5.3. ***Обработка запроса внешними пользователями и высылка образца ответа.*** После обработки информации запроса внешний пользователь заполняет обязательные поля образца ответа и посылает ответ в почтовый ящик ответов (Answer Box).

5.4. ***Получение и проверка ответов.*** Проверяется соответствие очередного ответа с данными образцов и тестов запроса. Результаты проверки ответа посылаются внутреннему пользователю. В случае неудовлетворения тот же вопрос помещается в User Box пользователя и посылается почтовое сообщение о результате проверки ответа.

5.5. ***Добавление ответа в БД.*** После положительного тестирования и проверки документы через шлюзы ISS автоматически заносятся в БД в виде добавления.

6. СИНТЕЗ РЕЗУЛЬТИРУЮЩЕЙ СИСТЕМЫ ЗАЩИТЫ

Результирующая система состоит из системы защиты и ActiveX элемента управления защитой и тестами. Результат генерации системы защиты и тестов, включающий:

- создание структур шаблонов запроса (Request Templet) и ответов (Answer Templet) на основе выбранных схем базовых структур шаблонов;
- создание и настройку схем алгоритмов в виде хранимых на сервере процедур;
- создание и настройку схем тестов в виде хранимых на сервере процедур.

ActiveX элементом управления защитой и тестами обеспечивается графический интерфейс пользователя для динамического управления доступом и для запуска тестов. Позволяет администратору проводить сеанс редактирования полномочий пользователей системы.

ЛИТЕРАТУРА

[1] *Kiuchi T., Sakurai T.* University Medical Information Network – Past , Present, and Future, 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

[2] *Hode T., Wattling D. and Alvarez R.* The Canadian Health Information Framework, 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

[3] *Norifusa M.* Internet security: difficulties and solutions. International Journal of Medical Informatics, Vol. 49, March, 1998, p. 69-74.

[4] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe* Convention 108, January 1981, –ISBN (1982) 92–871–0022–5.

[5] European Commission Directive 95/46/EC, On the Protection of Individuáls with Regard to: the Processing of Personal Data and on the Free Movement of such Data, OJ L281/31–50, 24 October 1995.

[6] *Ingham B. et al.* Supporting Highly Manageably Web Services" Dept. of Computer Sciences, University of Newcastle upon Tune.

[7] *Shoukourian S.K., Shukurian A.K., Avagyan A.A., Vasilyan A.M.* Designing a virtual operating room for prediction of operative interventions under some pathologies of middle ear. A case of the database, 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

[8] *Shoukourian S.K., Vasilyan A.M., Shukurian A.K.* Draft on a virtual operating room for prediction of hearing function changes and operative interventions under some pathologies of middle ear, Proceedings of the International Conference on Critical Technologies, Yerevan, 1995.

[9] *Авакян А.А., Василян А.М.* Методика проектирования и тестирования систем разграничения доступа для некоторых распределенных приложений, основанных на базах данных. – Настоящий сборник.

[10] *Василян А.М.* Система разграничения доступа для пользователей некоторых распределенных приложений, в рамках локальной сети. – Настоящий сборник.

[11] *Gundavaram Sh.* CGI–Programming on the World Wide Web. // O' Relly 1997.

МЕТОДИКА ПРОЕКТИРОВАНИЯ И ТЕСТИРОВАНИЯ СИСТЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ НЕКОТОРЫХ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ, ОСНОВАННЫХ НА БАЗАХ ДАННЫХ

Авакян А., Василян А.

Ереванский государственный университет

Рассмотрена методика проектирования и тестирования систем разграничения доступа (СРД) для распределенных приложений. Методика основана на комбинации в рамках единой оболочки механизмов и инструментов разграничения доступа в СУБД и ОС, современного инструментария прикладного программирования и формальной верификации, которые обычно используются раздельно. Предложена модель и механизмы их отражения в СУБД с учетом удаленных пользователей, подключенных через глобальные компьютерные сети.

