ции с помощью программных обеспечений Spam Brave, Spam Fighter и SpamArrow.

Суммируя полученные данные, мы пришли к выводу, что самым эффективным для фильтрации спама из рассмотренного программного обеспечения является SpamArrow. Следует отметить, что эффективность SpamArrow была связана с тем, что она предварительно была обучена. Таким образом, для практического использования антиспам-фильтров вначале следует установить необучаемые фильтры для сбора спам-сообщений, и лишь затем использовать обучаемые фильтры.

Заключение

Предлагаемый подход включает координацию работы всех агентов по фильтрации спамов в отдельности на каждом уровне: национальное (государственное), корпоративное, индивидуальное информационные пространства.

Отличием от всех существующих подходов к фильтрации СНР является то, что здесь рассматривается централизованное администрирование и управление фильтрацией, обнаруживающей сообщения спамного характера в национальной Интернет-инфраструктуре.

Список литературы

1. www.spamtest.ru/document?pubid=19222&context=1.
2. **Куликов Л. С., Телеснин Б. А.** и др. Модульный принцип при разработке систем обработки текстовых документов // Телекоммуникации. 2004. № 6. С. 6—11.
3. **Власов А. И., Цыганов И. Г.** Адаптивная фильтрация информационных потоков в корпоративных системах на основе механизма голосования пользователей // Информационные технологии. 2004. № 9. С. 12—19.
4. **Тропина Т. Л.** Криминализация электронных посягательств // Новые проблемы юридической науки: Сборник мат. конф. Владивосток. 2005. С. 264—271.
5. **Convention** of Cybercrime Budapest, 23.11.2001
6. **Алгулиев Р., Джабраилова З.** Азербайджан — соорганизатор Тунисского Саммита в создании информационного общества // Ренессанс. Баку: 15 ноября. 2005 (на азербайджанском).
7. **Баранов П. А.** Обзор средств борьбы со спамами и e-mail вирусами // Компьютерные системы. 2004. № 1. С. 44—50.
8. **Сырков Б. Ю.** "Киллеры" и "едоки" или борьба со спамами // Технологии и средства связи. 2004. № 4. С. 102—105.
9. **Рон Андерсон.** Избавляемся от спама // Сети и системы связи. 2004. № 11 (117). С. 94—104.
10. **Pelletier L., Almhana J., Choulakian V.** Adaptiv Filtering of SPAM // Proceedings of the Second Annual Conference on Communication Networks and Services Research. IEEE. 2004. P. 530—537.
11. **Scott A. D.** Multiagent Systems Engineering of Organization based Multiagent Systems // ACM. October 2005. P. 230—235.
12. **Тутубалин А., Ашманов И.** Методика тестирования качества антиспам-фильтров. 2003 // http://www.lexa.ru/articles/anti-spam-testing.html.
13. www.softplatz.com/software/anti-spam.

УДК 004.056

Р. Г. Шыхалиев,
Институт информационных технологий НАН Азербайджана

Об одном методе экранирования мультикаст-трафика во взаимоувязанных корпоративных информационных пространствах

Предлагается метод экранирования мультикаст-трафика во взаимоувязанных корпоративных информационных пространствах на основе межсетевого экрана (МСЭ). В основу метода положена структура SOCKS, которая является одним из решений МСЭ. Рассмотрены угрозы, связанные с мультикаст-технологией, и аспекты безопасности мультикаст-трафика, а также способы безопасной организации мультикаст-передачи пакетов через МСЭ на основе SOCKS.

Введение

Взаимоувязанные корпоративные информационные пространства (ВУКИП) являются совокупностью структурно и функционально интегрированных корпоративных информационных пространств (КИП). 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 числу пользователей. Например, мультикаст-технология может использоваться при создании потока мультимедийных данных для передачи блока новостей, корпоративных объявлений и проведения аудио- и видеоконференций. При мультикаст-передаче каждый пакет одновременно отправляется всем необходимым адресатам без дублирования.

Появление протокола Н.323, который поддерживает мультикаст-передачу пакетов и основанных на этом протоколе мультимедийных приложений, значительно увеличило возможности создания и передачи потоков мультимедийных данных. Однако имеются 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 *To-*

ken Ring), не обеспечивающих гарантированного качества обслуживания (*non-QoS*), и работоспособность критически важных сетевых сервисов может быть нарушена. Кроме того, у самой мультикаст-технологии имеются уязвимости, которые приводят к осуществлению тех или иных атак (мультикаст-*DoS*-атаки). В имеющихся работах по применению мультикаст-технологии в основном описываются проблемы управления мультикаст-трафиком без должного уделения внимания безопасности.

