заменить тип полей первичного ключа новым разработанным типом.

Как можно увидеть из всего вышеизложенного, при преобразовании обычной реляционной базы данных в темпоральную с использованием описанных средств все существующие запросы будут работать по-прежнему.

Таким образом, можно сказать, что в настоящий момент темпоральные базы являются перспективным направлением исследований. И наиболее оптимальным, по нашему мнению, является создание специальных расширений управления темпоральными данными для существующих СУБД. В данной работе эти идеи были реализованы применительно к PostgreSQL.

**Список использованных источников**

1. Snodgrass R.T. Developing time-oriented database application in SQL. – San Francisco: Morgan Kaufmann Publishers, 2000. –528p.

2. PostgreSQL 8.2.0 Documentation// PostgreSQL. - Режим доступа: http://www.postgresql.org/files/ documentation/pdf/8.2/postgresql-8.2-A4.pdf

3. Фути К., Судзуки Н. Языки программирования и схемотехника СБИС. – М.: Мир, 1988. – 224 с.

**Шыхалиев Р.Г.**

## ОБ ОДНОМ ПОДХОДЕ К ЭКРАНИРОВАНИЮ ВЗАИМОУВЯЗАННОГО КОРПОРАТИВНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК АЗЕРБАЙДЖАНА

*Институт информационных технологий Национальной академии наук Азербайджана, г.Баку*

**Введение.** Сегодня с уверенностью можно сказать, что у Национальной Академии Наук Азербайджана (НАНА) сформировалось взаимоувязанное корпоративное информационное пространство (ВУКИП), целью которого является автоматизация обработки информации и управления в масштабе НАНА. ВУКИП НАНА, – это интегрированное информационное пространство распределенных и локальных информационных ресурсов институтов и организаций НАНА, сервисов и комплексов программно-технических средств, обеспечивающее использование этих ресурсов и сервисов и полнофункциональное управление ими.

К настоящему времени в портале, институтах и организациях НАНА уже созданы и накоплены большие объемы информации в электронной форме. К ним относятся научные публикации, базы данных в различных областях науки, алгоритмы и программы, структурные и кадровые сведения и т.д. НАНА в целом располагает значительными техническими и информационными ресурсами и имеет корпоративную сетевую инфраструктуру. Она объединяет все научные организации НАНА (институты, Нахчыванское отделение НАНА, Гянджинский научный центр и т.д.) в масштабе страны. Задача объединения всех этих ресурсов в ВУКИП НАНА – эффективное использование информации, в частности, повышение качества научных работ, подготовки специалистов посредством внедрения в научную деятельность новых информационных технологий.

В ВУКИП НАНА в основном происходит интеграция информации двух основных типов: научно-методическая информация и организационно-управленческие и административно-хозяйственные ресурсы.

В общем случае информационные ресурсы НАНА представляются совокупностью гетерогенных информационных источников и сервисов. Поэтому управление доступом к информации из разных источников должно осуществляться совершенно по-разному. Таким образом, необходимо формирование ВУКИП НАНА, где информационные ресурсы и сервисы представляются пользователям непротиворечивым и интегрированным образом через единый интерфейс (через портал НАНА) с учетом прав пользователей. При этом инфраструктура ВУКИП НАНА должна обеспечивать расширение круга пользователей ресурса за счет повышения его доступности, удобства в использовании, поиске информации и предоставлении семантического содержания ресурса.

Формирование и сопровождение ВУКИП НАНА требует решения целого ряда организационных вопросов. Наиболее важным из них является обеспечение информационной безопасности, которую необходимо решать. Для обеспечения информационной безопасности ВУКИП НАНА в целом, т.е. организации противодействия любому несанкционированному вторжению в процесс его функционирования, а также попыткам модификации, хищения, вывода из строя или разрушения его компонентов, целесообразно использовать технологии экранирования.

Экранирование – функция межсетевого экрана (МЭ), позволяющая поддерживать безопасность объектов внутреннего корпоративного информационного пространства (КИП), игнорируя несанкционированные запросы из внешнего информационного пространства [1]. МЭ устанавливается на границе защищаемой сетевой инфраструктуры защищаемого КИП и фильтрует все входящие и исходящие данные, пропуская только авторизованные пакеты. МЭ является набором компонентов, настроенных таким образом, чтобы реализовать определенную политику контроля доступа в защищаемый КИП из нее [4, 5, 6].

В общем случае системы экранирования могут обеспечить следующие функции:

- идентификацию и аутентификацию пользователей;
- проверку подлинности передаваемых данных;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрацию и преобразование потока сообщений;
- трансляцию внутренних сетевых адресов для исходящих пакетов;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов;
- кэширование данных, запрашиваемых из внешней сети.