Ավագյան Ա., Վասիլյան Ա. **Տվյալների բազաների վրա հիմնված տեղաբաշխված կիրառությունների համակարգերից օգտվելու արտոնությունների սահմանափակումների ևախագծման և տեստավորման մեթոդիկան:** Դիտարկված է բաշխված կիրառությունների համակարգերից օգտվելու արտոնությունների սահմանափակման նախագծման և տեստավորման մեթոդիկան: Այն հիմնված է Օպերացիոն համակարգերի և Տվյալների Բազաների Կնկավարման Համակարգերի (ՏԲՂՀ) արտոնությունների սահմանափակումի, ինչպես նաև ժամանակակից ծրագրային միջավայրերի և ֆորմալ վերիֆիկացիայի միջոցով կոմբինացված մեկ միասնական մեխանիզմի և գործիքային բաղադրի ստեղծման վրա: Դրանք սովորաբար օգտագործվում են իրարից անջատ: Առաջարկված է համապատասխան մոդելը և ՏԲՂՀ-ի համար նրա արտապատկերման մեխանիզմները, հաշվի են առնված նաև այն օգտագործողները, որոնք միմում են գլոբալ համակարգչային ցանցի միջոցով:

Avagyan A., Vasilyan A. **Methology of designing and testing of systems for access differentiation system in distributed applications built on databases.** The paper suggests a detailed outline of a design and testing methodology for access differentiation systems (ADS) in distributed applications which use databases. The approach combines different protection mechanisms and tools in DBMS, OS and state of the art for application programming tools (object-oriented environments, system description and verification tools, SQL tools), that are usually used separately, in order to provide a practical integrated approach to the development of protection systems for specific applications with a particular emphasis on automation of design, implementation and verification. The appropriate model as well as tools for its mapping to a DMBS are suggested. Remote users connected via global computer networks are considered too.

1. Унифицированная методика проектирования и тестирования СРД.

В работах [1, 2] описана формализованная методика проектирования "сверху–вниз" распределенных баз данных, рассматриваемых как медиум (посредник) между виртуальной и реальной средами пользователя в некоторых медицинских приложениях.

Кратко описан ряд шагов начальных этапов проектирования и, в частности, шаг выбора СУБД по требованиям обработки в режиме реального времени, параллельной обработки запросов, аутентификации пользователей, описания прав отдельных групп пользователей на ресурсы БД, целостности и т.д.

Ввиду ограничений на объем статьи этот шаг представлен упрощенно и завершен выбором SQL сервера в качестве СУБД, поддерживающей указанные выше требования и соответственно SQL как языка взаимодействия с СУБД.

В то же время SQL сервер не обеспечивает существующие на сегодняшний день некоторые важные требования к аутентификации и описанию прав пользователей в рамках системы.

В настоящей статье рассмотрено расширение общей методики проектирования и тестирования систем разграничения доступа для приложений, основанных на базах данных. Предлагаемая методика приведена на *рис. 1.* Она применяется после проведения первых шагов формализованного проектирования, в ходе которых спроектирована объектная модель системы [2] и дано первичное размещение функций системы между клиентом и сервером. Методика позволяет применять унифицированную технику проектирования СРД для различных классов объектов системы. Основу методики составляют средства комбинации в рамках единой оболочки механизмов и инструментов разграничения доступа в СУБД и ОС, современного инструментария прикладного программирования и формальной верификации, которые обычно используются раздельно. На основе предыдущих шагов проектирования формулируется спецификация СРД, включающая в себя табулярное описание объектов защиты и ограничения, поставленные на эти объекты.

Первый этап проектирования системы защиты заключается в определении информационных структур СРД, на основе которых осуществляется защита и алгоритмов защиты, определенных на этих структурах. Одновременно с проектированием защиты на основе спецификации происходит проектирование структур и алгоритмов для тестов СРД, которые позволяют выявить и устранить несоответствия с поставленными ограничениями на каждом этапе проектирования СРД.