Для решения проблемы безопасности при использовании во ВУКИП мультикаст-технологии передачи пакетов предлагается использовать межсетевые экраны (МСЭ). Как известно, МСЭ является одним из механизмов, который широко используется для обеспечения информационной безопасности КИП, также МСЭ является самым важным объединяющим элементом различных КИП, использующих разную политику обеспечения безопасности. Концепция обеспечения информационной безопасности МСЭ состоит в предписании политики контроля доступа между двумя сетями. При этом роль МСЭ заключается в фильтрации сетевых пакетов на основе некоторых критериев, которые разрешают или запрещают прохождение пакетов, чтобы контролировать доступ к защищенной сети [1]. 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 в работах [2, 3] были предложены методы, которые позволяют туннелирование мультикаст-дейтаграммы через МСЭ. Туннелирование мультикаст-трафика заключается в инкапсуляции мультикаст-*UDP* дейтаграмм в уникаст-*UDP* дейтаграмм и осуществляется протоколом *UMTP* (*UDP Multicast Tunneling Protocol*). Однако эти методы не гарантируют того, что злонамеренный мультикаст-трафик не будет проходить в защищенные области.

Из сказанного выше следует простое утверждение, что необходимо решение, которое позволит обеспечить надежное экранирование ВУКИП. Работ по экранированию ВУКИП, в которых передается мультикаст-трафик, практически нет, и это область мало изучена. Поэтому данная статья посвящена так называемому "мультикаст-экранированию" ВУКИП, т. е. безопасному развертыванию мультикаста во ВУКИП на основе МСЭ. В статье рассматривается случай, когда во всех локальных сетях ВУКИП не поддерживается мультикаст-технология. Нетрудно предположить, что в этом случае при использовании мультикаст-технологии во ВУКИП обостряется проблема обеспечения ее информационной безопасности. Для мультикаст-экранирования ВУКИП предлагается вводить МСЭ наряду с фильтрующим уникаст-маршрутизатором. В этом случае уникаст-пакеты передаются через фильтрующий уникаст-маршрутизатор, а мультикаст-пакеты через МСЭ, который осуществляет политику безопасности мультикаст и управление полосой пропускания, путем разрешения или запрещения тех или иных мультикаст-пакетов на основе определенных правил. При этом для обеспечения безопасного прохождения мультикаст-трафика через МСЭ предлагается использовать структуру SOCKS, которая является одним из решений МСЭ. Использование структуры SOCKS для управления мультикаст-потоками во ВУКИП дает некоторые преимущества безопасности перед существующими подходами МСЭ.

Мультикаст-технология передачи пакетов

Мультикаст-передача пакетов была разработана из потребности эффективной посылки информации множеству получателей и служит для уменьшения объема передаваемой по сети информации. Эта технология определена IETF (*The Internet Engineering Task Force* — Оперативная группа проектирования Интернет) в 1989 г. Основная идея состоит в том, чтобы создать службу, которая позволит формировать коммуникационные группы. Коммуникационные группы состоят из нескольких членов, которые получают все данные, посланные группе. В *IP*-протоколе зарезервирован специальный блок адресов с 224.0.0.0 по 239.255.255.255 — это так называемые адреса групп, членами которых могут быть *IP*-адреса конкретных хостов в сети. Мультикаст-технология включает два существенных компонента:

- компонент, размещенный на маршрутизаторе, который позволяет любому маршрутизатору связаться с другими маршрутизаторами для надлежащего установления мультикаст-дерева;
- компонент, размещенный на хосте, который позволяет приложению приемника уведомить непосредственно граничащие мультикаст-маршрутизаторы о том, что он хочет присоединиться к мультикаст-группе или покидает группу, членом которой он является. Это осуществляется на основе протола *IGMP*. Мультикаст-маршрутизаторы периодически передают запросы о групповом членстве, чтобы определить, какие группы имеют членов, в непосредственно связанных с ним подсетях. Хост через определенное время посылает отчет о групповом членстве в каждую группу, к которой он принадлежит, чтобы избежать "затопления" *IP*-пакетами.

