О проблемах информационной безопасности в сети Интернет

В. А. Васенин, А. В. Галатенко
Центр телекоммуникаций и технологий Интернет
Московский государственный университет им. М. В. Ломоносова

Важность проблем информационной безопасности в сети Интернет проистекает из того значения, которое приобрела эта всемирная коммуникационная сеть в настоящее время и рост которого прогнозируется на будущее. Работы по различным аспектам информационной безопасности, информационно-вычислительных систем в том числе е и компьютерных сетей, ведутся и в России, и в остальном мире уже достаточно долго, но феномен чрезвычайно быстро развивающейся системы глобальных коммуникаций, какой является Интернет, выдвигает новые проблемы и ставит старые в новый контекст. Решение этих проблем требует, прежде всего, пристального рассмотрения с научных и практических позиций, анализа истории, текущего состояния и закономерностей развития главного объекта – всемирной компьютерной сети Интернет.

Важно отметить, что, несмотря на то, что на сегодняшний день в Интернет огромное количество информационных ресурсов, а США сосредоточено больше, чем во всех остальных странах мира, вместе взятых, сеть уже настолько плотно интегрирована в международное информационное и экономическое пространство, что не может использоваться группой людей или отдельной страной исключительно в собственных интересах. Она достаточно велика, чтобы развиваться по своим собственным законам и не быть в необходимой степени управляемой, чтобы существовала возможность эффективно в одностороннем порядке использовать её в качестве орудия нападения. Иными словами, при помощи сети можно нанести ущерб, но при этом невозможно сохранить приемлемый уровень собственной защищённости от аналогичных атак. В то же время, развитие Интернет сделало возможным проведение в сети согласованных акций с недостижимой ранее массовостью, в том числе и потенциально опасных – таких как сетевые атаки или, например, вычисления с целью взлома шифров.

Краткий обзор истории и перспектив развития Интернет

Развитие Интернет началось около 30 лет назад и большую часть времени происходило преимущественно в США. Сеть росла быстрыми темпами, и примерно 15 лет назад начался период её беспрецедентно быстрого роста, в том числе и в других странах мира. Сегодня общее количество хостов в Интернет близко к 100 млн., количество пользователей оценивается в 300 – 400 млн. чел., ёмкости магистральных каналов составляют сотни мегабит в секунду и приближаются к гигабитным величинам. Показатели России выглядят несколько более скромно: около 300 тыс. хостов, порядка 2 млн. активных пользователей, но процессы развития сети идут по крайней мере не менее интенсивно, чем в мире в целом.

Сети с пакетной коммутацией начали разрабатывать в 50-х годах по заказу военных. Целью было обеспечение устойчивости связи к нарушениям работы отдельных участков. Именно этот краеугольный принцип организации сети делает неэффективными и искусственные ограничения её функциональности. Лет через пять – в начале 60-х – стало понятно, что такую сеть можно создать. Но отдельными закрытыми группами реализовать такой проект невозможно, и поэтому в 1968 году к нему были подключены исследовательские лаборатории и научные центры. К 1969 году сложилась первая базовая инфраструктура, объединившая несколько коммуникационных узлов в ведущих университетах, и первые же эксперименты показали, что сеть работает. Инфраструктура была предоставлена учёным, техническим специалистам, которые должны были изучить и усовершенствовать её возможности и разработать технологии и методы её применения. Тогда были созданы сетевые службы, которые и сейчас являются базовыми для Интернет. В первой половине 70-х был разработан и затем почти десять лет проходил "обкатку" универсальный протокол TCP/IP, для которого к настоящему времени создано много различных приложений. Во все эти исследовательские проекты вкладывались в основном деньги американского правительства.

