsys. ntu-kpi. kiev. ua

Запропоновано адаптивний підхід до створення безпечних розподілених комп'ютерних систем (РКС), який дозволяє забезпечити необхідний рівень їх захищеності. Для гарантування цілісності інформації, що обробляється, запропоновано методи та засоби віддаленого завантаження операційного середовища на робочі станції. Застосування розроблених механізмів дозволяє створити безпечні РКС, до складу яких входять попередньо небезпечні ресурси, що особливо важливо в практичних застосуваннях.

Ключові слова: адаптація, захищенність, розподілені комп'ютерні системи

Is suggested the adaptive approach to creation of the secured distributed computer systems (DCS), which allows ensure a required security level for DCS. Also, there are suggested the methods and means for operating environment remote loading on workstations, which allow ensure the data integrity in DCS. The applying of the developed mechanisms allows create secured DCS with initially unsecured resources, that is especially important in the real practice.

Keywords: adaptation, security, distributed computer systems

Введение. Одной из новейших областей в разработке компьютерных систем является кластеризация, которая представляет собой альтернативу симметричной многопроцессорной обработке и сочетает высокую производительность и доступность, что особенно эффективно для серверных приложений. Кластер определяется как группа взаимосвязанных, совместно работающих компьютеров, называемых узлами или рабочими станциями (РС), которые представляют собой единый вычислительный ресурс. При этом создается эффект работы единой компьютерной системы, а также достигается высокая доступность ресурсов кластера путем балансировки загрузки и реакции на отказы отдельных компонентов. Подобные системы получили название кластерные распределенные компьютерные системы (РКС).

Ввиду постоянного расширения периметра использования кластерных распределенных компьютерных систем, широкого применения их в государственных, военных и коммерческих учреждениях, возникает проблема обеспечения безопасности хранящейся и обрабатываемой в них информации. В этой связи разработка методов и средств защиты данных в распределенных компьютерных системах является не только актуальной, но и необходимой.

Цель работы. Разработка адаптивного подхода к обеспечению безопасности РКС на основе интеграции в защищаемую систему настраиваемых средств контроля доступа, средств обеспечения целостности данных и средств управления конфигурацией программного обеспечения РС с учетом требуемого уровня защищенности РКС.

Материалы и результаты исследований. Кластерные РКС обладают четырьмя важными свойствами [1, 2]:

1) абсолютная масштабируемость – возможность создания кластеров любых размеров, которые способны по суммарной производительности превысить вычислительные мощности любого компьютера;

2) инкрементальная масштабируемость – кластер конфигурируется таким образом, чтобы можно было добавлять новые компьютеры-рабочие станции малыми порциями;

3) высокая доступность – сбой в работе или выход из строя одной из рабочих станций не приводит к снижению уровня производительности за счет реконфигурации ресурсов;

4) оптимальное отношение цена/производительность – кластерная система оказывается менее дорогой, чем отдельный компьютер аналогичной вычислительной мощности.

На рис.1 показана обобщенная структурная схема кластерной РКС.

Менеджер РС отвечает за поддержку участия данной РС в составе кластера. Периодически он посылает контрольные сообщения менеджерам других РС кластера. В случае, когда менеджер РС обнаруживает, что поток сообщений от некоторой РС прервался, он посылает широковещательное сообщение всем менеджерам РС кластера, что заставляет их обменяться сообщениями для проверки текущей конфигурации кластера. Если менеджер РС не отвечает на это сообщение, РС удаляется из кластера, и ее активные группы пересылаются одной или нескольким активным РС кластера.

Рисунок 1 – Обобщенная структурная схема кластерной РКС

Менеджер базы данных конфигураций поддерживает базу данных конфигурации кластера. Эта база данных содержит информацию о ресурсах и группах, а также о принадлежности РС к определенной группе. Менеджеры баз данных каждой из РС обмениваются данными друг с другом для поддержки согласованной картины конфигурационной информации.

Менеджер ресурсов и менеджер преодоления сбоев принимают все решения, связанные с группами ресурсов и инициируют требуемые действия кластера. В процессе преодоления сбоев соответствующие менеджеры выполняют перераспределение групп ресурсов отказавшей РС среди оставшихся работоспособных РС. Когда отказавшая РС вернется в рабочее состояние, менеджер преодоления сбоев может принять решение о возврате некоторых групп этой РС. В частности, у каждой группы может быть указан предпочтительный владелец и после восстановления работоспособности данного владельца группа может быть возвращена ему.

