Джураев Р. Х.
Джаббаров Ш.Ю.
Холмурадов Т.Н.
Юлдашева Ш.Ш.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ NGN

Аннотация. В данной статье рассматриваются основные стандарты в области обеспечения информационной безопасности сетей NGN ведущих международных организаций по стандартизации.

The present article views the main standards and requirements within the information securing of the leading international organizations of standardization.

Закономерным результатом эволюции сетей телекоммуникаций становятся сети следующего поколения (Next Generation Network, NGN), которые станут основой национальной инфокоммуникационной инфраструктуры.

Однако интенсивное развитие сетей NGN обуславливает появление проблем, касающихся их информационной безопасности. Это требует необходимости пересмотра ее значения в связи с возрастанием зависимости национальной инфокоммуникационной нфраструктуры от безопасного функционирования сетей NGN.

Обеспечение безопасности сетей NGN представляет собой комплексную проблему, которая решается в направлениях совершенствования правового регулирования их применения, совершенствования методов их разработки, обеспечения соответствующих организационно- технических условий эксплуатации. Ключевым аспектом решения проблемы безопасности NGN является выработка системы требований, критериев и показателей для оценки уровня безопасности NGN.

Между ведущими международными организациями достигнуты договоренности в области стандартизации и обеспечения совместимости различных решений по вопросам безопасности сетей телекоммуникаций. Координатором данных работ является сектор стандартизации телекоммуникаций Международного союза телекоммуникаций (Telecommunication Standardization Sector of International Telecommunication Union, ITU-T), который взял на себя, помимо разработки нормативных документов и рекомендаций, ответственность по мониторингу аналогичных действий в ряде других международных и региональных организаций. Также разработкой международных стандартов в области обеспечения информационной безопасности сетей NGN, находящейся еще на начальном этапе, занимается ряд международных организаций (ISO, ETSI, IETF 3GPP и 3GPP2.), которые решают следующие основные вопросы: разработка общепринятых терминов и определений, что способствует созданию единого языка общения специалистов;

- разработка стандартов в области архитектуры безопасности, определяющих область применения и общие принципы построения систем обеспечения информационной безопасности;
- обеспечение технологической и организационной совместимости при реализации мер по обеспечению информационной безопасности сетей NGN.

Ключевыми нормативными документами ITU-T по вопросам безопасности NGN являются Рекомендация X.805 «Архитектура безопасности систем телекоммуникаций, обеспечивающих связь «из конца в конец» (X.805. Security architecture for systems providing end-to-end communications. 2003) и совместно разработанный с ISO стандарт ISO/IEC 18028-2 «Архитектура безопасности сетей» (ISO/IEC 18028:2006. Information technology - Security techniques - IT network security).

В настоящее время в ITU создана рабочая группа FGNGN (NGN Focus Group), основной задачей которой является изучение потребностей индустрии

телекоммуникаций для реализации NGN. В составе FGNGN было создано семь рабочих групп, которые учитывают поступающие предложения и выполняют стандартизацию по различным аспектам NGN. В FGN разрабатываются нормативные документы «Guidelines for NGN security» (Руководство по безопасности NGN) и «NGN security requirements for Release 1» (Требования по безопасности NGN для версии 1). В вышеуказанном Руководстве рассматривается модель угроз для сетей NGN, основанная на рекомендациях ITU X.800 и X.805, приводятся риски различных пользователей NGN, даны рекомендации по размещению механизмов и сервисов безопасности на различных уровнях эталонной модели взаимодействия открытых систем. В документе «Требования по безопасности NGN-Релиз 1» содержатся требования по безопасности к услугам и пользователям сетей следующего поколения, включая интерфейсы транспортного уровня и уровня услуг. В этих требованиях отражены основные положения безопасности, изложенные в Рекомендации ITU X.805, а также требования безопасности транспортного уровня и требования безопасности уровня услуг. «Требования по безопасности NGN-Релиз 1» были оформлены в виде Рекомендации ITU Y.2701 «Сети следующих поколений. Безопасность» (Security requirements for NGN release 1. 2007), содержащей требования, согласно которым необходимо обеспечивать безопасность сети для взаимодействия конечных пользователей через многосетевые административные домены.

