Российский Интернет и проблемы информационной безопасности

В.А.Васенин
доктор физ.-мат. наук, профессор
МГУ им. М.В.Ломоносова
Центр телекоммуникаций и технологий Интернет
Механико-математический факультет

Введение

Интернет как транснациональная сетевая инфраструктура является сегодня основной информационно-проводящей средой для хозяйственного комплекса и экономики многих государств мира [1,2]. Вместе с огромными достижениями феномен Интернет породил и целый ряд проблем законодательного, административного, технического и технологического характера, от разрешения которых во многом зависит социотехнологический фундамент будущего общества [2,3]. В таком или, как его называют Информационном Обществе, информация будет не только исходной посылкой, объектом, инструментом познания, но и одной из главных целей человеческой деятельности.

В настоящее время актуальной и важной для Интернет является проблема защищенности структур отдельных сетей в Интернет, их информационных ресурсов как от преднамеренных несанкционированных или противоправных действий, так и от действий незлоумышленных, в том числе и от природных явлений. Эта проблема ставит целый ряд новых задач. Настоящее сообщение посвящено обсуждению таких задач, изложению общих подходов к их решению, описанию механизмов и инструментальных средств, которые могут быть использованы или уже реализуются на практике.

Российский сегмент в мировом Интернет

Развитие Интернет как транснациональной сетевой инфраструктуры породило ряд очень сложных проблем. В начале 70-х, когда зарождалась протокольная база Интернет, трудно было предположить, что Сеть Сетей будет объединять 200 стран мира и более 100 млн сетевых компьютеров, продолжая столь же стремительно расширяться [3]. Многие из потребностей будущего не могли быть предусмотрены традиционным стеком интернет-протоколов. В силу этих причин на повестке дня сегодня остро стоят проблемы исчерпания адресного пространства, его мобильность, возможности маршрутизаторов предотвратить «тромбы» на магистральных каналах,
для того, чтобы обеспечить необходимые скорости обработки сетевых пакетов, проблемы качества передачи для мультимедиа-систем. Большие трудности связаны с реализацией механизмов информационной безопасности, защитой данных и сетевой инфраструктуры. Такая озабоченность не является праздной для Интернет, в котором сосредоточено огромное количество иинформации, в том числе конфиденциальной, доступ к которой является нарушением прав отдельной личности, организации или ведомства. Сегодня мы все чаще являемся свидетелями того, что сетевые технологии используются в преступных целях.

Эти и ряд других важных проблем – это вызов современным сетям, коммуникационным и информационным технологиям, которые они поддерживают. Под угрозой транснациональная сетевая инфраструктура, которая сегодня «де-факто» является кровеносной системой мировой экономики. Вместе с тем это новые цели и новое перспективное поле деятельности, в первую очередь, для науки и образования. В настоящее время активная работа в этом направлении проводится на исследовательских полигонах (HP–R&E networks – High Performance Research and Educational networks) многих стран мира [4]. Такие сети, поддерживающие технологии следующего поколения создаются на базе национальной сетевой среды (Abilene/Internet-2, vBNS, NREN (США), Super Janet (Англия), Renater (Франция) и объединяются в траснациональные образования (Nordunet, GEANT (Европа), APAN (Азия).

Аналогичные исследования в России ведутся с 1996 года в рамках Межведомст венной программы "Создание национальной сети компьютерных телекоммуникаций для науки и высшей школы. Вот только перечень отдельных направлений такой деятельности, где российские исследователи имеют практические результаты [2,5-7]:

- высокопроизводительные интегрированные информационные системы и сети;
- проблемы создания распределенных сетевых приложений на гетерогенной среде;
- информационная безопасность в открытых IP- сетях;
- сетевые мультимедиа системы в образовании и научных исследованиях;
- методология мониторинга крупных сетевых структур, в том числе основных параметров российского сегмента Интернет.

На основании результатов исследований по последнему из направлений приведу основные тенденции развития Интернет в России.