Результатом проектирования является инструментальная среда, поддерживающая выбранную архитектуру, модели составных и распределенных составных объектов, интерфейс с базой данных. В рамках системы обеспечиваются средства Online и Offline тестирования системы.

Аналогичная техника применяется для проектирования и тестирования СРД для пользователей, подключенных через глобальные компьютерные сети.

2. Ключевые объекты и подсистемы защиты.

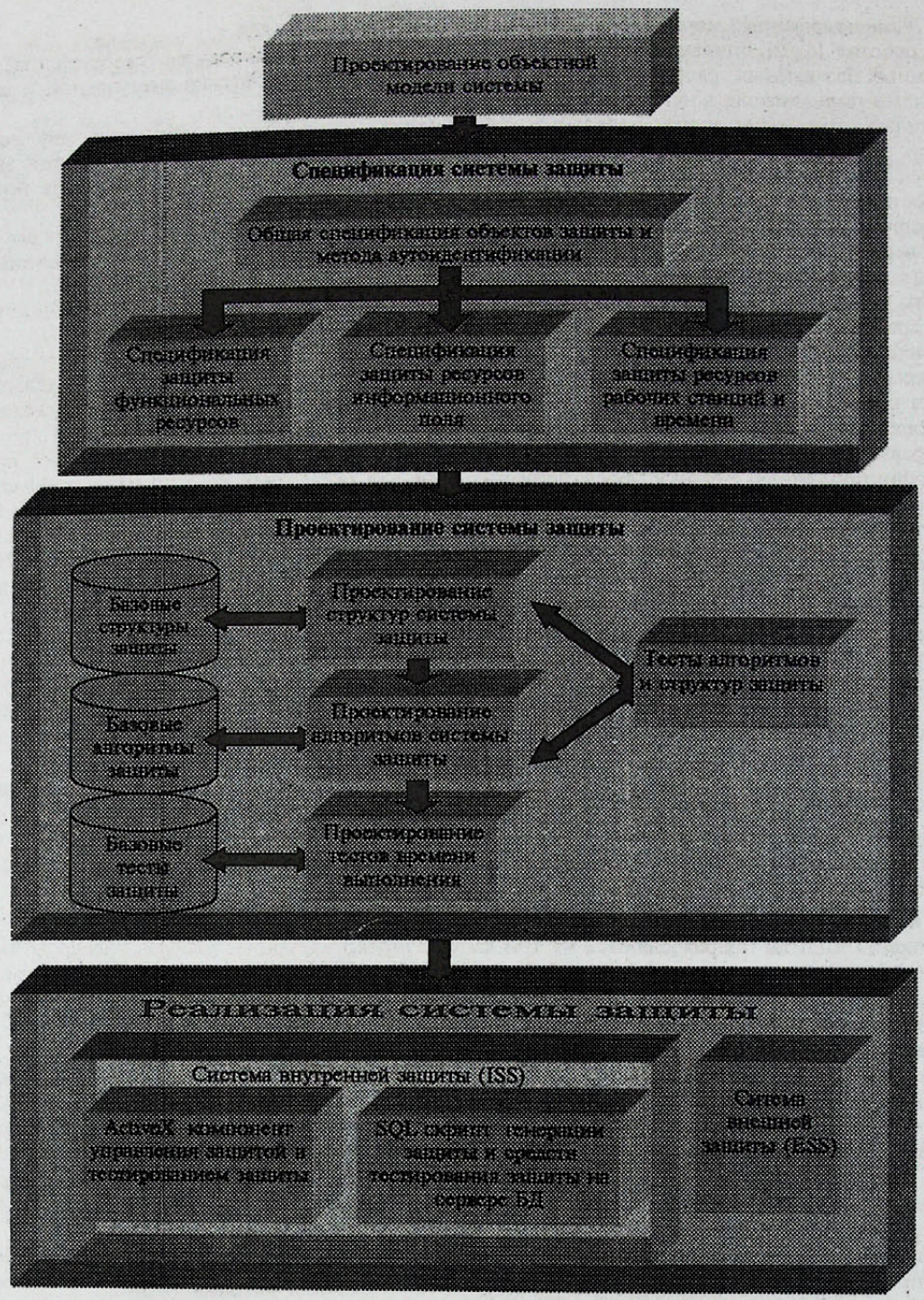
Объекты защиты подразделяются на три класса: функциональные ресурсы, ресурсы информационного поля, ресурсы времени и рабочих станций. Спецификация системы защиты определяется заданием: 1) функций защиты в целом; 2) функций, общих для всех классов; 3) функций защиты отдельных объектов; 4) ограничений на используемые функциии.