Процессор событий управляет инициализацией сервиса кластера, связывается со всеми компонентами сервиса кластера и обрабатывает обычные операции. Менеджер коммуникаций управляет обменом сообщениями с другими РС кластера.

Средства и методы защиты информации в кластерных РКС. Методологической основой применяемых механизмов безопасности в РКС являются стандарты международной организации по стандартизации ISO и эталонные модели взаимодействия открытых систем (ЭМВОС) [3]. В настоящее время лишь комплексный подход к защите информации, т. е. реализация всех базовых функций защиты информации, позволяет поддержать требования стандартов к обеспечению безопасности информации. при этом ключевую роль в системе защиты РКС играют системы контроля доступа и разграничения полномочий как наиболее универсальные средства защиты информации [4].

Большинство используемых локальных и сетевых операционных систем (ОС) были разработаны без учета требований к защите информации, поэтому они являются либо вообще незащищенными, либо средства защиты и контроля доступа в них играют роль дополнений к исходной системе. Операционные системы, в которых средства обеспечения безопасности информации предусматривались уже в процессе их разработки, появились только в последние 10 –15 лет [3].

Таким образом, сложилась ситуация, для которой характерно использование самых различных операционных систем в рамках одной РКС. Поэтому, остается актуальной задача обеспечения взаимодействия операционных систем с разной степенью защищенности. Например, на практике часто возникает необходимость обеспечить безопасную работу пользователя за рабочей станцией, на которой установлена незащищенная ОС.

Адаптивный подход к построению защищенных РКС. В общем выделяются три основных подхода к построению защищенных РКС:

1) Разработка новых систем, в которых решается весь комплекс проблем защиты информации (креативный подход).

2) Модификация существующих РКС с целью дополнения их функциями защиты информации (аддитивный подход).

3) Разработка подсистем защиты информации, реализующих отдельные задачи обеспечения безо-

пасности данных, и их адаптация к существующим РКС (адаптивный подход).

Креативный подход предлагает наиболее радикальный способ решения проблемы обеспечения безопасности информации. Однако разработка новой сложной информационной системы требует значительных временных и финансовых затрат. В связи с этим широкое распространение получил аддитивный подход к построению защищенных систем. Применение данного подхода позволяет сократить время на разработку защищенной системы за счет использования существующих прикладных средств обработки информации. Однако, анализ современных средств, построенных на основе аддитивного подхода, показывает высокую уязвимость подобных систем. Это, в частности, связано с многовариантностью путей обмена информацией в современных прикладных системах, что не позволяет обеспечить надежный контроль над всеми информационными потоками.

Адаптивный подход является развитием этих двух подходов. Он принципиально отличается от двух предыдущих тем, что система безопасности создается путем интеграции средств защиты к стандартным прикладным средствам и адаптации средств защиты к требуемому уровню безопасности каждой подсистемы или системы в целом. При использовании адаптивного подхода, в отличие от креативного, система строится на основе готовых блоков, что заметно снижает трудоемкость разработки. Принципиальное отличие от аддитивного подхода состоит в технологии объединения прикладных средств и средств защиты, которая подразумевает плановую интеграцию средств защиты с прикладной системой и их адаптацию к требуемому уровню безопасности. Таким образом, сохраняя преимущества как аддитивного (совместимость со стандартным ПО), так и креативного (системные принципы построения архитектуры безопасности) подходов, адаптивный подход устраняет некоторые присущие им недостатки.

Для реализации адаптивного подхода построения РКС предлагается специальная методика на основе следующих принципов:

1) разграничение среды обработки и среды хранения информации;

2) унификация всех взаимодействий в системе;

3) выделение средств защиты в отдельные подсистемы;

4) стандартизация интерфейса взаимодействия подсистем защиты с другими подсистемами РКС.

Разделение среды обработки и среды хранения информации обусловлено необходимостью анализа обращений к информационным ресурсам и управления доступом к ним. Анализ всех информационных потоков возможен лишь в том случае, если все взаимодействия между средой обработки и средой хранения информации осуществляются на основе механизма передачи сообщений.

Унификация взаимодействий в системе позволяет упростить реализацию механизма управления доступом, и, соответственно, снизить вероятность ошибок в реализации данного компонента.

Реализация средств защиты в виде отдельных подсистем позволяет разрабатывать их независимо от модулей, реализующих прикладные функции. При этом необходима стандартизация интерфейса взаимодействия подсистем защиты между собой и с другими подсистемами.

