

УДК 681.322

## МЕТОДЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ NGN

**А.С. Аджемов**, генеральный директор ФГУП ЦНИИС, к.т.н.

**В.А. Ефимушкин**, директор по науке ФГУП ЦНИИС, к.ф.-м.н.

**Введение.** В настоящее время на российском и зарубежных телекоммуникационных рынках происходят изменения, оказывающие существенное влияние на деятельность операторов связи. Они характеризуются рядом рыночных, технических и регуляторных тенденций, обозначенных, например, в [1]. Ведущие зарубежные операторы внедряют масштабные проекты по модернизации сетей связи на базе пакетных технологий, строительству сетей следующего поколения (NGN, NGN Next Generation Network). К операторам, модернизация сетей которых является приоритетным стратегическим шагом, относятся British Telecom, KPN, Telecom Italia, France Telecom, Verizon, NTT, China Telecom, компании, входящие в ОАО «Связьинвест». При этом ведущие производители (Siemens, Nortel, Lucent, Ericsson, Italtel и др.) прекратили или уже прекращают выпуск оборудования с коммутацией каналов. Традиционные операторы связи реализуют масштабные проекты по строительству сетей доступа на базе оптических и других технологий следующего поколения для обеспечения рыночных требований к широкополосному доступу. Растет конкуренция со стороны новых участников рынка — поставщиков услуг Интернета (Google, Skype, Mail.ru, Rambler) и операторов вещания («Корбина», «Стрим»), оказывающих привлекательные услуги и заинтересованных в снижении цен на услуги доступа операторов связи.

Транспортной составляющей быстро развивающихся сетей NGN и Интернет является пакетная сеть. Поскольку концепция сети NGN зиждется на использовании IP-сетей и обширного, постоянно расширяющегося стека протоколов TCP/IP в качестве своей транспортной основы, в ближайшем будущем все услуги связи, от привычной нам телефонии, до современных мультимедийных, по сути, могут стать технологическими заложниками сетей IP. Таким образом, сети IP, образуя общий для Интернета и сетей NGN ресурс, являются в настоящее время важнейшим объектом с точки зрения возникновения реальных угроз информационной безопасности сетевого и информационного пространства России и других государств, особенно при трансграничном обмене.

**Конвергенция сетей NGN и Интернет.** Интернет состоит из сетей, эксплуатируемых государственными учреждениями, университетами, корпорациями и другими организациями, взаимосвязанными друг с другом различными видами оборудования, такими, как маршрутизаторы, мосты, коммутаторы. Для связи сетей, входящих в Интернет, используется договор пиринга — обмена трафиком Интернета между двумя и более сетями. Пиринг может осуществляться либо через частное соединение «точка-точка» между двумя сетями, либо через точку обмена трафиком для большего числа сетей. Крупнейшая в России точка обмена трафиком — московская система обмена Internet Exchange (MSK-IX). Число участников системы MSK-IX превысило 100 Интернет-провайдеров, при этом помимо московских провайдеров к MSK-IX подключены провайдеры С.-Петербурга, Иркутска, других городов России, а также Казахстана и Украины. Система обмена MSK-IX имеет распределенную структуру и включает в себя несколько точек, соединенных волоконно-оптическим кабелем, часть из которых объединена в замкнутую кольцевую структуру с резервированием трафика. В

случае сбоя в работе канала между двумя точками, трафик передается по альтернативному пути, в обход проблемного участка через другие точки. Благодаря распределенной структуре MSK-IX существенно расширяются возможности для московских и региональных провайдеров по подключению к системе обмена IP-трафиком, так как в любой точке доступа осуществляется высокоскоростное подключение.

Аналогичные точки обмена трафиком под управлением АНО «Российский НИИ развития общественных сетей» (РосНИИРОС) функционируют в С.-Петербурге (SPB-IX) и Новосибирске (NSK-IX). Предусматривается строительство региональных точек обмена трафиком во всех городах России с населением больше 1 млн человек.

Таким образом, современная сеть Интернет, базирующаяся на высокоскоростной оптической транспортной среде и широкополосных радиоканалах, развитом управлении процессами установления соединений и организации многосторонних сеансов связи, ориентированная на предоставление неограниченного множества мультимедийных услуг с использованием стандартизированных средств разработки и удаленного введения их в эксплуатацию, находится в процессе конвергенции с нынешними инфокоммуникационными сетями, и, прежде всего, с сетями NGN, что приводит к появлению всепроникающего глобального инфокоммуникационного пространства с возможностями самоорганизации и неограниченного роста информационного содержания [2].