Мультикаст-дерево — кратчайший путь распространения мультикаст-трафика от источника к получателям, который соединяет всех членов мультикаст-группы.

Мультикаст-передача пакетов имеет два главных преимущества:

- простая адресация — данные к мультикаст-группе посылаются по единственному адресу, идентифицирующему эту группу, и только один раз (рис. 1); каждый член группы получает посланные группе данные;
- низкое потребление ресурсов — данные, доставляемые по дереву мультикаста за одно соединение, передаются однократно, т. е. они на соответствующих точках только один раз копируются и передаются.

Для более широкого внедрения мультикаст-приложений и услуг в 1992 г. была создана специальная

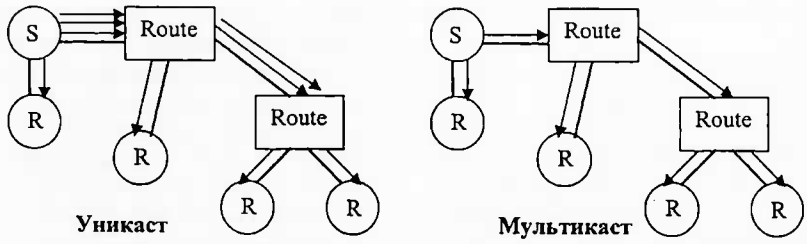

Рис. 1. Передача пакетов в уникаст- и мультикаст-системах, где *S* — *source* (источник), *R* — *receiver* (получатель)

информационная магистраль в рамках сети Интернет — *Multicast Backbone (MBone)*. Эта магистраль появилась в результате первых экспериментов комитета IETF, в которых аудио- и видеоинформация передавалась с применением мультикаст в сети Интернет. Цель создания *MBone* состояла в построении тестовой магистрали, поддерживающей мультикаст-передачу пакетов для последующей разработки, тестирования и внедрения приложений, поддерживающих мультикаст.

Угрозы, связанные с мультикаст-технологией

При рассмотрении угроз, связанных с мультикаст, немаловажным является понимание фундаментальных отличий между мультикаст- и уникаст-технологиями передачи. При уникаст-технологии соединение осуществляется только между парами участников. Безопасность таких соединений основывается на безопасности этих участников (например, на аутентификации каждого участника). Кроме того, доверие в уникаст-соединении может базироваться на доверии к каждому участнику, а также к данным. Наоборот, мультикаст-технология для соединения вовлекает произвольное число участников, с потенциально изменяющимся составом, чье членство никогда полностью неизвестно. Поэтому безопасность мультикаст-соединений основывается на безопасности данных, а не участников. В частности, мультикаст-соединение может быть аутентифицировано посредством аутентификации пакетов данных, например, с использованием цифровой подписи, а для обеспечения его конфиденциальности использовано шифрование данных. Доверие в мультикаст-соединении базируется исключительно на доверии к данным.

Способ адресации, используемый в мультикаст-технологии передачи вносит определенные проблемы безопасности, поскольку созданный при соединении так называемый "псевдоним адреса" (*address alias*) может использоваться для злонамеренного исследования портов.

Основная проблема безопасности при использовании мультикаст-технологии появляется тогда, когда хост присоединяется к мультикаст-группе, что дает посторонним возможность направлять трафик к любому его UDP-порту, включая порты, которые должны быть доступны только по явному разрешению. Таким образом, мультикаст-технология позволяет нападавшему иметь доступ к любому порту на хосте, как только этот хост присоединяется к мультикаст-группе. Поэтому номер порта дейтаграмм должен проверяться и фильтроваться. Вопрос заключается в том, как администратор безопасности может решить, какие номера портов он может разрешить, а какие фильтровать. Из соображения безопасности конфигурацией по умолчанию должен быть запрещен доступ ко всем UDP-портам. Однако в действительности проблема с UDP связана с приложениями, которые используют этот протокол, например, такими как *NFS* (*Network File System* — сетевая файловая система) или *NIS* (*Network Information System* — сетевая информационная система) и т. д. Блокирование доступа к тем или иным портам, которые используются определенными приложениями, несущими угрозы, приводит к тому, что эти приложения на отдельных хостах не запускаются.

