The International Scientific Conference "Problems of Cybernetics and Informatics", October 24-26, 2006, Baku, Azerbaijan. Section #3 "Information Technology"
www.pci2006.science.az/3/09.pdf

Р.Г. Шыхалиев

ПРОБЛЕМЫ ЭКРАНИРОВАНИЯ ВЗАИМОУВЯЗАННЫХ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ ПРОСТРАНСТВ

Институт информационных технологий НАНА, Баку, Азербайджан
ramiz@science.az

1. Введение. Известно, что внедрение информационных технологий в различных странах длительный период проводилось в рамках отдельных предприятий независимо друг от друга и они функционировали разобщённо, в результате чего сформировалось множество независимых корпоративных информационных пространств (КИП). При этом эффективность совокупности КИП различных предприятий в масштабах государств оставалась низкой, так как корпоративная разобщенность затрудняла обмен информацией между различными КИП и доступ к ним. КИП – это совокупность информационных ресурсов и систем, телекоммуникационных систем и сетей, функционирующих на основе единых корпоративных принципов и по общим правилам, обеспечивающим оптимальное информационное взаимодействие субъектов, а также наиболее полное удовлетворение их информационных потребностей. Однако со временем мир становится все более открытым и взаимоувязанным, в результате открытыми и взаимоувязанными становится и КИП как в рамках отдельных стран, так и за их пределами.

Необходимым условием создания информационного общества в любой стране, в том числе и в Азербайджане является формирование единого государственного корпоративного информационного пространства (ЕГКИП) и интеграции его в глобальное мировое информационное пространство. ЕГКИП Азербайджанской Республики можно рассматривать как комплекс взаимосвязанных и взаимодействующих отраслевых, корпоративных и проблемно-ориентированных информационных сред, в том числе.

- органов государственной власти и местного самоуправления;
- социальной, индивидуально-бытовой и правовой сферы (наука, высшая школа, образование, культура, средства массовой информации, здравоохранение, социальное обеспечение, занятость, жилищно-коммунальные службы, юридические консультации и т.д.);
- сфер производства и производственной инфраструктуры (сельское хозяйство, промышленность, энергетика, связь, транспорт, строительство и т.д.);
- сфер рыночной инфраструктуры (банки, фонды и т.д.).

При интеграции различных КИП необходимо обеспечение взаимоувязанности этих информационных пространств. Взаимоувязанность обеспечивает структурную и функциональную целостность единого корпоративного информационного пространства (ЕКИП), полученного в результате интеграции различных КИП.

В связи с необходимостью создания ЕГКИП очень существенным является формирование взаимоувязаннных корпоративных информационных пространств (ВУКИП). ВУКИП – это территориально-распределенная информационная структура, являющаяся совокупностью взаимосвязанных и взаимодействующих КИП на базе единых корпоративных стандартов, которая обеспечивает доступ к информации пользователей в рамках их полномочий, в какой бы КИП они ни оказались. Причем, базовым системообразующим фактором ВУКИП является формирование ЕКИП. При этом границы КИП, входящие во ВУКИП могут быть опредлены не только установленным оборудованием, а также политикой безопасности, которой придерживаются участники информационного обмена ВУКИП. В таких случаях на различных узлах и сегментах сложной сетевой среды ВУКИП могут отличаться требования к информационной безопасности.

Определяющим фактором при формировании ВУКИП, на которое необходимо обратить внимание, является обеспечение информационной безопасности. Для решения

этой задачи, необходимо в рамках ВУКИП создать такую защищенную среду, которая обеспечит защиту корпоративного сетевого пространства, информационных ресурсов и предоставление пользователям возможности безопасной работы с информационными ресурсами в каком бы КИП они ни находились. Средством, позволяющим создать такую среду, является межсетевой экран (МСЭ). Обычно МСЭ располагается между двумя КИП имеющими различные политики безопасности и контролирует все информационные потоки, проходящие через него. Основной задачей МСЭ является пресечение попыток несанкционированного доступа в защищаемое КИП.

2. Основные проблемы экранирование ВУКИП. Экранирование – это функция МСЭ, позволяющая поддерживать безопасность объектов внутреннего информационного пространства, игнорируя несанкционированные запросы из внешнего информационного пространства. Экранирование ВУКИП достигается путем установления МСЭ в местах подключения данного КИП к открытым информационным пространствам (например, Интернет) и другим КИП. Также экранирование ВУКИП предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования ВУКИП, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту всех компонентов ВУКИП – аппаратных средств, программного обеспечения, данных и персонала.