При таком рассмотрении синтез системы можно проводить независимо от отдельных классов и рассматривать только взаимосвязь данного класса и функций, общих для всей системы.

Приведем составные части общей спецификации объектов защиты: 1) список используемых классов объектов защиты; 2) способ аутентификации пользователей (например, через сервер БД или через сервис аутентификации сетевой операционной системы); 3) дополнительная поддержка журнала действий пользователей; 4) ограничение на общее количество пользователей системы; 5) ограничение на общий объем дисковой памяти, запрашиваемой системой защиты; 6) ограничение на время ответа на запрос о проверке полномочий системой защиты.

Проектирование и синтез защиты для класса ресурсов времени и рабочих станций сводится к созданию интерфейсов к соответствующим службам ОС и, следовательно, к использованию стандартных или достаточно известных процедур [3], и далее здесь не рассматриваются.

Одинаковая среда функционирования подсистем защиты для классов функциональных ресурсов и ресурсов информационного поля сервер БД определяет похожие механизмы их проектирования и тестирования. Однако если защита функциональных ресурсов задается многоуровневой иерархией относительно статических ресурсов, то ресурсы информационного поля описываются трехуровневой иерархией, но обладают большим динамизмом управления СРД. Построение внутренней системы защиты (Internal Security System – ISS) для распределенных приложений, функционирующих в рамках локальных сетей, рассмотрено в настоящем сборнике [4].



Прямое добавление внешних пользователей во внутреннюю систему защиты, путем увеличения параметров защиты, не представляется целесообразным ввиду следующего принципиального ограничения: внешние подключения происходят через существующие глобальные компьютерные сети и, в частности, через наиболее распространенную сеть Internet. Принципиальные трудности построения эффективных методов защиты этих сетей приводят к значительному ухудшению характеристик ISS и многочисленным возможностям ее взлома пользователями Internet [5].

Поэтому нами выбран ограниченный способ обращения внешних пользователей к ресурсам системы, основанный на следующих положениях: 1) внешний пользователь имеет право доступа только к информации, которая выставлена в виде формы запроса для обращения извне; 2) запрос со стороны внешнего пользователя может поступить только в ответ на извещение о предоставле-

нии такой информации; 3) предоставленная информация изолирована от БД локальных пользователей; 4) ответы внешних пользователей регистрируются в форме ответа на запрос и заносятся в БД только в виде добавлений, после предварительного тестирования и проверки.

Этот способ реализован в виде отдельной подсистемы External Security System (ESS). Детальное описание ESS рассмотрено в настоящем сборнике[6].

3. Результат синтеза целевой системы защиты.

Ввиду ограничений, рассмотренных в [1], в качестве оболочки реализации целесообразно выбрать открытую среду, поддерживающую архитектуру клиент–сервер, активное управление защитой, модели составных и распределенных составных объектов, открытый интерфейс с базой данных. Перечисленным требованиям удовлетворяет среда программирования MS Visual Basic [7, 8]. Поэтому результат синтеза целевой системы разграничения доступа выражается в виде двух частей: системы управления защитой и тестами защиты в виде ActiveX компонента, реализованного в среде MS Visual Basic, и системы генерации защиты на сервере БД в виде SQL скрипта. В результате запуска сгенерированного SQL скрипта создается специализированная БД защиты и API запомненных на сервере процедур.