- На середину 2001 г. общее число сетевых компьютеров в российском сегменте Интернет превышает 500 тысяч, из них 70% поддерживают коммерческий, а 30% - научно-образовательный сектор.

- Российский Интернет обслуживает более 250 поставщиков сетевого сервиса (Internet Service Provider – ISP), зона действия которых покрывает всю территорию страны.

- Рост канальных емкостей в Глобальный Интернет с 1996 года идет экспоненциально.

- Темпы и тенденции развития опорно-транспортной среды в России соответствуют мировым. Хотя по-прежнему сохраняются диспропорции между центральными (Москва, Санкт-Петербург) и более удаленными регионами, а также между областными, районными центрами и особенно сельской местностью.

Сегодня с полным основанием можно констатировать, что российский сегмент Интернет стал одним из факторов, активно влияющих на национальный хозяйственный, промышленный, научно-технический комплекс, другие сферы деятельности и экономику страны в целом. Это обстоятельство является одной из главных причин, заставляющих обращать пристальное внимание на технологические вызовы, которые ставит Интернет перед обществом. В настоящее время такой полигон на технологиях нового поколения создается в России. Его основу составляет национальная высокопроизводительная исследовательская сеть, создаваемая с 1998 года в рамках российско-американского проекта Mirnet [4]. Замечу, что значительная часть крупных международных научных проектов, в том числе в области информатики и телематики выполняется в последние годы на инфраструктуре этой сети [2].

Таким образом, Интернет в России как на традиционной технологической базе, так и на новых технологиях, имеет в настоящее время все атрибуты аналогичных национальных сегментов других стран мира.

Информационная безопасность – проблема интернациональная.

Проникая во все сферы жизнедеятельности отдельных государств, способствуя объективно протекающим в мире процессам глобализации и интеграции, Интернет становится тем феноменом (управляющим рычагом), который позволяет не только регулировать, но и влиять на общемировые тенденции. Следует отметить, что глобализация не всегда приносит мировому сообществу желаемые результаты. Вместе с положительными тенденциями в научно-технической, промышленной и бизнес сферах, мы наблюдаем целый ряд негативных последствий.

Становление Интернет связано с появлением новой транснациональной по своей природе технологической среды для массового информирования. В отличие от традиционных радио и телевидения, не имея пока столь внушительной абонентской аудитории, Интернет имеет целый ряд преимуществ. Они связаны с возможностью эффективной интеграции аудио и видео, в том числе на мобильной основе, без необходимости иметь для этого специально выделенные транспортные сети, потенциально неограниченный круг технических возможностей и интернациональную пользовательскую аудиторию. Однако существующие и в традиционных СМИ проблемы контроля со стороны общества за содержанием представляемых материалов в данном случае существенно усложняются. Сегодня мы являемся свидетелями того, как информация в Интернет используется для пропаганды извращенной морали и нравственности, отчуждения духовных ценностей. Через Интернет деформируется самобытность отдельных наций и народностей. Эффективных способов воздействия на эти негативные проявления пока, к сожалению, не найдено.

Беспрецедентно быстрые темпы развития Интернет привели к тому, что информационные ресурсы Сети, которые накоплены годами в настоящее время представляют собой необозримое, плохоупорядоченное (с точки зрения технологической) поле, поиск (того, что необходимо в данный момент) и эффективное манипулирование с данными на котором крайне затруднены. Заметим, что это не только проблема информационных ресурсов в глобальном или национальном, но даже и ведомственном, корпоративном масштабе. Об этом свидетельствуют многочисленные исследования и практические результаты последних лет в области создания методологии, механизмов и инструментальных средств интеграции информационных ресурсов. Изложенное обстоятельство позволяет, и не без определенной доли истины, некоторым «скептикам» называть Интернет «всемирной помойкой».