Несмотря на то, что МСЭ широко применяется для обеспечения информационной безопасности КИП, необходимо подчеркнуть, что многие вопросы, связанные с организацией и проектированием системы для экранирования таких распределенных информационных пространств как ВУКИП, пока еще остаются нерешенными,. так как для ВУКИП требуется стратегия экранирования, существенно отличная от используемой в отдельно взятых КИП. При этом ВУКИП вводят новые требования для технологии экранирования, которые не могут быть выполнены с использованием существующих моделей. Исходя из этого, при экранировании ВУКИП необходимо решить ряд основных задач, к которым относятся:

- определение, предписание и осуществление контроля доступа во ВУКИП;
- определение точек контроля и формирование защитного контура на границах ВУКИП;
- проверка безопасности механизмов фильтрации, т.е. проверика функциональных возможностей МСЭ;
- разработка архитектурных основ экранировани ВУКИП;
- оценка эффективности экранирования ВУКИП;
- экранирование мультимедийного трафика во ВУКИП;
- анализ корректности политики безопасности, осуществляемая МСЭ;
- формализация процесса экранирования;
- и т.д.

3. Некоторые методы решения проблем экранирования ВУКИП. Во ВУКИП число пользователей и компьютеров может измеряться тысячами, число серверов превышать несколько сотен, число записей в базе данных несколько миллионов, что усложняет определение, предписание и осуществление контроля доступа и требуется иной подход в отношении доступа, чем в традиционных информационных системах. Это связано с тем, что во ВУКИП существует множество различных категорий пользователей, которые отличаются правами доступа, и множество различных категорий объектов с различными уровнями доступа, причем категории могут включать и подкатегории. В этих условиях классифицировать эти группы пользователей только на основании их IP-адреса, как это традиционно делали МСЭ, практически невозможно, учитывая применение таких методов управления IP-адресами как DHCP, NAT и туннелирование. Традиционно, контроль доступа определялся отношением доступа (или "матрицей доступа"), в которой подробно вводится информация о том, какие пользователи, к каким ресурсам могут получить доступ. Однако в больших распределенных системах, таких как ВУКИП это не

приемлемо, так как матрицы доступа занимают большие системные ресурсы. Для определения и предписания доступа необходимо раскрыть пользовательскую иерархию и иерархию ресурса ВУКИП в отношении доступа и объединения их в единую архитектуру [1]. Объединенная иерархия может упростить и компактно описать контроль доступа во ВУКИП.

Для обеспечения огромного разнообразия потребностей к безопасности различной информации и ресурсов ВУКИП предлагается каскадный метод экранирования, а именно каскадное размещение МСЭ [2]. Каскадное размещение МСЭ может повысить безопасность узлов ВУКИП с критической информацией из-за того, что укорачивается опасный путь от нападавшего до критического узла, и в итоге повышается общая безопасность ВУКИП. Каскадное размещение МСЭ позволяет расширить периметр защиты и в итоге полностью охватить всевозможные сценарии нападения, а также обеспечить различные уровни безопасности в различных частях ВУКИП. Также надо отметить, что при каскадном экранировании МСЭ независимы друг от друга, и компрометация одного МСЭ не приводит к компрометации всей системы.

В существующих МСЭ используются различные механизмы безопасности, такие как фильтрация IP-пакетов, трансляция адресов, посредничество, инспекция состояния и т.д. В совокупности эти механизмы делают МСЭ комплексным. МСЭ, в которых используется механизм фильтрации IP-пакетов, являются самыми широко распространенными. Большинство МСЭ с фильтрацией IP-пакетов могут пропускать или блокировать IP-пакеты на основе информации, позволяющей ассоциировать данный пакет с конкретным отправителем и получателем. При реализации МСЭ с фильтрацией IP-пакетов становится необходимым проверка безопасности механизма фильтрации, т.е. проверка его функциональных возможностей. Для этого необходимо проверить настройки правил фильтрации, корректность политики безопасности, осуществляемых МСЭ, а также анализ их работы. Модель МСЭ с фильтрацией IP-пакетов, для формализованного описания которого используются Раскрашенные Сети Петри, позволяет более адекватно и удобно выражать особенности их функционирования [3].