Синтез вышеуказанных частей происходит на базе протестированных структур и алгоритмов путем компоновки модулей из соответствующих библиотек.

Средства Online и Offline функционального тестирования системы защиты также представлены в виде SQL скриптов.

4. Математическая модель.

Построенная модель защиты естественным образом отображается на соответствующую алгебру цепочек дескрипторов. Задачи построения полной системы эквивалентных преобразований для цепочек дескрипторов, их оптимизации по критериям объема и времени выполнения будут рассмотрены в наших последующих публикациях.

Математическое обоснование для тестов проверки системы защиты можно проводить в рамках модели, аналогичной рассмотренной в работе [9]. Пример построения тестов типа online, вытекающий из результатов построенных для этой модели, также будет рассмотрен в нашей последующей публикации.

5. Заключение.

Предложенная методика может быть использована как основа для построения интегрированной инструментальной среды для проектирования и тестирования систем распределения доступа. Конкретные примеры ее использования рассмотрены в настоящем сборнике [4, 6].

Существующие CASE системы разработки распределенных приложений могут быть дополнены средствами проектирования и тестирования защиты, позволяющими одновременно с проектированием приложения выполнять формализованное проектирование и тестирование СРД для данного приложения. Совмещение средств проектирования и тестирования СРД позволит уменьшить стоимость создаваемых приложений.

ЛИТЕРАТУРА

[1] *Shoukourian S.K., Vasilyan A.M., Shukurian A.K.* Draft on a virtual operating room for prediction of hearing function changes and operative interventions under some pathologies of middle ear, Proceedings of the International Conference on Critical Technologies, Yerevan, 1995.

[2] *Shoukourian S.K., Shukurian A.K., Avagyan A.A., Vasilyan A.M.* Designing a virtual operating room for prediction of operative interventions under some pathologies of middle ear. A case of the database, accepted for presentation and publication in Proceedings of 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August, 1998.

[3] *Baker B.* Patient data and security: an overview. – International Journal of Medical Informatics, v. 49, March, 1998, p. 19-30.

[4] *Василян А.М.* Система разграничения доступа для пользователей некоторых распределенных приложений, функционирующих в рамках локальной сети. – См. настоящий сборник.

[5] *Norifusa M.* Internet security: difficulties and solutions. – International Journal of Medical Informatics, v. 49, March, 1998, p. 69-74.

[6] *Аваkян А.А.* Система разграничения доступа для пользователей некоторых распределенных приложений, подключенных через Internet. – См. настоящий сборник.

[7] Visual Basic® 5.0 Programmer's Guide. Microsoft® Press 1997.

[8] *William R.* Vaughn, Hitchhiker's Guide to Visual Basic®.& SQL Server™. Microsoft® Press 1997.

[9] *Shoukourian S.K.* A Unified designing methodology for offline and online testing, IEEE design and test of computers, April-June, 1998, p.72-78.

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА В РАМКАХ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ

Василян А.

Ереванский государственный университет

Приведен пример применения методики проектирования и тестирования систем разграничения доступа (СРД) для распределенных приложений, использующих базы данных. Пример приведен для двухуровневой архитектуры клиент–сервер, функционирующей в рамках локальной сети, где сервер представлен СУБД MS SQL Server 6.5. Описана реализация механизма распределения доступа и рассмотрены примеры ее использования клиентом, реализованным в среде MS Visual Basic 5.0.

***Վասիլյան Ա.*, Հասանելիության տարբերակման համակարգ լոկալ համակարգչային ցանցում գործող, տեղաբաշխված կիրառական ծրագրերի համար.** Հոդվածում դիտարկված է տվյալների հենքերի վրա հիմնված, տեղաբաշխված կիրառական ծրագրերի համար հասանելիության տարբերակման համակարգի