Мультикаст-технология является уязвимой к *DoS* атакам. Имеются три типа мультикаст-*DoS*-атак: *MSDP*, *ICMP* и *PIM DoS*-атаки. Некоторые атаки следуют из некорректного выполнения протокола. Однако большинство проблем происходят вследствие недостаточной спецификации протоколов. Например, протокол *MSDP* имеет некоторые слабости, т. е. этот протокол активно рекламирует источник, передающий мультикаст по всей инфраструктуре мультикаст. Он обменивается полезной информацией, используя механизм лавины, который делает *MSDP* по сути немасштабируемым. Атаки черви *RAMEN* и более новые черви *Sapphire* являются примерами того, как *MSDP* механизм лавины может использоваться для проведения *MSDP DoS*-атаки [4]. Другим классом *DoS*-атаки, заслуживающим рассмотрения, является тот, который осуществляется на основе протокола *IGMP*, т. е. *IGMP DoS*-атаки. Эта *DoS*-атака может осуществляться конечными хостами очень легко, так как они могут подсоединяться к большему числу мультикаст-групп и затопить внутреннюю сеть нежелательным трафиком. Наконец, третьей *DoS*-атакой является *PIM DoS*-атака, которая основывается на перегрузке маршрутизаторов большим числом *PIM* состояний, которые создаются для того, чтобы рассылать нежелательный трафик.

Проблема с *DoS*-атаками может быть наиболее эффективно решена двумя способами. Первый способ заключается в ограничении использования мультикаст, т. е. оно должно быть разрешено только доверенным хостам и группам. Это может предотвратить *IGMP* и *MSDP DoS*-атаки, начатые внутри сети. Второй способ заключается в фильтрации поддельных пакетов, которые генерируются в результате *DoS*-атак, начатых из внешних сетей.

Политика экранирования мультикаст

Политика экранирования мультикаст заключается в определении набора разрешенных мультикаст-групп и соответствующих UDP-портов, которые являются канди-

датами на передачу через МСЭ. Администраторы сети должны быть уверены, что группы/порты мультикаст, которые они определяют для передачи, действительно являются безопасными. В частности, администраторы должны быть знакомы с приложениями, которые получают и обрабатывают мультикаст-данные (а также и с уникаст-приложениями), и быть уверенными, что они не могут причинить вреда (например, выполнят опасный код, полученный по сети). Имеются три основных пути, по которым МСЭ может поддержать такую политику:

1. *Статическая конфигурация.* МСЭ, при котором множество кандидатов групп/портов может быть определено заранее, например, в файле конфигурации.

2. *Явная динамическая конфигурация.* Множество кандидатов групп/портов может быть определено (и обновлено) динамически на основе явного запроса одного или многих доверенных пользователей (предположительно внутренних). Например, МСЭ может содержать механизм дистанционного управления, который позволяет этим доверенным клиентам после аутентификации модернизировать набор кандидатов групп/портов.

3. *Неявная динамическая конфигурация.* Множество кандидатов групп/портов может быть определено неявно на основе некоторой предварительно авторизованной мультикаст-группы/порта, типа директории сессии (*session directory*). Например, предположим, что политика безопасности разрешает произвольной *MBone SAP/SDP* директории сессии [5] быть переданой так же, как любые сессии, которые объявлены в этой директории. МСЭ может использовать содержание директории сессии, чтобы динамически модернизировать состав кандидатов.

В ВУКИП важным является динамическое определение того, когда и какие мультикаст-группы должны передаваться через МСЭ. Однако для обеспечения высокой степени безопасности, даже, если мультикаст-группа становится кандидатом для передачи через МСЭ, фактическая передача не должна быть осуществлена сразу, а только тогда, когда есть фактический интерес в передаче этой группы. Причины этого следующие: во-первых, передача мультикаст-группы требует, чтобы пользователи одной или обеих сторон МСЭ присоединились к группе, это устанавливает МСЭ в состояние мультикаст-маршрутизатора. Это неэффективно, если нет никакого текущего интереса в передаче группы (особенно, для Интернет-интранет передачи). Во-вторых, акт передачи нежелательной мультикаст-группы потребляет ненужные ресурсы непосредственно самого МСЭ. Поэтому лучший путь определения для МСЭ, когда группа-кандидат должна быть передана, является использование фактической информации мультикаст-маршрутизации, и при этом МСЭ действует как межсетевой мультикаст-маршрутизатор. Во ВУКИП, который состоит из большого числа подсетей, для определения членства пользователей в группе-кандидате на передачу может использоваться механизм, называемый *"Domain Wide Multicast Group Membership Reports"* [6].