Как было сказано выше, экранирование ВУКИП достигается путем установления МСЭ в местах подключения данного КИП к открытым информационным пространствам (например, Интернет) и другим КИП. При этом построенная распределенная система МСЭ позволяет защищать ВУКИП как от внешних, так и внутренних сетевых атак. Однако при обработке трафика во ВУКИП МСЭ, объединенными в логическую сеть, могут возникнуть очереди, в результате чего может нарушиться доступность той или иной услуги или ресурса. Поэтому необходима оценка эффективности распределенной системы экранирования ВУКИП при осуществлении МСЭ типовых функций, исходя из требований доступности, т.е. возможности пользователей за приемлемое время получать доступ к требуемой услуге или ресурсу в рамках своих полномочий. Для оценки используется модель теории массового обслуживания, представляющая распределенную систему экранирования ВУКИП в виде разомкнутой стохастической сети, которая позволяет определить среднее время обслуживания запросов пользователей на доступ к услугам или ресурсам [4].

Известно, что мультимедийные данные являются составляющей частью КИП, и необходимость передачи мультимедийного трафика во ВУКИП увеличивает потребность в использовании мультикаст технологии передачи пакетов. Эта технология позволяет создавать широкомасштабную среду для эффективного распределения информации большому количеству пользователей. При мультикаст передаче каждый пакет одновременно отравляется всем необходимым адресатам без дублирования. Однако имеется несколько причин, по которым сегодня мультикаст технология не так широко применяется во ВУКИП. Основной из этих причин является проблема обеспечения информационной безопасности. В частности, передача мультикаст трафика весьма интенсивно нагружает каналы связи, особенно в сетях (в сетях пакетной коммутации IP и IPX на базе Ethernet, Fast Ethernet и Token Ring), не обеспечивающих гарантированного

качества обслуживания (non-QoS), и работоспособность критически важных сетевых сервисов может быть нарушена. Кроме того, у самой технологии мультикаст имеются уязвимости, которые приводят к осуществлению тех или иных атак (мультикаст DoS-атаки). Для решения проблемы безопасности при использовании во ВУКИП мультикаст технологии передачи пакетов предлагается использовать МСЭ. Однако существующие МСЭ фактически не пропускают мультикаст пакеты, так как они предназначены только для обработки уникаст пакетов. Также из соображений безопасности МСЭ по умолчанию блокируют UDP порты, открытость которых для мультикаст передачи является необходимостью. Для обеспечения прохождения мультикаст трафика через МСЭ, были предложены методы туннелирования, которые позволяют туннелирование мультикаст дейтаграммы через МСЭ. Туннелирование мультикаст трафика заключается в инкапсуляции мультикаст UDP дейтаграмм в уникаст UDP дейтаграмм. Однако эти методы не гарантируют того, что злонамеренный мультикаст трафик не будет проходить в защищенные области. Для мультикаст экранирования ВУКИП предлагается вводить МСЭ наряду с фильтрующим уникаст маршрутизатором [5]. В этом случае уникаст пакеты передаются через фильтрующий уникаст маршрутизатор, а мультикаст пакеты через МСЭ, который осуществляет политику безопасности мультикаст, также управление полосой пропускания путем разрешения или запрещения тех или иных пакетов мультикаст на основе определенных правил. При этом для обеспечение безопасного прохождения мультикаст трафика через МСЭ предлагается использовать структуру SOCKS5, которая является одним из решений МСЭ. Использование структуры SOCKS5 для управления мультикаст потоками во ВУКИП дает некоторые преимущества безопасности перед существующими подходами МСЭ.

Литература

1. Алгулиев Р.М. Шыхалиев Р.Г. Об одном методе определения отношения доступа во взаимоувязанных корпоративных информационных пространствах // Известия НАНА, №2, 2005.
2. Шыхалиев Р.Г. Каскадное экранирование взаимоувязанных корпоративных информационных пространств. XIV Общероссийская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", Санкт-Петербург, Россия, 05-07 октября 2005.
3. Шыхалиев Р.Г. Моделирование межсетевых экранов с фильтрацией пакетов на основе сетей Петри // Известия НАНА, №2, 2005.
4. Алгулиев Р.М., Шыхалиев Р.Г. Об одном методе оценки эффективности экранирования взаимоувязанных корпоративных информационных пространств // Информационные технологии моделирования и управления, №3(28), 2006.
5. Шыхалиев Р.Г. Об одном методе экранирования мультикаст трафика во взаимоувязанных корпоративных информационных пространствах// Информационные технологии №8, 2006.