Когда в 1985 году образовалась сеть NSFNET, ёмкость каналов, соединявших ее опорные узлы, составляла всего 56 кбит/с. Правительство США выделило на срок до 1995 года средства на дальнейшие исследования, апробацию перспективных технологий и приложений , а также доводку инфраструктуры сети до промышленной эксплуатации. В начале 90-х к проектам

активно начали привлекать крупные коммерческие компании, которые стали участвовать в совершенствовании инфраструктуры, исследованиях приценяться к разработкам и вкладывать средства в те из них, которые можно быстро превратить в законченные продукты. С развитием компьютерной техники и сетевых технологий стала быстро расти популярность сети как в академических, так и в промышленных кругах, сфере бизнеса, появился значительный платежеспособный спрос. Так сеть, первоначально требовавшая на своё развитие значительных инвестиций государства, постепенно вышла на самоокупаемость. К 1995 году, концу данного периода развития, уже появились коммерческие продукты и специалисты, которые были в состоянии их обслуживать. Сложившаяся сеть полностью перешла в коммерческую эксплуатацию – так появился Интернет.

С небольшим опозданием, но с аналогичной поддержкой государства и активным участием крупного бизнеса в тесном взаимодействии с Интернет в США в те же годы развилась европейская инфраструктура Интернет.

Развитие сетевой инфраструктуры в России началось позже, с конца 80-х годов. Однако темпы роста российского сегмента Интернет с 1994 года даже несколько превосходят среднемировые, о чем свидетельствует, например, динамика роста количества хостов, емкости внешних шлюзов в международные сети, показатели развития опорной инфраструктуры и освоения технологий Интернет [1, 2].

С 1995 года в США выполняется крупномасштабная программа по развитию новой исследовательской сети на базе высокоскоростной магистрали – vBNS. Так начались работы по созданию сети нового поколения, условно называемой Internet2 (так же называется один из крупнейших проектов в этом направлении). Работы распланированы до 2005 года. В проекте уже участвуют сотни американских университетов, научных центров, каждый из них разрабатывает какую-то часть новых технологий, сервисов и приложений на их основе, и одновременно готовит необходимые для их развития кадры. Формируется высокопроизводительная исследовательская сеть, которая пока не используется для передачи обычного трафика Интернет. Но через несколько лет она станет основой общедоступной сети нового поколения, работающей на коммерческих началах. В новом проекте государство вкладывает средства не только в развитие базовой сетевой инфраструктуры, но в большей степени в конкретные перспективные сетевые технологии, сервисы и приложения.

И в Европе, и в развитых регионах Азии государства пошли по пути, аналогичному США – вкладывают деньги в перспективу. Европейские сети продвинулись даже дальше, поскольку объединились не в национальную структуру, как в США, а в межгосударственную – TEN-155. Почти все европейские страны вкладывают в неё средства. Она также замкнута и не обеспечивает прямого подключения участников к традиционному Интернет. Пройдет ещё несколько лет, и в её рамках будут созданы решения, которые станут основой новых сетевых технологий: новые протоколы маршрутизации, решения, ориентированные на IPv6, новые службы, создание которых было невозможно на Интернет первого поколения. Тогда созданные учёными технологии будут переданы в коммерческое использование. К этому времени будет подготовлена и инфраструктура, и необходимые приложения, на ней работающие, и соответствующие кадры. Именно в развитии подобных проектов, на мой взгляд, должна выражаться основная поддержка Интернет со стороны государства и в России.

В настоящее время государственная поддержка развития компьютерных телекоммуникаций осуществляется в основном через Межведомственную программу НСКТ НВШ (Национальная сеть компьютерных телекоммуникаций для науки и высшей школы). В отличие от аналогичных Национальных программ крупнейших стран мира Межведомственная программа в России сохраняет финансирование обоих направлений:

– технологии, ресурсы и приложения традиционного Интернет как Метасети общего пользования (на базе опорной сети RBNet);
– технологии, ресурсы и приложения Интернет нового поколения как вновь нарождающейся высокопроизводительной инфраструктуры со своей (отличной от традиционного Интернет) политикой использования и развития.

Необходимость финансирования работ на первом направлении связана с более поздним включением России в мировое Интернет-сообщество, с неразвитостью базовых составляющих Национальной сетевой инфраструктуры, в первую очередь, транспортной среды, наличием монополизма и рядом других объективных факторов.

В рамках первого направления Межведомственной программы на базе волоконно-оптической магистрали АО «Ростелеком» (на условиях аренды канальных емкостей) в 1996 –

1998 гг. построена и успешно эксплуатируется RBnet (Russian Backbone network) [3,4] – Национальная опорная сеть для науки и образования. Российская опорная сеть RBnet создана как магистральная инфраструктура для Национальной научно-образовательной сети. В настоящее время это одна из самых больших магистральных IP–сетей в России, соединяющая более 30 регионов страны.