Применение средств защиты на прикладном уровне дает возможность создавать средства обеспечения безопасности без привязки к конкретной операционной системе. Недостаток реализации средств и механизмов защиты внутри приложений состоит в том, что они могут стать специфичными для конкретного приложения, что не позволит повторно использовать уже разработанные механизмы защиты и ведет к дублированию разработок.

Для устранения данного недостатка предлагается предоставлять приложениям доступ к функциям защиты, используя общий стандартный интерфейс сервиса прикладного уровня, что позволит избежать дублирования реализаций, а также решить проблему добавления новых средств защиты в систему. Предлагаемая методика является достаточно универсальной и может применяться как при разработке РКС, так и при построении защищенных ОС и сложных прикладных программных комплексов.

Модель защищенной РКС.

Использование средств защиты в виде самостоятельных служб, реализованных без привязки к конкретной ОС, требует разработки специальных методов, позволяющих интегрировать такие службы в прикладную систему.

Рассмотрим модель РКС, в которую предполагается внедрение средств защиты. Введем понятия субъекта, объекта и пользователя системы.

Пользователь – физическое лицо, аутентифицируемое некоторой информацией и управляющее субъектами системы через средства управления компьютерной системой. Субъект – активный ресурс, осуществляющий какие-либо действия над другими ресурсами. Объект – пассивный ресурс, используемый субъектом для выполнения операций. Обозначим через $O=\{o_i\}$ множество всех объектов системы и назовем данное множество средой хранения информации. Обозначим через $S=\{s_i\}$ множество всех субъектов системы и назовем данное множество средой обработки информации.

Взаимодействие субъектов и объектов системы осуществляется путем посылки субъектами сообщений объектам. Пусть P – множество сообщений между субъектами и объектами. Данное множество разобьем на два непересекающихся подмножества $P = N \cup L$, $N \cap L = \varnothing$, где N – множество сообщений, характеризующее несанкционированный доступ, L – множество легальных сообщений.

Критерий разбиения на множества N и L определяет заданная политика безопасности. Правила разграничения доступа субъектов к объектам – формально описанные выражения, принадлежащие

множеству L. Политика безопасности должна включать:

- множество методов доступа $A=\{a_i\}$;
- для каждой пары «субъект – объект» (s_i, o_j) подмножество $A' \subseteq A$ методов доступа, которые разрешены для данной пары.

Введем в систему специальный субъект – монитор безопасности РКС. Монитор безопасности РКС – это монитор обращений, который разрешает лишь те сообщения, которые принадлежат множеству легальных сообщений L. Основной операцией, выполняемой монитором безопасности, является проверка каждого отдельного сообщения (1):

$$r = Access\ (s_i, o_j, a_k), \qquad (1)$$

где $a_k \in A$ – конкретный тип доступа из множества допустимых; $r \in$ {TRUE, FALSE} – решение о предоставлении доступа, причем r = TRUE, если доступ a_k субъекта s_i к объекту o_j разрешен и r = FALSE в противном случае.

Для принятия решений о предоставлении доступа используется база данных (БД) правил безопасности, в которой хранятся атрибуты безопасности всех субъектов и объектов, а также сами правила разграничения доступа. Вся информация о работе средств защиты протоколируется в журнале аудита. Полученная в результате модель РКС с внедренными средствами контроля доступа приведена на рис. 2.