**Уязвимость протоколов стека TCP/IP.** Уязвимости протоколов стека TCP/IP используются злоумышленниками для проведения атак на сеть и ее информационные ресурсы. Наиболее часто уязвимости появляются из-за дефекта программного обеспечения или неправильной настройки, а также из-за несовершенства формализованных правил и процедур самих протоколов, определяющих формат и способ передачи данных.

К типовым удаленным атакам на информацию в сети вследствие несовершенства IP-протоколов относятся: анализ сетевого трафика сети, внедрение ложного объекта сети, внедрение ложного маршрута.

Уязвимости присущи протоколам различных уровней стека TCP/IP: сетевому, транспортному и прикладному, причем наиболее уязвимыми являются самые распространенные протоколы Интернета, что связано с тем, что во времена их разработки вопросам безопасности не уделялось должного внимания. За прошедшие годы подход к обеспечению информационной безопасности распределенных сетей существенно изменился. Разработаны различные протоколы обмена, позволяющие защитить сетевое соединение и зашифровать трафик (SSL, SKIP и т. п.), однако они не сменили традиционные протоколы и не стали стандартом (может быть, за исключением SSL). На сегодняшний день в подавляющем большинстве используются стандартные протоколы семейства TCP/IP, среди которых к наиболее уязвимым относятся следующие: протоколы управления передачей TCP, межсетевое взаимодействие IP, разрешения адресов ARP, управляющих сообщений сети Интернет ICMP, эмуляции терминала Telnet и передачи файлов FTP, службы доменных имен DNS и сетевого управления SNMP.

Таким образом, задача выявления и ликвидации уязвимостей протоколов стека TCP/IP с целью снижения угроз и рисков, повышения эффективности мер безопасности сети и информационных ресурсов крайне актуальна в контексте конвергенции сетей NGN и Интернет.

Архитектура безопасности сети Интернет описывается документами IETF. Основными направлениями стандартизации здесь являются:

- обеспечение безопасности сетевой инфраструктуры (архитектура безопасности IP-протокола и обеспечение безопасности протоколов управления TCP/IP-сетями на сетевом и транспортном уровнях);
- обеспечение безопасности обмена информацией между конечными системами, приложениями или пользователями (протоколы обеспечения безопасных коммуникаций между уровнями прикладного уровня).

Приоритетным считается использование средств безопасности на прикладном уровне, что позволяет получать многие услуги с соответствующим программным обеспечением, группами сетевых протоколов и различными сетевыми операционными системами. Реализация функций безопасности в виде дополнений к основным протоколам позволяет использовать их в зависимости от требуемого уровня безопасности или доверительности к промежуточным системам.

Архитектура безопасности сети на базе стека протоколов TCP/IP предполагает применение механизмов контроля доступа в соответствии с системой распределения открытых ключей, изложенной в Рекомендации [4] МСЭ-Т. Данная система используется для защиты данных в электронной почте повышенной секретности (PEM, Privacy Enhanced Mail), в системах и службах обработки сообщений [5], а также для поддержки механизмов безопасности службы директорий [6] и управления сетями связи [7].

Важным элементом этой архитектуры является обеспечение безопасности сетевых приложений сети Интернет, требующих использования на прикладном уровне аутентификации, контроля доступа, др.

**Проблема международной информационной безопасности.** Почти 10 лет назад, в принятом в сентябре 1998 г. на встрече президентов России и США совместном заявлении с символическим названием «Об общих вызовах безопасности на рубеже XXI века», констатировалось согласие активизировать совместные усилия по противодействию транснациональным угрозам экономике и безопасности наших стран, включая преступления с использованием компьютерной техники и других высоких технологий. Данные вызовы привели к необходимости поставить проблему обеспечения международной информационной безопасности (МИБ) перед международным сообществом. Россия — инициатор этого процесса — в ходе 53-й Сессии Генеральной ассамблеи ООН представила проект резолюции, принятый 4 декабря 1998 г. консенсусом № 53/70 под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [7]. Документ № A/54/213, внесенный Россией в ООН 9 июня 1999 г., уже тогда предлагал в целях построения МИБ среди 16 основополагающих принципов разработать процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия.