Одной из важнейших целей Межведомственной программы было построение экспериментального ядра высокоскоростной сетевой инфраструктуры для исследования и апробации телекоммуникационных и информационных технологий нового поколения, суперкомпьютерных приложений и поэтапное развитие с целью превращения в инфраструктуру сети национального масштаба. Первым проектом в этом направлении было создание в 1996 – 98 гг. экспериментального ATM–полигона на базе сети MSUNet Московского государственного университета им. М. В. Ломоносова и организация современных высокоскоростных служб Интернет поверх протокола ATM.

В настоящее время высокопроизводительные экспериментальные полигоны на базе ATM построены и успешно эксплуатируются не только в Москве, (сеть RASNet РАН, Freenet, Relarn IP и др.) и Санкт-Петербурге (RUNNet, Роксон, RUSNet), но и в Екатеринбурге и Владивостоке, Ростове, Самаре. и Краснодаре . Идет процесс объединения таких исследовательских полигонов в единую высокопроизводительную научно-образовательную сеть России.

Формирование высокопроизводительных сетей в России вызвало интерес со стороны Национального научного фонда США. Результатом сотрудничества в этой областиМинистерства науки и технологий РФ и Национального научного фонда США стало открытие в 1999 г. в рамках проекта MirNet прямого цифрового ATM-канала связи между вновь формирующейся российской высокопроизводительной сетью и самой скоростной на сегодня в мире американской сетью vBNS. Точкой доступа к этому каналу в США стал первый узел транснационального обмена трафиком высокопроизводительных международных и национальных сетей науки и образования STAR TAP в Чикаго. С появлением этого канала связи российские высокопроизводительные сети науки и образования получили возможность доступа к аналогичным сетям не только США, но и других стран мира [5]. Таким образом, созданы предпосылки для равноправного участия России в наиболее передовых проектах по развитию современных сетевых технологий.

Основные проблемы Интернет сегодняшнего дня:
- ограниченность адресного пространства;
- перегрузка маршрутизаторов на магистральных каналах;
- необходимость обеспечения качества сервиса – QoS и резервирования ресурсов;
- информационная безопасность;
- регулируемость.

Главные задачи проектов NGI и Internet-2 (США) в ближайшие годы: магистрали ёмкостью до 2,4 Гбит/с, экспериментальная сеть с полосой пропускания до 1 Гбит/с (сквозной), достижение скорости коммутации пакетов 1 Тбит/с. С этой целью ведётся работа над службами, протоколами и системами, по таким направлениям, как:
- QoS;
- безопасность и устойчивость;
- управление и техническое сопровождение сетевых систем и ресурсов;
- протоколы маршрутизации, коммутации, широковещания, транспортирования, защиты;
- новые операционные платформы компьютеров;
- распределённые среды для коллективной разработки приложений.

В относительно краткий и заведомо неполный список основных направлений развития технологий Интернет, по которым на сегодняшний день ведутся активные работы в России, в том числе в МГУ им. М. В. Ломоносова, можно включить следующие:
- сетевая поддержка высокоскоростной интегрированной сети (новые протоколы маршрутизации, IPv6, IP поверх ATM, обеспечение качества сервиса и многое другое);
- безопасность сети (защищённые операционные среды, активный аудит, управляемость сети, современные системы идентификации и аутентификации);
- распределённые приложения (технологии CORBA, XML и т. д.);
- многоадресные и широковещательные мультимедиа-системы;
- современные кластерные технологии;
- сетевой мониторинг (контроль ATM-каналов с оперативным анализом результатов);
- модели и методы исследования крупных сетевых структур.