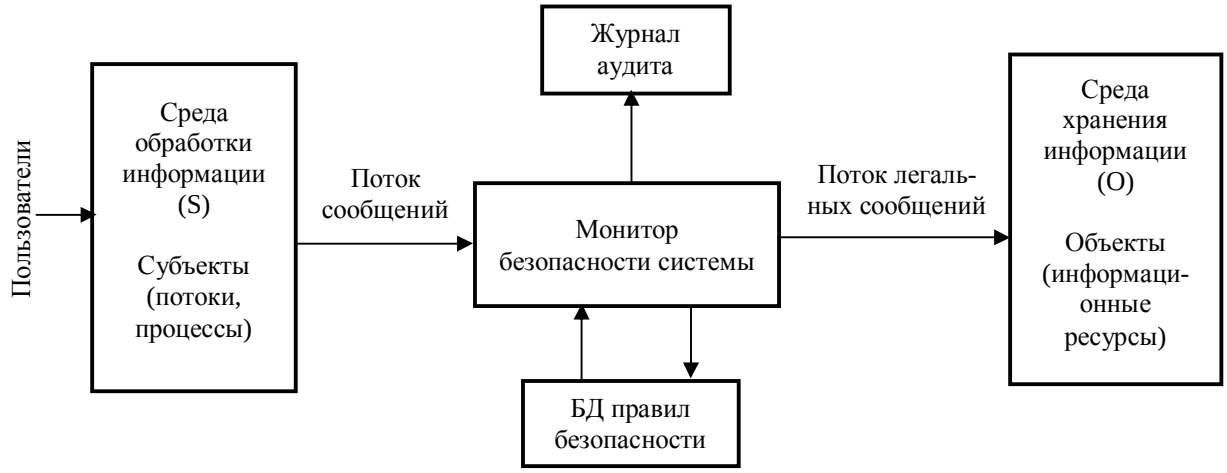

Рисунок 2 – Модель РКС с интегрированными средствами контроля доступа

Предложенная модель системы позволяет эффективно внедрить формальную модель безопасности (ФМБ), построенную по принципу предоставления прав доступа.

Средства обеспечения целостности информации в РКС.

Для решения задач обеспечения целостности среды обработки информации в РКС предлагается подход на основе удаленной загрузки операционной среды на рабочую станцию. Применение удаленной загрузки операционной среды позволяет обеспечить целостность образа среды обработки информации, а именно, целостность начальной конфигурации рабочей станции и целостность программ обработки данных. Образ операционной среды хранится на специально выделенном сервере удаленной загрузки. При запуске рабочей станции происходит считывание данного образа с сервера, проверка его на целостность и загрузка в память станции всего необходимого системного и прикладного программного обеспечения (ПО). Выполнение этой процедуры гарантирует, что при каждом включении станция будет находиться в безопасном начальном состоянии (ПО станции находится в заданной конфигурации и целостность его проверена).

Для описания метода обеспечения целостности образа операционной среды рабочей станции дополним рассмотренную выше модель защищенной РКС. Пусть $U=\{u_i\}$ множество пользователей системы, $T=\{t_i\}$ – множество терминалов РКС, $OS=\{os_i\}$, $OS \subseteq O$ – множество образов операционных сред, $Z=\{z_i\}$ – множество операционных сред. Кроме того, в модель РКС введен специальный субъект – сервер удаленной загрузки рабочих станций, основной функцией которого является генерация операционной среды рабочей станции на основе информации о пользователе u_l, терминале t_m, с которого инициирована загрузка и заранее подготовленного образа операционной среды os_i рабочей станции (2):

$$Create\ (t_m, u_l, os_i) \rightarrow z_k. \qquad (2)$$

Архитектура подсистемы загрузки операционной среды на рабочую станцию приведена на рис. 3.

Алгоритм загрузки операционной среды на рабочую станцию состоит из следующих этапов:

1) идентификация терминала t_m;

2) идентификация пользователя u_l;

3) проверка прав пользователя u_l по использованию рабочей станции t_m;

4) выбор образа операционной среды os_i для загрузки;

5) контроль целостности образа операционной среды os_i;

6) очистка остаточной памяти терминала t_m;

7) удаленная загрузка проверенной на целостность операционной среды os_i на терминал t_m.

