(таково количество студентов в подгруппе, с которой преподаватель проводит в дисплейном классе предусмотренное расписанием занятие).

Была проведена исследовательская работа, на основании которой были рассмотрены возможные способы реализации стенда. Был изучен вариант с аппаратной конфигурацией узлов под управлением операционной системы Linux и разделяемым дисковым пространством, реализуемым с помощью технологии iSCSI. Этот вариант обеспечивает приемлемую производительность работы стенда и в то же время накладывает наименьшие ограничения в выборе аппаратных компонентов и необходимости лицензирования.

Проводился набор испытаний собранного кластера по требованиям масштабируемости и высокой доступности. Удалось добиться увеличения пропускной способности тестируемой системы при работе в кластерной конфигурации по сравнению с работой в конфигурации с одним узлом. Тип нагрузки, при котором проводилось сопоставление кластерного и бескластерного вариантов тестируемых систем, — динамическая обработка транзакций. Также удалось продемонстрировать прозрачное переключение сессий СУБД на другой узел в случае отказа отдельных компонентов кластера. Проведенные исследования на стенде с аппаратной реализацией кластеров Oracle помогли перейти к реализации варианта демонстрации кластерных технологий с использованием нескольких виртуальных машин [4], устанавливаемых на каждом рабочем месте студента в дисплейном классе, где проходят занятия.

По результатам работы было подготовлено описание лабораторной работы «Повышение доступности базы данных технологиями Oracle RAC». Подготовка дисплейного класса к выполнению лабораторной работы предполагает «разливку» на компьютеры на рабочих местах студентов заранее подготовленного администратором дисплейного класса образа с виртуальными машинами (с установленным на них необходимым программным обеспечением Oracle), настроенными под технологии Oracle RAC.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hunter J.* Build Your Own Oracle RAC 10g Release 2 Cluster on Linux and Firewire. URL: http://www.oracle.com/technology/pub/articles/hunter_rac10gr2.html.
2. *Dyke J., Shaw S.* Pro Oracle Database 10g RAC on Linux: Installation, Administration, and Performance. Apress, 2006.
3. *Hunter J.* Build Your Own Oracle RAC Cluster on Oracle Enterprise Linux and iSCSI. URL: http://www.oracle.com/technology/pub/articles/hunter_rac10gr2_iscsi.html.
4. *Chang V.* Install Oracle 10g on Enterprise Linux Using VMWare Server. URL: http://www.oracleracsig.org/pls/apex/Z?p_url=RAC_SIG.download_my_file?p_file=1001522&p_id=1001522&p_cat=documents&p_user=nobody&p_company=994323795175833.

Д. О. Ковалев, Н. Г. Милославская

АДАПТИВНАЯ ЗАЩИТА АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЫ ПРИ ПОМОЩИ ОПЕРАЦИОННОГО ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При создании системы защиты в банке, как и в любой другой организации, необходимо одновременно обеспечивать защищенность активов и удобство использования АБС. Поддержание данного

баланса особенно актуально сейчас, поскольку банкам необходимо привлекать новых и удерживать существующих клиентов в непростых условиях экономического кризиса. Безопасность банка, интерактивность и простота предоставляемых клиентам банка сервисов, а также скорость работы банковских сотрудников могут быть определяющими факторами в борьбе с конкурентами. Однако часто меры защиты сильно понижают удобство пользования банковскими системами и сервисами. Для решения данной проблемы предлагается создание адаптивной системы безопасности.

Подобные системы часто встречаются в областях, смежных с ИБ. В качестве примера можно привести систему пожаротушения: при отсутствии дыма — ситуации, которая не сигнализирует об опасности, — ничего не происходит, в случае задымления помещения срабатывает датчик-детектор и комнату заливает водой. При этом ложное срабатывание приводит к минимальным негативным последствиям, а в случае реального пожара критичные активы будут спасены. Таким образом, система пожарной безопасности адаптивно подстраивается под условия внешней среды.

Термин «адаптивная безопасность» давно существует в сфере ИБ. Часто под этим термином понимается способность системы безопасности справляться с атаками нулевого дня. Однако в соответствии со значением самого слова «адаптивный» правильнее подразумевать под этим термином способность системы защиты приспосабливаться к различным угрозам ИБ. С учетом требований, которые банковские организации предъявляют к системам защиты, адаптивная система должна, с одной стороны, обеспечивать необходимую защищенность, с другой — удобство использования. Именно подобную адаптивную систему безопасности возможно реализовать в рамках ОЦИБ. Это обусловлено следующими факторами:

— сегодня как никогда много параметров, на основании которых можно принимать управляющие воздействия (сообщения ИБ, результаты корреляционного анализа, требования политики безопасности, нормативных документов, соглашений о предоставлении услуг и т. п.);

— средства защиты информации (СЗИ) на сегодняшний день обладают развитым функционалом и гибкими настройками. Возможность динамического выбора необходимых настроек безопасности создает основу для адаптивной защиты;

— ОЦИБ концентрирует в себе огромное количество знаний по безопасности банковской организации, а также является центральной точкой управления СЗИ и развертывания политик ИБ, поэтому идеален для реализации адаптивной безопасности;

–принятие закона о персональных данных и стандарта PCI DSS привело к ужесточению требований по обеспечению защищенности АБС;

— в связи с развитием социальных сетей сильно изменился облик типичного банковского работника, потому к интерактивности банковских сервисов и так называемому опыту и ощущениям пользователя при работе с АБС также предъявляются повышенные требования.