**Постановка задачи.** Специфика НАНА как объекта информатизации заключается в том, что значительную часть корпоративного информационно-

го трафика составляет научная информация, поступающая наряду с управленческими данными. Большая часть научной информации является, как правило, слабоструктурированной или неструктурированной. Кроме того, разделить информацию на управленческую и научную трудно. На рис.1 показаны структура ВУКИП НАНА и информационный трафик.


Рис. 1. Структура ВУКИП НАНА

Основой для сетевой составляющей ВУКИП НАНА является созданная корпоративная сетевая инфраструктура НАНА, которая состоит из двух основных узлов: I Азербайджанского узла НАНА и II Азербайджанского интернет-узла сети НАНА, где сосредоточены все институты, организации НАНА и локальная корпоративная сеть (ЛКС) Президиума НАНА.

ВУКИП НАНА составляет всевозможные информационные ресурсы: вычислительные системы, Web-сайты, цифровые библиотеки, электронные журналы, распределенные и локальные базы, как уже существующие в организациях и институтах НАНА, так и планируемые. Главная задача, решаемая инфраструктурой ВУКИП НАНА, – обеспечение интеграции распределенных ресурсов для их безопасного представления через портал НАНА. При этих условиях требуется создать такую систему экранирования, которая позволит обеспечить высокий уровень безопасности ВУКИП НАНА.

Задачу экранирования ВУКИП НАНА можно сформулировать как интеграцию управления сетевого и прикладного уровней на базе общей политики безопасности, состоящей из совокупности формализованных правил доступа к сегментам корпоративной сети НАНА, хостам, портам, сервисам, приложениям, правил идентификации и аутентификации субъектов доступа ВУКИП НАНА.

**Разработка системы экранирования ВУКИП НАНА.** Известно, что

современные МЭ обеспечивают многоуровневую безопасность. В основном все МЭ используют информацию разных уровней эталонной модели OSI/ISO. В общем случае, чем выше уровень эталонной модели OSI/ISO, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты [1-3].

Основную роль в экранировании ВУКИП НАНА, да и ВУКИП любой организации, играют сетевой и прикладной уровни эталонной модели ISO/OSI [1]. При этом функции защиты, выполняемые на различных уровнях эталонной модели ISO/OSI, существенно отличаются друг от друга. Например, на прикладном уровне в основном необходимы функции: идентификация пользователей; аутентификация пользователей; управление доступом к информационным ресурсам; контроль подлинности и целостности некоторых ресурсов; мониторинг и аудит.

Для противодействия существующим угрозам на сетевом уровне эталонной модели ISO/OSI требуется организовать защиту от атак как из внешней, так и из внутренней сети НАНА. При этом для защиты от атак из внешней сети необходимы следующие функции безопасности: создание периметра защиты ВУКИП НАНА; организация защищенного обмена информацией с внешними источниками. А для защиты от атак изнутри требуется решать следующие задачи: устранение/уменьшение угроз, связанных с неправомочными действиями внутренних пользователей; выявление уязвимости и слабости программно-технических средств; сегментирование сетевой инфраструктуры ВУКИП НАНА по уровням конфиденциальности, территориальному и функциональному признакам.

Для реализации указанных выше функций наряду с МЭ может быть использована технология VPN (Virtual Private Network – виртуальная частная сеть).

Идея, лежащая в основе концепции VPN, заключается в использовании преимуществ открытой коммуникационной инфраструктуры, например, разделенной инфраструктуры сети Интернет, которая является недорогой и готова к работе в глобальном масштабе, так и в состоянии противостоять всем современным угрозам информационной безопасности [2, 3].

Для построения комплексной системы экранирования ВУКИП НАНА удобно представить ее в виде совокупности подсистем, каждая из которых ориентирована на отдельный уровень эталонной модели ISO/OSI. В качестве базового варианта предлагается следующий состав функциональных подсистем системы экранирования ВУКИП НАНА:

- управление безопасностью;
- идентификация и аутентификация;
- управление доступом к информации;
- контроль целостности информации;
- регистрация и аудит.

Данные подсистемы охватывают как прикладной, так и сетевой уровни эталонной модели ISO/OSI. Архитектурное решение экранирования ВУКИП НАНА, показанное на рис. 2, реализует эти подсистемы и интегрирует их в

единое целое.