Информационная безопасность в открытых IP-сетях

Одной из важнейших проблем, обусловленных беспрецедентно быстрым ростом Интернет и его влиянием на все сферы жизни общества, стала проблема обеспечения безопасности информационных ресурсов сети, и защиты сетевой инфраструктуры, поддерживающей эти ресурсы. Для этого есть веские основания. Достаточно констатировать объёмы угроз на примере США: по результатам исследований (опросов) Института компьютерной безопасности и ФБР в течение 1999 г. 30% сетевых компьютеров взломано, 57% – атаковано внешними пользователями, 55% – внутренними, а по 33% не известно, были ли взломаны, или нет, общий ущерб за год составил несколько млрд. долл.. В проекте бюджета США на 2000 г. выделено около 1,5 млрд. долл. на компьютерную безопасность и защиту критически важной информации.

Одним из первых в этом направлении было исследование Министерства обороны США (DoD), в результате которого в 1980 – 82 гг. были разработаны рекомендациями по использованию межсетевой архитектуры протоколов DARPA в качестве базовых на DDN (Defence Digital Networks). С тех пор работы в этом направлении целенаправленно ведутся не только на IP-сетях "силовых" ведомств США, но и других экономически развитых стран мира. Позже, но с не меньшей интенсивностью, начались работы по созданию. систем информационной безопасности в Интернет в интересах других направлений государственного производственно-хозяйственного комплекса, академической сферы, бизнеса и др.. Большинство исследований в области информационной безопасности проводятся коллективами научных центров и университетов в рамках проектов на высокопроизводительных полигонах исследовательских сетей.

Подходы к решению проблем информационной безопасности на российских IP-сетях должны строиться на основе анализа опыта на этом направлении, но с учетом специфики процессов развития российского Интернет. В условиях ограниченных возможностей государственного финансирования этих работ необходимо сосредоточить внимание на наиболее важных (ключевых) задачах и найти методы их решения, опирающиеся на высокий потенциал российских математических и программистских школ.

Национальный сегмент Интернет, как и Метасеть в целом, представляет собой совокупность множества сетей (локальных, местных или региональных, ведомственных или корпоративных), имеющих прямые (ISP) или опосредованные (через ISP или субпровайдера) каналы связи с зарубежными сетями. Каждая из таких сетей имеет свою административную подчинённость, обладает своей инфраструктурой и информационно-вычислительным ресурсом, которые определяют специфику именно этой сети в реализации системы мер на административном (политика безопасности), операционном (работа с людьми) и, соответственно, программно-техническом уровне. Однако, отталкиваясь от сложившейся структуры российского сегмента Интернет (да и не только российского), в качестве типового элемента сложной иерархической системы составляющих её сетей, инфраструктурных и информационно-вычислительных ресурсов, которые требуют защиты, следует рассматривать корпоративную (или ведомственную) сеть. Такая сеть, как правило, подчинена крупной организации или ведомству, имеет несколько распределённых (на местном или даже межрегиональном уровне) точек присутствия (кампусов).

Содержанием задачи информационной безопасности (ИБ) в сети является защита информации и сетевой инфраструктуры от широкого спектра угроз – внутренних и внешних, преднамеренных и случайных. Для выбора адекватных мер противодействия угрозам необходима их подробная классификация. В частности, различная политика безопасности требуется для различных объектов (сетей): режимного учреждения, коммерческого предприятия, некоммерческой (академической) организации. Источниками угроз могут быть как люди (пользователи и администраторы, умышленно или по некомпетентности), так и неисправные технические средства, и, при определённых условиях, природные явления. В числе основных направлений противодействия угрозам можно указать следующие:

- ликвидировать возможность осуществить атаку, тем самым предотвратить ущерб;
- принять меры по сокращению ущерба:
  - сократить подверженный угрозе объём ресурсов,
  - сократить время восстановления,
  - организовать раннее предупреждение;
- обнаружить злоумышленника после атаки.

Для сетевой информации принято различать угрозы доступности (невозможность получить информацию за приемлемое время), целостности (нарушение актуальности, непротиворечивости, разрушение или несанкционированное изменение) и конфиденциальности (несанкционированный просмотр). С учетом многообразия субъектов – потенциальных нарушителей, методов и средств как подготовки и реализации атаки, так и защиты, эти проблемы традиционно включают несколько уровней реализации, каждый из которых имеет свои задачи и пути решения. В числе таких уровней можно указать законодательный, административный, операционный и программно-технический.[6].