В типовой банковской организации существует большое количество СЗИ (таких, как средства контроля доступа, системы обнаружения и предотвращения вторжений (СОВ), межсетевые экраны (МЭ), СОВ уровня хоста и т. п.) При этом СОВ может работать в режимах обнаружения или предотвращения, МЭ способен работать на разных уровнях протоколирования событий ИБ, СОВ уровня хоста может реализовывать различные по строгости политики. Защищенность АБС зависит от различных факторов: количества угроз ИБ, уязвимости конечных систем и СЗИ, настроек системы безопасности и т. п. При этом на определенные факторы организация влиять не может (например, количество угроз ИБ), а ряд факторов может быть изменен (например, в случае появления новой уязвимости будет обновлено ПО). Однако самый быстрый способ повлиять на защищенность системы — это изменить настройки системы безопасности.

Таким образом, адаптивная система безопасности — это система, которая влияет на свои настройки в зависимости от различных факторов и тем самым обеспечивает необходимый уровень

защищенности, функциональности, производительности и удобства использования. Выбор нужных настроек безопасности осуществляется на основании методов поддержки принятия решений с использованием многомерной информации, хранящейся в ОЦИБ (Рис. 1). Адаптивный ОЦИБ оценивает состояние защищенности банковской организации и динамически формирует некоторую консолидированную оценку защищенности АБС. По результатам этой оценки ОЦИБ вырабатывает управляющее воздействие — какие настройки безопасности должны быть применены в настоящий момент:

— минимальные настройки безопасности — слабая защита, высокое удобство пользования;

— усиленные настройки безопасности — сильная защита, низкое удобство пользования;

— стандартные настройки безопасности — компромиссный вариант между первыми двумя.

Выбор настроек в зависимости от внешних факторов позволит влиять на поведение системы и тем самым повысить одновременно защищенность и удобство пользования АБС, что подтверждено результатами моделирования и рабочим экспериментом.

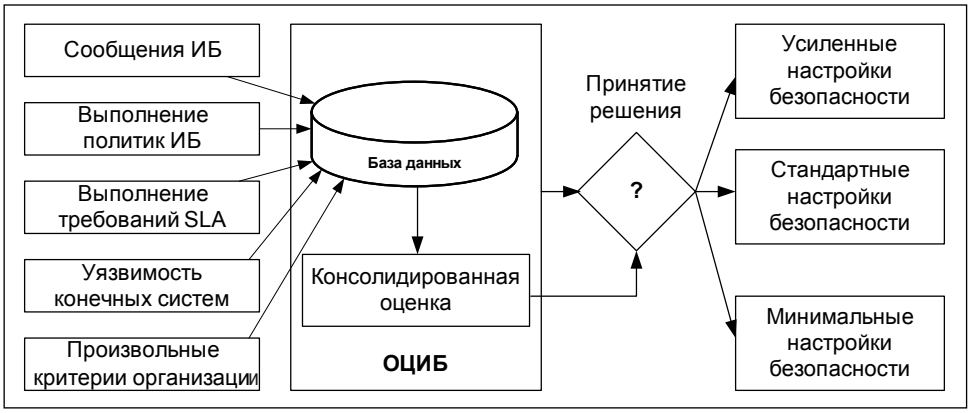

Рис. 1. Схема работы адаптивного ОЦИБ

Д. О. Ковалев, Н. Г. Милославская

МЕЖКОРПОРАТИВНАЯ КОРРЕЛЯЦИЯ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автоматизированные банковские системы (АБС) исторически считались закрытыми средами. Однако сегодня доступ к определенной банковской информации предоставляется широкому кругу лиц при помощи служб дистанционного банковского обслуживания (ДБО). ДБО реализуется посредством банковских интернет-приложений. Данные приложения позволяют клиентам банка управлять своим банковским счетом и пользоваться другими финансовыми услугами, не отходя от персонального компьютера. Общение с подобными приложениями происходит в интерактивном режиме через веб-сайт, размещенный в сети Интернет. Поскольку к веб-сайту могут обращаться как законные пользователи, так и злоумышленники, необходимо использование соответствующих средств защиты. При этом базовые механизмы защиты — аутентификация пользователей, шифрование данных и межсетевое экранирование — часто оказываются неэффективными перед такими атаками, как манипуляция параметрами, межсайтовый скриптинг и инъекция SQL-кода.