Мультикаст-экранирование ВУКИП

Для обеспечения безопасного развертывания мультикаст во ВУКИП МСЭ должен обеспечивать решение следующих задач:

- контроль выходящего за пределы ВУКИП мультикаст-трафика;
- контроль поступающего во ВУКИП мультикаст-трафика;
- контроль доступа (подключения) к мультикаст-группам;
- обеспечение безопасности внутренних пользователей, которые присоединяются к внешней мультикаст-группе (совместимой с безопасностью, определенной уникаст-политикой безопасности);
- обеспечение детальной регистрации всех мультикаст сессий;
- ограничение использования полосы пропускания поддерживающей сетевой инфраструктуры ВУКИП потоками, которая может привести к *DoS*-атакам.

Метод, предлагаемый нами для мультикаст-экранирования ВУКИП, который позволяет решить перечисленные задачи, заключается в том, что наряду с фильтрующим уникаст-маршрутизатором предлагается использовать структуру SOCKS, которая является одним из решений МСЭ (рис. 2).

В этом случае фильтрующий уникаст-маршрутизатор осуществляет экранирование уникаст, а SOCKS — экранирование мультикаст, т. е. контроль доступа к мультикаст и управление полосой пропускания выполняется путем разрешения или запрещения тех или иных мультикаст-пакетов, используемых мультимедийными приложениями. Структура SOCKS состоит из двух частей: первая часть — это сервер *MSS* (*Multicast SOCKS Server*), который играет роль прокси, а вторая часть — клиент *MSC* (*Multicast SOCKS Client*), который размещается в хостах ВУКИП.

Использование структуры SOCKS для управления мультикаст-потоком в ВУКИП обеспечивает следующие преимущества в обеспечении безопасности перед существующими подходами МСЭ:

- MSS на основе аутентификации идентифицирует пользователя, ко-

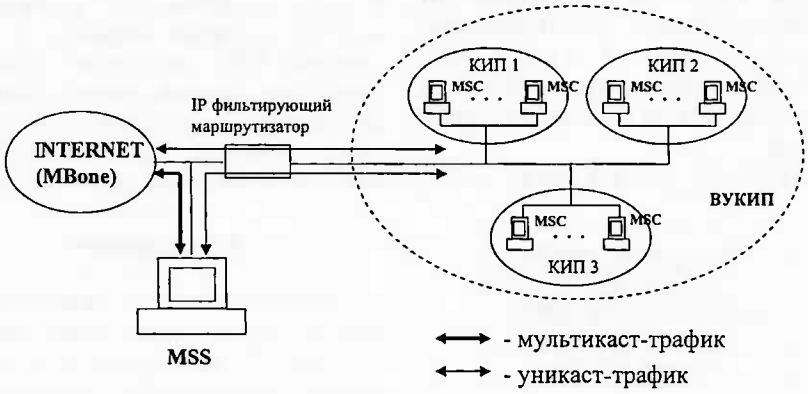

Рис. 2. Мультикаст-экранирование ВУКИП

торый требует соединения с мультикаст-группой, в обычном же подходе простая текущая проверка запроса *ICMP* указывает только то, что какой-то пользователь хочет присоединиться к конкретной группе;

- MSS, кроме адреса группы, к которой пользователь хочет присоединиться, также известен порт, что позволяет MSS фильтровать трафик на основе конкретного адреса группы и порта и блокировать трафик, который имеет адрес этой группы, но направлен к иному порту. Это дает возможность защитить пользователей, которые присоединяются к внешней группе, в обычном же подходе, где МСЭ проводит текущий контроль запроса ICMP, определяется только адрес группы;
- сервер SOCKS играет роль прокси, который может преобразовать мультикаст-пакеты в уникаст и при этом может обеспечить высокий уровень безопасности (аутентификацию, целостность, конфиденциальность).

SOCKS был создан для того, чтобы обеспечивать стандартную среду для прозрачного и безопасного выполнения уникаст-передачи пакетов через МСЭ [7]. Для этого между транспортным и прикладным уровнями добавляется уровень SOCKS (рис. 3). При таком решении соединение между парами узлов состоит из двух соединений: одно соединение осуществляется между первым узлом и МСЭ, а второе — между МСЭ и вторым узлом. Установка соединения проводится с клиентского приложения, находящегося на рабочих станциях клиентов. Соединение перехватывается клиентской библиотекой SOCKS с последующим преобразованием в протокол SOCKS. При этом сторонам кажется, что они непосредственно соединены друг с другом.