В рекомендации ITU-T Y.2201 «Требования к NGN. Версия 1», наряду с высокоуровневыми требованиями для разработки набора рекомендаций, которые будут служить основой для построения сетей NGN, определены также и основные требования к безопасности NGN, такие как идентификация, аутентификация, авторизация, общие требования к безопасности, живучесть (требования к защитной коммутации, повторной маршрутизации и способности услуг к восстановлению), защита важной инфраструктуры и неразглашение информации в межсетевых интерфейсах NNI.

Существуют различные варианты построения сетей NGN. Первым шагом к этому можно считать создание Европейским институтом стандартов телекоммуникаций(European Telecommunications Standards Institute, ETSI) рабочей группы TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks). Важным этапом работы TIPHON стала разработка сетевой модели распределенного шлюза, физически разделившая функции сети по управлению вызовом и функции по поддержанию сессии обмена данными. В 2003 году в ETSI в результате слияния рабочих групп TIPHON и SPAN (Services and Protocols for Advanced Networks) была образована рабочая группа TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking), которая в настоящее время является основным подразделением ETSI по стандартизации. Она отвечает за стандартизацию современных и перспективных конвертируемых сетей, включая VoIP и NGN, а также за все, что связано с архитектурой IMS. На данный момент в области информационной безопасности NGN TISPAN разработаны следующие стандарты:

- ETSI TS 187 001 VI. 1.1 (03/2006) «Безопасность NGN. Требования», в котором предложены требования безопасности, как для магистральной сети, так и для сети доступа. Также разработанные требования безопасности приведены в соответствие с подсистемами и интерфейсами NGN: подсистемой доступа к сети NASS, подсистемой управления ресурсами и доступом RACS, подсистемой передачи мультимедийных данных по IP-сетям, подсистемой эмуляции ТфОП/ISDN - PES и сервером приложений AS;
- ETSI TR 187 002 VI. 1.1 (03/2006) «Безопасность NGN. Анализ угроз и рисков безопасности», в нем представлены результаты анализа рисков и уязвимости при возможных угрозах (Threat Vulnerability Risk Analysis, TVRA) для двух сценариев NGN версии 1: эмуляция ТфОП/ISDN и групповая аутентификация NASS-IMS. Также в этом стандарте определяются интерфейсы и сценарии, влияющие на безопасность NGN,

проводится анализ NGN с точки зрения возможных угроз и рисков безопасности, и кроме того проводится классификация установленных слабых мест и связанных с ними рисков;

– ETSI TS 187 003 VI. 1.1 (02/2008) «Безопасность NGN. Архитектура безопасности), в нем представлена архитектура, удовлетворяющая требованиям безопасности NGN версии 1, а также определены архитектуры безопасности для обеспечения защиты всех функциональных архитектур сетей и подсистем NGN (NASS, RACS, PES, IMS). Данный стандарт рассматривает аспекты безопасности для базовой сети NGN и для сети доступа, включая оконечные станции NGN в домене индивидуальных пользователей.

Оконечные станции NGN являются логической пограничной точкой между абонентским доменом, базовой сетью и сетью доступа NGN и поддерживают соответствующие интерфейсы. В приложении к стандарту представлен список и описание интерфейсов безопасности для всех сетей и подсистем NGN.

ETSI TISPAN работает в тесном сотрудничестве с рабочей группой 3 3GPP по вопросам NGN/IMS- безопасности: регулярно проводятся рабочие встречи, обсуждения и обмен информационными материалами с целью недопущения параллельной работы по одной проблеме, но в разных направлениях, конечным результатом которой не должно быть две совершенно разных спецификации по безопасному доступу.

Вопросами безопасности в 3GPP занимается рабочая группа 3, работы которой включают в себя анализ угроз, в том числе и новые типы угроз для IP-услуг, требования по безопасности и решения по защите. Серия спецификаций 33 в настоящее время включает в себя 43 спецификации, посвященных аспектам безопасности 3G. 3GPP задает архитектуру IP мультимедиа-подсистемы (IMS) для мобильных систем телекоммуникаций третьего поколения, поддерживающих видео-, аудио- и мультимедиа-конференции,

используя SIP в качестве протокола сигнализации и IP в качестве транспортной среды.