За прошедший период проблема обеспечения МИБ при трансграничном обмене информацией с использованием сетей на базе IP, включая сети NGN и Интернет, существенно обострилась и требует расширения межгосударственной координации, в том числе в рамках деятельности ООН, ШОС, МСЭ, форумов по вопросам управления использованием Интернета [8].

Использование трансграничного обмена по Интернету хакерскими сообществами уже сейчас просматривается в отдельных событиях мировой политики — от участия в информационных войнах во время локальных конфликтов (Палестина — Израиль, США — Ирак и т. д.) до антиглобалистских акций (кража и распространение секретной информации во время Давосского форума) [9].

Соответствующие указанному направлению законодательные принципы действуют в области информационной и телекоммуникационной сферы Российской Федерации [10—12], многих других стран мира. В Указе президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [13] подчеркивается необходимость обеспечения информационной безопасности при передаче информации через государственную границу, в том числе при использовании международной компьютерной сети Интернет.

При этом мы не должны забывать, что архитектура Интернета создавалась в условиях, когда внутри сети существовало доверие к действиям отдельных участников. В результате разросшийся Интернет несет на себе отпечаток «младенчества» и почти не содержит встроенные механизмы безопасности. Если участник сети (маршрутизатор) заявляет, что он владеет блоком адресного пространства, остальная часть сети IP верит ему на слово и адресует ему весь соответствующий трафик. Значит, можно создать любой сетевой блок и запустить его в IP-сети, придав анонимность любой атаке. «Сумеречные зоны», наряду с технологиями подмены авторства кардинально меняют способы ведения войны в пространстве сетей Интернета и NGN, в том числе удаленно, трансгранично, что выводит проблему МИБ при управлении ресурсами Интернета на одно из первых мест [9, 14].

Успехи в построении информационного общества в России, активизация процессов глобализации инфокоммуникаций, в которых Россия уверенно встраивается в группу основных участников, требует решения проблем международной информационной безопасности в сетях NGN и в последующем — во всепроникающем глобальном инфокоммуникационном пространстве.

Растущий уровень угроз информационно-телекоммуникационным ресурсам и масштабы преступности с их использованием — существенный довод в пользу создания защищенной транспортной сети на базе технологий и стека протоколов TCP/IP, внедрения государством технологий обязательной идентификации пользователей.

**Методы обеспечения информационной безопасности в NGN в контексте МИБ.** Поддержание информационной безопасности в сети NGN в контексте МИБ должно обеспечиваться реализацией следующих общих методов:

- защита сети NGN от преднамеренных и непреднамеренных трансграничных дестабилизирующих воздействий, способных нарушить предоставление абонентам услуг связи;
- централизованный аудит и мониторинг событий трансграничного характера, связанных с нарушениями безопасности сети NGN;
- аутентификация и авторизация персонала, имеющего доступ к программным и аппаратным средствам управления сетями NGN;
- защита передаваемой информации управления вызовами и сетью NGN.

За поддержание информационной безопасности сети NGN с учетом аспектов МИБ должна отвечать система информационной безопасности.

Основными ее задачами являются:

- обеспечение устойчивости сети к преднамеренным и непреднамеренным трансграничным дестабилизирующим воздействиям, способным нарушить предоставление абонентам услуг связи с заданным уровнем качества обслуживания;
- организация аудита и мониторинга событий трансграничного характера, связанных с информационной безопасностью;
- реализация усиленной аутентификации и авторизации персонала, имеющего доступ к программным и аппаратным комплексам управления сетью NGN;
- разделение передаваемого трафика абонентов оператора сети NGN, обеспечивающее взаимное непроникновение трафика различных абонентов;
- обеспечение конфиденциальности и целостности передаваемой информации управления.