Законодательный уровень ИБ включает в себя как меры прямого законодательного действия (квалифицирующие нарушения и нарушителей), так и меры направляющие и координирующие (образование в области ИБ, разработки и распространение средств обеспечения ИБ).

Административный уровень ИБ предусматривает следующие составляющие:

- политика безопасности (документированные управленческие решения для защиты информации и инфраструктуры на основе анализа рисков),
- управление рисками, координация деятельности, стратегическое управление и контроль,
- контроль сервисов безопасности .

Операционный уровень ИБ подразумевает такие мероприятия, как:

- управление персоналом,
- физическая защита,
- поддержание работоспособности и восстановление после сбоев,
- заблаговременная проработка реакции на нарушения режима ИБ.

Программно-технический уровень ИБ содержит следующие сервисы:

- идентификация и аутентификация,
- управление доступом,
- протоколирование и аудит,
- криптография,
- экранирование.

Этот уровень, как наиболее специфический для проблем безопасности в Интернет, рассмотрим более подробно.

Программно-технический уровень информационной безопасности

Программно-технические меры, обеспечивающие информационную безопасность в Интернет, строятся на тех возможностях, которые предоставляет для этого межсетевой протокол IP (сетевой уровень является ключевым, наиболее подходящим для решения этих задач) и стек протоколов TCP/IP на его базе. Изначально разрабатываемая для исследовательской сети (1973 – 83 гг.), без учёта темпов развития Интернет в будущем и его влияния на общество, место в мировом информационном пространстве, внутренняя структура IP-пакетов не была в должной мере ориентирована на решение задач информационной безопасности в том объёме и масштабах, которые предъявляют сегодня (а тем более, на будущее) интернет-приложения.

Для построения системы информационной безопасности, адекватной потребностям корпоративной IP-сети, необходимы следующие средства защиты программно-технического уровня:

- средства реализации защищённых коммуникаций по открытым каналам между точками присутствия сети;
- межсетевые экраны (разграничение доступа);
- средства идентификации/аутентификации, поддерживающие концепцию единого входа в сеть (пользователь один раз при входе доказывает свою подлинность и далее имеет доступ ко всем сервисам сети в соответствии с имеющимися полномочиями);
- средства протоколирования и аудита, обеспечивающие мониторинг сети на всех уровнях, выявляющие подозрительную активность и реализующие оперативное реагирование;
- средства защиты, входящие в состав приложений, сервисов и аппаратно-программных платформ;
- средства централизованного администрирования сети.

Совокупность этих средств призвана в значительной степени покрыть потребности защиты на программно-техническом уровне. Однако следует заметить, что на сегодня такого набора средств, обеспеченных сертификацией по требованиям безопасности, ни для

государственных учреждений или ведомств, ни, тем более, коммерческих структур в необходимом объёме не существует. Сертифицированные ФАПСИ система "ШИП" для поддержания частных виртуальных сетей, средства криптографической защиты "Верба", ряд межсетевых экранов для использования в сетях государственных организаций, защищённые ОС и СУБД составляют лишь малую часть необходимого набора. С одной стороны, это объективно, принимая во внимание тот короткий временной интервал, в течение которого происходило становление российского сегмента Интернет, и экономическую ситуацию в стране в эти годы. С другой стороны, отмеченные обстоятельства указывают на необходимость поиска неординарных, комплексных подходов на этом направлении, объединения усилий ведущих в этой области организаций и специалистов для подготовки необходимого набора средств программно-технического уровня в относительно короткие сроки.

Для этого необходимо определить сетевые полигоны, на которых эту работу можно было бы эффективно организовать (как на поисковом, исследовательском, опытно-конструкторском этапе, так и на этапе апробации и тестирования), целенаправленно, с учетом уже имеющихся опыта и наработок провести подбор организаций и групп специалистов, подготовить скоординированную программу действий (проекты), определиться с источником финансирования и приступить к реализации программы.

То, что такие организации, специалисты, полигоны есть, существует опыт и целый ряд наработок в этой области, сомнения не вызывает. Примеров, связанных с реализацией тех или иных средств программно-технического уровня, можно приводить много. Коротко остановимся на каждом из программно-технических сервисов с комментариями по проблемам, которые существуют и могут быть примерами того, что сделано (нам это легче делать на опыте сети MSUNet Московского университета) и что следовало бы по каждому сервису сделать, на наш взгляд, в ближайшее время.