Протокол SOCKS также определяет метод аутентификации связывающихся узлов. Так как мультикаст-передача не направлена на соединения между парами узлов как в уникаст-передаче, то для нее модель SOCKS является менее подходящей. Однако в доработках модели, SOCKS v5 [8], были предложены возможности организации мультикаст-передачи через МСЭ. Возможны два способа организации мультикаст-передачи пакетов через МСЭ:

- *multicast-to-unicast mode* (*MU-mode*), в которых в пределах внутренней сети (между МСЭ и каждым членом внутренней мультикаст-группы) используется уникаст-соединение, т. е. поступающий извне мультикаст-трафик преобразуется в уникаст и, наоборот, уникаст-трафик, который отправляется из внутренней мультикаст-группы, преобразуется в мультикаст;
- *multicast-to-multicast* (*MM-mode*), в которых уникаст-соединение используется для управления передачей клиент—МСЭ, а мультикаст-соединение — для других соединении в пределах внутренней сети.

При нашем подходе экранирования ВУКИП предлагается использовать первый способ, так как способ MU обеспечивает более высокий уровень обеспечения безопасности мультикаст, чем способ MM. Это объясняется следующими причинами:

- при MU способе уникаст-пакеты, сформированные MSS для MSC, и наоборот, становятся трудно перехватываемыми для устройств перехвата сообщений;
- использование аутентификации при инкапсуляции UDP пакетов поддерживается способом MU тогда как способом MM не поддерживается. Таким образом, в MU способе MSS, используя аутентификацию пакетов, может решить, отправлять пакет или нет, тогда как в способе MM необходимо проверить *IP*-адрес источника.

Прикладной уровень
SOCKS уровень
Транспортный уровень
Сеансовый уровень
Сетевой уровень

Рис. 3. Модель SOCKS

Заключение

Необходимость использования мультимедийных приложений в ВУКИП увеличивает потребность в применении мультикаст-технологии передачи пакетов. Однако передача мультикаст-трафика в ВУКИП 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 гарантированное качество обслуживания (*non-QoS*), и работоспособность критически важных сетевых сервисов может быть нарушена. При этом недостатки в управлении мультикаст-трафика могут привести к мультикаст-*DoS*-атакам.

Для решения проблемы безопасности при использовании во ВУКИП мультикаст-технологии передачи пакетов предлагается использовать МСЭ. Однако существующие МСЭ фактически не обрабатывают мультикаст-трафики, так как они предназначены только для обработки уникаст-передачи пакетов.

Для мультикаст-экранирования ВУКИП мы предлагаем структуру SOCKS v5, которая является одним из механизмов МСЭ. Использование структуры SOCKS v5 для управления мультикаст-трафиком обеспечивает некоторые преимущества в обеспечении безопасности (аутентификация, целостность и конфиденциальность) перед существующими подходами МСЭ.

Список литературы

1. **Алгулиев Р. М., Шыхалиев Р. Г.** Методы и технологические аспекты экранирования взаимоувязанных корпоративных информационных пространств. Баку: Элм, 2003. 106 с.
2. **Finlayson R.** The UDP Multicast Tunneling Protocol // Internet Engineering Task Force (IETF), draft-finlayson-umtp-*.txt. 2002 September.
3. **Chouinard D.** SOCKS V5 UDP and Multicast Extensions to facilitate multicast firewall traversal // Internet Engineering Task Force (IETF), draft-ietf-aft-mcast-fw-traversal-*.txt. 1997. November.
4. **Djahandari K., Sterne D. F.** An MBone Proxy for an Application Gateway Firewall // IEEE Symposium on Security and Privacy. 1997.
5. **Handley M., Jacobson V.** SDP: Session Description Protocol, FC 2327. 1998. April.
6. **Fenner B.** Domain Wide Multicast Group Membership Reports, Work-in-Progress, Internet-Draft draft-ietf-idmr-membership-reports-01.txt, August, 1998.
7. **Leech M.** et. al. SOCKS Protocol Version 5 // RFC 1928. 1996. March.
8. **Chouinard D.** SOCKS V5 UDP and Multicast Extensions, Work-in-Progress // Internet-Draft "draft-chouinard-aft-socksv5-mult-00.txt". 1997. July.