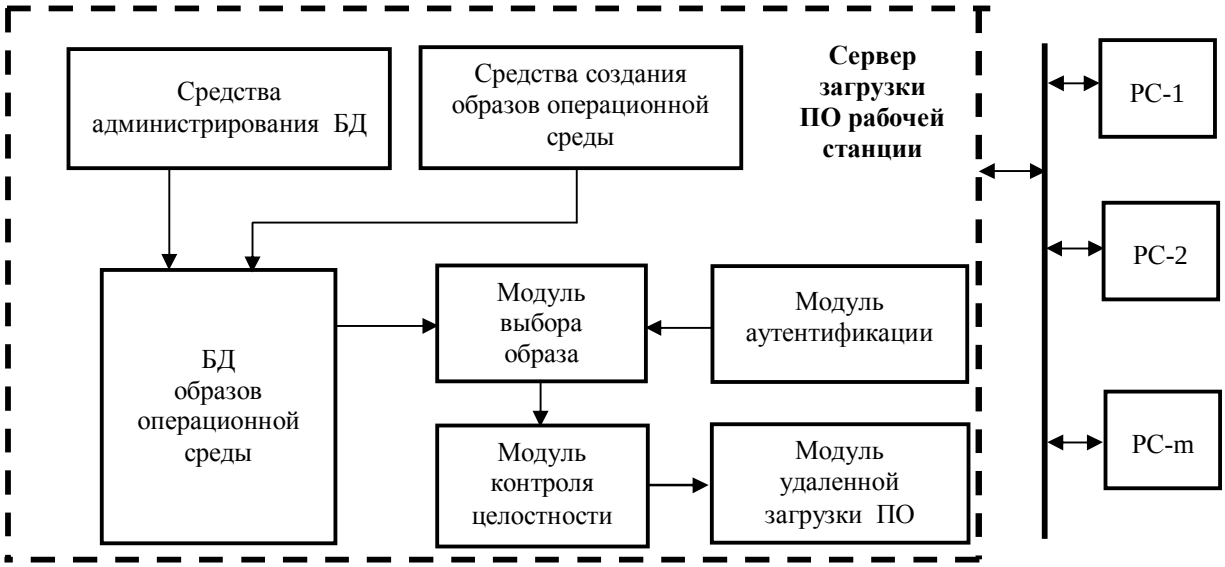

Рисунок 3 – Архитектура подсистемы удаленной загрузки операционной среды рабочей станции

Предлагается общая методика удаленной загрузки ОС для РКС, которая включает в себя следующие этапы:

1) Инициализация удаленной загрузки. В ходе этапа выполняются следующие действия: определение адреса сервера удаленной загрузки, идентификация терминала, получение параметров начальной загрузки с сервера (сетевое имя PC, сетевой адрес и др.), получение образа начальной загрузки и передача ему управления.

2) Запуск начального загрузчика. Данный этап выполняется кодом начального загрузчика, полученным на предыдущем этапе с сервера. В ходе этапа выполняются такие действия: дополнительная идентификация и аутентификация терминала, идентификация и аутентификация пользователя, инициализация загрузки и подготовка к запуску на станции штатной оболочки для данного пользователя.

3) Запуск оболочки рабочей станции. Данный этап выполняется кодом оболочки рабочей станции. В ходе этапа выполняется загрузка ядра операционной системы, а также дополнительная идентификация и аутентификация пользователя, загрузка рабочего стека протоколов, после чего инициируется процесс настойки персональной конфигурации ПО пользователя.

4) Настройка персональной конфигурации ПО PC пользователя. Данный этап выполняется кодом оболочки рабочей станции. В ходе этапа выполняются следующие основные действия: подключение сетевых ресурсов, окончательная загрузка и настройка среды работы пользователя. Также на данном этапе устанавливается требуемый уровень защищенности программно-аппаратных средств PC.

Применение данной методики позволяет универсальным образом осуществлять загрузку операционной среды на рабочие станции в РКС.

Выводы. Предложенные механизмы безопасности РКС позволяют обеспечить контроль доступа к информационным ресурсам системы, а также гарантировать целостность образа операционной среды рабочих станций. Разработанный адаптивный подход основывается на концепции разделения среды обработки и среды хранения информации, на абстракции информационного ресурса, на стандартизации и отделении средств защиты от прикладных средств, на разделении механизмов контроля доступа и реализации правил политики безопасности, а также на максимальной унификации всех взаимодействий в системе.

Выполнение указанных функций средств защиты не требует использования специальных средств обработки информации и модификации стандартных прикладных средств. Средства защиты и методы их интеграции реализуются таким образом, что они позволяют компенсировать уязвимости прикладных средств обработки. В результате предоставляется возможность создания безопасных РКС, в которых для обработки информации используется изначально небезопасное прикладное ПО, что особенно важно в практических приложениях.

ЛИТЕРАТУРА

1. Buyya R. High Performance Cluster Computing: Programming and Applications. – NJ, Prentice Hall, 1999. – 532 p.

2. Столлингс В. Операционные системы. Внутреннее устройство и принципы проектирования. М.: изд-во «Вильямс», 2002. – 844 с.

3. Щербаков А. Ю. Компьютерная безопасность. Теория и практика. — М.: изд-во «Нолидж», 2001. – 352 с.

4. Farmer W. M., Guttman J. D., Swarup V. Security for Mobile Agents: Issues and Requirements.// Proc. of 19-th National Information Systems Security Conf., 1996. – pp. 591– 597.

Статья поступила 26.09.2007
Рекомендовано к печати к. физ. — мат. н., доц. Ляшенком В. П.