Идентификация и аутентификация – первый и основной рубеж обеспечения безопасности на программно-техническом уровне, так как остальные сервисы этого уровня, как правило, работают с поименованными субъектами. Идентификация позволяет субъекту (пользователю, процессу, устройству и т. п.) назвать себя, аутентификация – подтвердить свою подлинность. Подлинность может быть доказана путем предъявления одной из следующих сущностей:

– того, что субъект знает (например, пароля);
– того, чем субъект владеет (например, магнитной карточки);
– того, что является неотъемлемой частью субъекта (например, образца голоса).

Основные принципы построения системы аутентификации:

– целостность,
– централизованность,
– гибкость,
– модульность.

В настоящее время существует достаточно много методов идентификации и аутентификации для различных вариантов и сред доступа, стойких ко многим видам атак. К основным проблемам на пути их внедрения следует отнести следующие:

– существующие методы и средства идентификации/аутентификации не составляют унифицированной (единой) системы, которая обеспечивала бы общие (не зависящие от отдельных приложений) механизмы её пополнения, использования и развития;
– объективно гетерогенная аппаратная база и программное обеспечение (в первую очередь ОС – операционная среда) в интернет-сетях усложняют создание унифицированной (хотя бы по подходам к созданию) системы идентификации/аутентификации.

Как первые шаги в этом направлении можно рассматривать результаты работ в рамках международного проекта PAM (Pluggable Authentication Modules – встраиваемы модули аутентификации [http://linux.kernel.org/pub/linux/libs/pam/index.html].Преимущества центрированной, модульной динамической схемы аутентификации были оценены, PAM получил широкое распространение, став частью ОС RedHat (Linux). Продолжением этих работ, направленным на устранение недостатков PAM, следует рассматривать работы над проектом PNIAM (Pluggable NonInteracive Authentication Modules [http:www.msu.ru/pniam/ pniam.html]

Управление доступом призвано задавать и контролировать выполнение правил, в соответствии с которыми субъекты (пользователи) обращаются к объектам (ресурсам, информации и др.). Логическое (в отличие от физического) управление доступом – это основной

механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, частично, их доступность. Это одна из самых сложных задач в области обеспечения информационной безопасности. Сложность её связана с большим количеством объектов, форм их представления (данные, гипертекст, мультимедиа) и, соответственно, видов доступа (ftp, telnet, http, …). Эти обстоятельства диктуют необходимость построения системы управления доступом не на уровне отдельных сообщений или документов, а на уровне информационных ресурсов.

В настоящее время в качестве математических моделей большинства систем управления доступом используются дискреционная и мандатная модели. Каждая из них имеет свои преимущества и недостатки (в рамках принятой политики безопасности), например, для усиления контроля конфиденциальности и целостности чаще используется мандатная модель. В некоторых случаях используется смещение корня файловой системы и ряд других методов.

Анализ преимуществ и недостатков различных моделей, систем и методов, их реализация для различных ОС, поиск элементов унификации систем управления доступом на гетерогенных средах составляют перечень важных взаимосвязанных задач.

Протоколирование и аудит – это сбор, накопление и анализ информации о событиях, происходящих в информационной системе с целью ее использования для сетевого менеджмента, оперативного реагирования на ситуации, которые приняты администрацией в качестве "нештатных" (нарушение информационной безопасности, отказ аппаратно-программных средств сетевой поддержки и т. п.[http://www.jetinfo.ru/1999/8/1/articlel.8.1999 .html]. Это один из самых важных и сложных для построения программно-технических механизмов обеспечения информационной безопасности. В качестве основных проблем на пути решения этой задачи можно отметить:

– сложность построения такой иерархической системы на гетерогенной среде при наличии большого числа коммуникационных узлов, что, как правило, присуще ведомственной или корпоративной сети;
– необходимость редукции большого числа параметров, характеризующих состояние реальной системы до ограниченного набора параметров, определяющих модель (адекватно описывающих поведение реальной системы);
– отсутствие вычислительных средств (аппаратно-программных), которые бы обеспечивали функциональность системы в реальном времени;
– необходимость построения математических моделей, характеризующих типичное сетевое поведение (профили, сигнатуры), а также нетипичные или заведомо злоумышленные действия;
– построение базы знаний, системы "on-line" анализа и автоматического (или хотя бы полуавтоматического, с участием оператора) реагирования.