Спецификации безопасности для IMS описаны в документе 3GPP TS 33.203 версия 7.5.0 релиз 7 «Безопасность 3G. Безопасность доступа для услуг на основе 1P». В данной спецификации определены особенности и механизмы защиты для безопасного доступа к IMS для мобильных систем телекоммуникаций третьего поколения. В приложении к документу также представлены материалы, которые отражают, как основные положения документа могут быть применимы к фиксированным широкополосным сетям.

Документ TR 33.802 «Анализ возможности технической реализации расширений безопасности IMS» определяет требования и решения по безопасности для фиксированного широкополосного доступа к IMS как продолжение спецификации TS 33.203. Очевидно, что «ранние» (первые) внедрения IMS были построены без полного соответствия требованиям TS 33.203.

Технический отчет 3GPP TR 33.978. Версия 6.6.0. Релиз 6 «Аспекты безопасности для ранних подсистем IMS» на основе требований для «начальных внедрений» определяет простые механизмы безопасности, базируясь на существующей безопасности сетей.

Проект 3GPP2 появился как детище Международной инициативы мобильных телекоммуникаций IMT-2000 (International Mobile Telecommunications), существующей в рамках ITU. Проект 3GPP2 занимается проблемами высокоскоростных, широкополосных и основанных на IP-протоколе мобильных телекоммуникационных систем. Работой над спецификациями 3GPP2 занимаются четыре технические группы (Technical Specification Groups - TSG), где вопросы безопасности находятся под контролем рабочей группы 4 - «Безопасность», входящей в группу TSG-S - «Аспекты систем и услуг». На основе спецификации 3GPP TS 33.203 v5.4.0 была разработана спецификация 3GPP2 S.R0086-A vl.O «Структура безопасности IMS». Этот документ направлен на обеспечение безопасного доступа и безопасности сети для

сервисов, основанных на IP-протоколе. Областью применения данной технической спецификации является определение характеристик безопасности и механизмов для защиты доступа к IMS.

IMS поддерживает такие мультимедийные IP-приложения как видео-, аудио - и мультимедийные конференции, используя протокол SIP в качестве протокола сигнализации для установления и завершения мультимедийных сессий. Эта спецификация обращена только к таким случаям, как защита сигнализации SIP между абонентом и IMS, а также аутентификация абонента в IMS и аутентификация IMS абонентом.

Кроме вышеперечисленных организаций, занимающихся стандартизацией в области информационной безопасности NGN, существует также рабочая группа по стандартам для сети Интернет. В рамках IETF работают 17 рабочих групп, занимающихся вопросами информационной безопасности. Практически во все разрабатываемые спецификации включаются разделы, посвященные обеспечению безопасной работы описываемой технологии.

К настоящему времени международной организацией IETF разработано множество спецификаций, фактически имеющие статус стандартов, предназначенных для обеспечения информационной безопасности при работе в общедоступной сети Интернет. Поскольку в сетях следующего поколения используется много различных протоколов IETF, то можно отметить следующие спецификации, в которых рассматриваются вопросы безопасности NGN:

- RFC 2460 «Спецификация Интернет-протокола. Версия 6» (Internet Protocol, Version 6 (IPv6). Specification. 1998);
- RFC 3550 «Транспортный протокол для приложений реального времени» (RTP: A Transport Protocol for Real-Time Applications. 2003);
- RFC 2326 «Протокол потоковой передачи реального времени» (Real Time Streaming Protocol, RTSP. 1998);

- RFC 2327 «Протокол описания сеансов» (SDP: Session Description Protocol. 1998);
- RFC 3015 «Протокол медиа- шлюзов» (Megaco Protocol Version 1.0. 2000);
- RFC 3261 «Протокол инициирования сеансов» (SIP: Session Initiation Protocol. 2002);
- RFC 3711 «Защищенный транспортный протокол реального времени» (The Secure Real-time Transport Protocol (SRTP). 2004).

Во всех этих спецификациях, напрямую не относящихся к механизмам обеспечения информационной безопасности, присутствует раздел, описывающий возможные угрозы и пути их предотвращения.