Технически система информационной безопасности сети NGN может быть построена в соответствии со следующими основными принципами:

- централизованное управление компонентами сети с автоматизированного рабочего места администратора информационной безопасности;
- реализация централизованной усиленной аутентификации на отдельной независимой аппаратной платформе с использованием современных средств идентификации и единой базы пользователей;
- централизованное управление аутентификационной информацией пользователей с единой консоли, установленной на автоматизированном рабочем месте администратора информационной безопасности;
- использование механизмов активного аудита на сетевом и системном уровне и централизованного хранения информации аудита;
- консолидация всех событий, связанных с информационной безопасностью в единой базе данных (например, с использованием механизмов syslog) и применение автоматизированных средств анализа журналов аудита на основе программного обеспечения;
- разделение, по необходимости, передаваемого трафика пользователей услугами связи с использованием средств MPLS VPN;
- резервное копирование критичных компонентов сети;
- использование резервного (спутникового) канала связи для случаев, когда управление через магистральные каналы невозможно.

Система информационной безопасности сети NGN должна состоять из структурных подсистем администрирования и мониторинга/аудита, ориентированная в контексте МИБ прежде всего на трансграничные воздействия. Первая из подсистем — централизованная, с автоматизированным рабочим местом администратора ИБ, должна содержать технические решения, реализующие функции:

- аутентификации и авторизации обслуживающего персонала;
- контроля доступа и защиты от несанкционированного доступа с использованием механизмов MPLS VPN и средств межсетевое экранирования;
- контроля защищенности сетевых объектов и компонентов системы информационной безопасности с применением сканеров защищенности;
- резервного копирования критичной информации систем информационной безопасности и управления;
- управления компонентами системы информационной безопасности, реализующими функции данной структурной подсистемы, а также обеспечения безопасного удаленного доступа к оборудованию сетевых узлов.

Подсистема мониторинга и аудита содержит технические решения, реализующие такие функции системы информационной безопасности, как:

- активный аудит объектов защиты, а также сегментов сети IP, системы управления с использованием средств обнаружения и пресечения атак трансграничного характера;
- регистрацию событий международной информационной безопасности и автоматизированный анализ журналов аудита;
- управление компонентами.

Подсистема мониторинга и аудита может реализовывать функции активного аудита, регистрации событий в контексте международной информационной безопасности, подсистему управления.

**Заключение.** Проблема информационной безопасности телекоммуникационных сетей в контексте МИБ в настоящее время, в условиях существенного роста тенденций к конвергенции сетей связи следующего поколения и Интернет, взаимопроникновения их услуг и приложений выходит на одно из главных мест и требует серьезного внимания.

#### ЛИТЕРАТУРА

1. Telecommunications Predictions — 2008 // Deloitte, TMT Trends-2008.
2. **Стрельцов А.А., Аджемов А.С., Гермогенов А.П., Ефимушкин В.А.** Основные аспекты управления использованием ресурсами Интернета в целях обеспечения международной информационной безопасности // В сб. трудов 9-й международной конференции «Состояние и перспективы развития Интернета в России: от сетей к сервисам». — М.: Изд-во МТУСИ, 2008.
3. Recommendation ITU-T X.509. Open systems interconnection — The Directory: Public-key and attribute certificate frameworks. — 2000.
4. Recommendation ITU-T X.400. — June, 1999.
5. Recommendation ITU-T X.500. Open Systems Interconnection. The Directory: Overview of concepts, models and services. — 2001.
6. Recommendation ITU-T X.700. Management framework for Open Systems Interconnection (OSI) for CCITT applications. — 1992.
7. **Крутских А.В.** Война или мир: международные аспекты информационной безопасности // Политика. — 2001, № 45.
8. **Streltsov A.A.** International information security: description and legal aspects // Disarmament Forum. — 2007, № 3.
9. **Песков Д.Н.** Интернет в мировой политике и международных отношениях // В сб.: Современные международные отношения и мировая политика. Под ред. А.В. Торкунова. — М., 2005.
10. Федеральный Закон Российской Федерации от 7 июля 2003 г. № 126-ФЗ «О связи».
11. Федеральный Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. Федеральный Закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
13. Указ президента РФ от 19 марта 2008 г. «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
14. **Аджемов А.С., Гермогенов А.П., Ефимушкин В.А.** Ограничение анонимности при трансграничном электронном обмене как механизм обеспечения международной информационной безопасности // Труды семинара ЮНИДИР «Информационные и коммуникационные технологии и международная безопасность», 24—25 апреля 2008. — Женева, Швейцария.

Получено 24.09.08