В настоящее время имеется достаточно много источников протоколирования, от ОС до приложений, которые реализуются стандартным коммуникационным оборудованием. Для аудита используется сравнение с образцами атак, выявление нетипичного поведения (путём сравнения с образцами типичного). Однако пока ни одна из получивших распространение подобных систем не является ни удовлетворительно функциональной, ни эффективной. Причина тому – отсутствие решений для указанных выше проблем. Значительная часть из них носит математическую и программно-техническую направленность и с успехом может быть решена в России.

Криптография – один из основных инструментов обеспечения целостности и конфиденциальности информации. Основными методами являются симметричное (один и тот же ключ для шифрования и расшифровки информации) и асимметричное (один ключ открыт, общеизвестен для шифрования, второй – закрыт, доступен только одному для расшифровки). Достоинство симметричного метода – в наличии надежных и быстрых алгоритмов шифрования и дешифрования, но недостаток в широком распространении ключа. К недостаткам алгоритмов асимметричного метода шифрования относится низкое быстродействие сети при его реализации.

Наибольшее распространение в Интернет получили смешанные алгоритмы: сначала с помощью асимметричной криптографии генерируется общий секрет участников информационного обмена, затем этот общий секрет используется как ключ симметричного алгоритма. Для обеспечения целостности информации используется асимметричная криптография с хэшированием.

В целом, говоря об этом направлении деятельности, следует отметить успехи российских математиков в области создания теоретических основ и моделей криптографии. Необходим поиск подходов к созданию эффективных алгоритмов и программного обеспечения для сопровождения в Интернет приложений, критичных к нарушениям целостности и конфиденциальности.

Экранирование позволяет повысить доступность сервисов внутренней области (например, локальной сети организации), уменьшая нагрузку из внешней области (например, Интернет). Экранирование также уменьшает уязвимость внутренних сервисов безопасности, так как внешнему злоумышленнику первоначально нужно пройти сквозь экран.

Межсетевые экраны предназначены для разграничения доступа клиентов из одного множества информационных систем к серверам из другого. Как правило, задача формулируется несимметричным образом: одно множество является "внутренним" (например, локальная сеть организации), а другое – внешним (например, внешним сегментом Internet).

Межсетевой экран можно представить как последовательность фильтров. Каждый фильтр может не пропустить данные, сразу перекинуть данные на другую сторону или передать данные следующему фильтру. Экраны, как правило, работают на сетевом, транспортном или прикладном уровне модели OSI.

Работы по созданию эффективных межсетевых экранов имеют очень важное значение и ведутся, как правило, организациями, специализирующимися в этой области.

Литература

1. Васенин В. А.. Российские академические сети и Интернет (состояние, проблемы, решения) / Под ред. В. А. Садовничего. – М.: РЭФИА, 1997, 173 с.
2. Садовничий В. А., Васенин В. А., Мокроусов А. А., Тутубалин А. В.. Российский Интернет в цифрах и фактах. М.: Изд-во Московского университета, 1999, 148 с.
3. Системный проект Межведомственной программы «Создание национальной сети компьютерных телекоммуникаций для науки и высшей школы». М., 1996.
4. Бойко В. В., Васенин В. А., Платонов А. П.. Опорная инфраструктура национальной сети компьютерных телекоммуникаций для науки и высшей школы // «Телематика’96» Всеросс. научно-метод. конф.. Тезисы докл. 13 – 17 мая 1996 г.. С.-Петербург, с. 20 – 22.
5. Васенин В.А. Высокопроизводительные научно-образовательные сети России. Настоящее и будущее. - М:Изд-во Московского университета, 1999, 32с.
6. Бетелин В.Г., ГалатенкоВ.А. Информационная безопасность в России: опыт составления .карты. - Jet Info, N1(56)/1998.

7 Галатенко А.В. Активный аудит.-Jet Info, Информационный бюллетень, N8(75)/1999.