В Международном институте стандартизации (ISO) стандартизацией вопросов IT-безопасности занимается специальная комиссия 27 Объединенного технического комитета 1 (Joint Technical Committee 1 Special Committee 27, JTC 1/SC 27), в которую входит пять рабочих групп, которые занимаются рассмотрением следующих вопросов:

- требования, службы безопасности и общие принципы;
- методики и механизмы безопасности;
- общие критерии безопасности;
- средства управления и службы безопасности;
- управление идентификацией и технологии защиты конфиденциальности.

Одним из множества важных стандартов является стандарт ISO/IEC 15408:2005 «Критерии оценки безопасности информационных технологий» (Information technology - Security techniques - Evaluation criteria for IT security), называемые «Общими критериями».

Выполнение требований стандарта ISO/IEC 15408 - необходимое, но далеко не достаточное условие информационной безопасности информационных систем, наряду с ним существуют другие важные стандарты, рациональное использование которых может положительно сказаться на достигаемом уровне информационной безопасности информационных систем.

ISO/IEC TR 15443:2005 «Структура обеспечения безопасности 1Т». Стандарт состоит из трех частей и является руководством для профессионалов в области информационной безопасности при выборе подходящего гарантированного метода для определения выбора или развертывания услуг безопасности, продукта или фактора влияния окружающей среды, например, организации или персонала.

ISO/IEC 17799:2005 «Практические правила управления информационной безопасностью» предлагает широкий взгляд на управление информационной безопасностью. В качестве элементов управления рассматриваются технические и организационно- административные меры, направленные на обеспечение конфиденциальности, целостности, достоверности и доступности информации.

Стандарт ISO/IEC TR 18044:2004 «Управление инцидентами информационной безопасности» устанавливает рекомендации по менеджменту инцидентов информационной безопасности для руководителей подразделения по информационной безопасности, информационных систем, сервисов и сетей.

ISO/IEC 27006:2007 «Требования для органов аудита и сертификации систем управления информационной безопасностью» определяет требования и обеспечивает управление для лиц, проводящих аудит и сертификацию систем управления информационной безопасностью, в дополнение к требованиям, содержащимся в ISO/IEC 17021 и ISO/IEC 27001.

Также одним из основных стандартов ISO/IEC в области IT- безопасности является разработанный совместно с ITU стандарт ISO/IEC 18028, состоящий из пяти частей:

- управление сетевой безопасностью;
- архитектура сетевой безопасности;.
- безопасная связь между сетями с использованием шлюзов;
- безопасный удаленный доступ;
- безопасная связь с использованием виртуальных частных сетей».

В целях ускорения разработки отраслевой нормативной базы в области информационной безопасности, определяющей вопросы скоординированного и согласованного внедрения защищенных технологий NGN, необходимо создание отраслевых стандартов в сфере связи и информатизации на основе прямого применения международных рекомендаций ITU-T и документов ETSI. Кроме того в целях совершенствования законодательства в области обеспечения информационной безопасности необходимо дополнить существующие законы, в статьях которых говорится об информационной безопасности, указаниями о необходимости использования оборудования, сертифицированного по требованиям безопасности информации.

Список использованной литературы:

1. Next Generation Network Security. ITU-T/IETF Workhsop on NGN. 1 -2 May 2005. Geneva.
2. ISO/IEC 18028:2006. Information technology - Security techniques – IT network security.
3. МСЭ-Т. X.805. Security architecture for systems providing end-to-end communications. 2003.
4. ETSITS 187 001 v 1.1.1 (2006-03) NGN SECurity (SEC); Requirements.
5. Грибунин В.Г. Безопасность сетей NGN. / «Информационная безопасность», №№ 1 , 2 - 2006.
6. Соколов И. Ф. Роль стандартов в обеспечении информационной безопасности. / Проблемы информатизации. - 2001. - № 2. - С. 22-26.
7. Джураев Р.Х., Давронбеков Д.А., Джураев О.Р. Особенности сертификации систем и средств ИКТ на основе общих критериев. Вестник ТУИТ – 2010 г. №2.