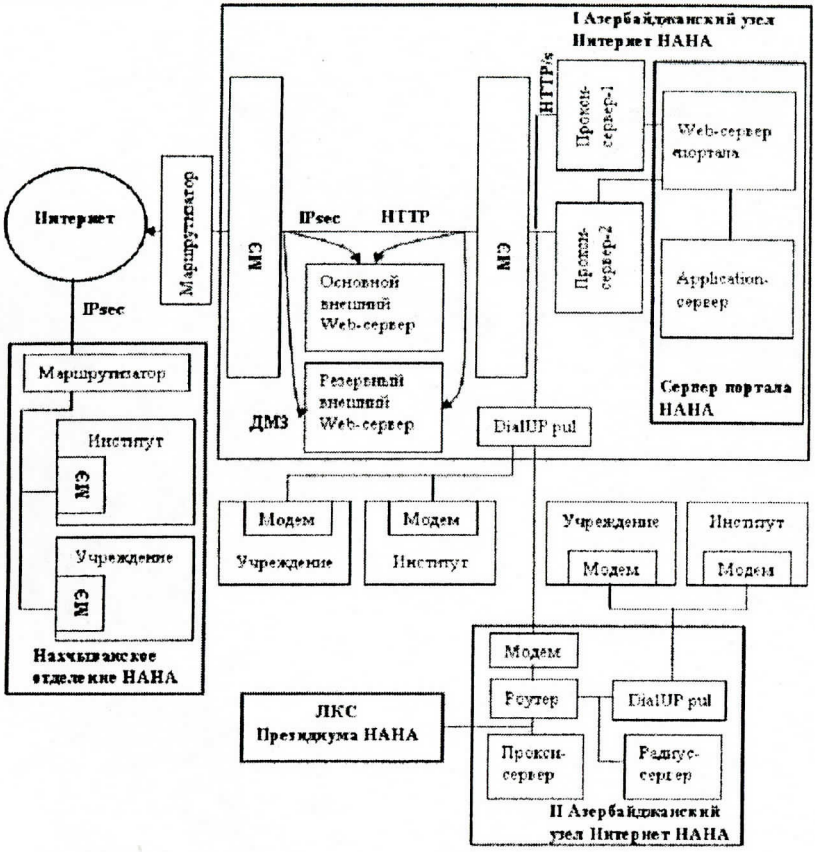


Рис. 2. Архитектура экранирования ВУКИП НАНА

В представленной на рис. 2 архитектуре системы экранирования ВУКИП НАНА можно видеть комплекс средств защиты периметра. Следует подчеркнуть, что система экранирования должна контролировать доступ аутентифицированных пользователей и запрещать доступ посторонних в ВУКИП НАНА. Причем система управления доступом построена на базе двух прокси-серверов, первый из которых на основе ролей и матрицы доступа разграничивает доступ зарегистрированных пользователей портала НАНА к его ресурсам, а второй (выходной) – доступ таких же пользователей в Интернет. При этом для посетителей портала НАНА (неавторизованных субъектов) доступен только Web-сервер, расположенный в демилитаризованной зоне.

Защита соединения с удаленным сегментом корпоративной сетевой инфраструктуры НАНА (например, с Нахчыванским отделением НАНА) осуществляется с использованием VPN-технологии, в которой применяется протокол IPSec.

Таким образом, экранирование ВУКИП НАНА осуществляется на основе сформированной общей политики безопасности в виде совокупности правил доступа к сегментам корпоративной сетевой инфраструктуры ВУКИП НАНА, хостам, портам, сервисам и правил прокси-доступа к сервисам и информационным ресурсам.

**Заключение.** Основное преимущество реализованного решения экранирования ВУКИП НАНА состоит в гибкой адаптации к имеющейся в НАНА иерархической дисциплине, основанной на имеющемся структурном и кадровом подчинении. Перспективой развития данной системы экранирования является возможность интеграции ВУКИП НАНА с КИП других научных центров страны и зарубежных. Архитектура экранирования может быть принята как обобщенная и применена для экранирования ВУКИП широкого круга организаций и является многоуровневой, что может обеспечить защиту ВУКИП от множества различных типов угроз. Типовые протоколы сетевого уровня (IP/IPSec) и прикладного уровня (HTTP/HTTPS) улучшают интегрируемость средств защиты и реализуемость функций безопасности.

## Список использованных источников

1. Алгулиев Р.М., Шыхалиев Р.Г. Методы и технологические аспекты экранирования взаимоувязанных корпоративных информационных пространств. Баку, «Элм», 2003. – 106 с.

2. Оглтри Т. Firewalls. Практическое применение межсетевых экранов: Пер. с англ. – М.: ДМК «Пресс», 2001. – 400 с.

3. Польман Н., Кразерс Т. Архитектура брандмауэров для сетей предприятия.: Пер. с англ. – М.: ИД «Вильямс», 2003. – 432 с.

4. Firewall Policy Guide – NCSA, 1997.

5. Ranum M. Thinking About Firewalls. In SANS-II Conference, April 1993.

6. NIST Special Publication 800-41. Guidelines on Firewalls and Firewall Policy. *MIS Training Institute, January 2002.