Перечень таких негативных тенденций можно продолжить, однако в качестве одной из важнейших следует выделить проблему, связанную с защитой сетевой инфраструктуры и ее информационно-вычислительных ресурсов. Возможность через деструктивные воздействия в сети влиять на хозяйственно-экономические комплексы национального масштаба, ее обороноспособность, делает Интернет не только полем потенциальных правонарушений криминального (уголовного) характера, но и террористических действий. К сожалению, средств и систем защиты, адекватных сути

этих проблем, включая законодательный, административный, операционный или программно-технический уровни их реализации, в мире пока не создано.

Эта проблема не является проблемой отдельной страны или группы стран. Традиционный стереотип об информационной безопасности, как направлении, ориентированном на сугубо «закрытые» задачи национальных силовых ведомств, должен уступить место другим, более приемлемым в современном киберпространстве тенденциям, обусловленным необходимостью совместных действий в целях устранения общих угроз. Примеры таких подходов в мире сегодня существуют. Они направлены на предотвращение распространения и применения оружия массового уничтожения, экологических катастроф, терроризма и т.п.

Эффективные подходы и адекватные механизмы разрешения задач, связанных с созданием систем информационной безопасности, могут быть найдены и практически реализованы только во взаимодействии ученых, специалистов разных сфер деятельности (техники и юристы, психологи и экономисты, политологи и др.) из разных стран мира.

Проблемы, задачи и направления решения.

Информационная безопасность – понятие очень широкое, которое можно отнести к любому виду информации как таковой, ее носителям, средствам передачи и т.п. Здесь и далее рассматривается информационная безопасность в среде компьютерных телекоммуникаций, и даже, более узко, - в Интернет, представляющем собой совокупность сетей и поддерживаемых ими информационно-вычислительных ресурсов, взаимодействие которых осуществляется на основе стека протоколов TCP/IP. В самом общем случае информационную безопасность (ИБ) в таком понимании можно рассматривать как защищенность информации и поддерживающей ее инфраструктуры (транспортная среда, аппаратные средства и программное обеспечение) от внутренних возникающих внутри отдельной сети или структуры, поддерживающей ее или внешних угроз, обусловленных преднамеренными или случайными воздействиями.

Уже само определение информационной безопасности указывает на многоаспектный характер проблемы, которая характеризуется различными категориями субъектов, вступающих в информационные отношения. Например, это объекты с различными требованиями к защите своих ресурсов (режимное учреждение, коммерческая структура, академическая организация), различные категории субъектов (конечный пользователь, техническое средство, природное явление), которые потенциально представляют угрозу для ресурсов, подлежащих защите, и категории действий (злоумышленные действия или случайная неисправность), а также различные типы угроз.

В отличии от традиционных задач, которые ставит проблема ИБ на изолированных локальных и небольших ведомственных или закрытых корпоративных сетях, задачи в открытых интернет – сетях имеют свою специфику. В таких сетях потенциальный доступ к ресурсам (даже при наличии систем защиты и дифференцированного доступа к ресурсам) может иметь в любое время, любой пользователь из любой точки земного шара. Традиционные административные и операционные рычаги управления доступом и контроля использования ресурсов в таких сетях становятся не столь эффективны, и на первый план выходят программно-технические регуляторы.

Проблемы идентификации пользователей и разграничения доступа к ресурсам в соответствии с принятым в той или иной сети регламентом (политикой), а также своевременную реакцию на нештатные ситуации берут на себя аппаратно-программные средства.

Другой особенностью реализации ИБ в Интернет является то обстоятельство, что обновление программного обеспечения, технологий преодоления систем ИБ идет очень быстро. Новые методы атак (с помощью того же Интернет) появляются почти ежемесячно и разработчикам средств и систем защиты, администраторам ИБ, необходимо принимать адекватные меры. Для этого требуется, во-первых, их высокая квалификация, во-вторых, высокая квалификация разработчиков системного и сетевого программного обеспечения, а в-третьих, относительно высокая квалификация как владельцев, так и пользователей сетевых и информационно-вычислительных ресурсов. К сожалению, степень реализации этой задачи пока оставляет желать лучшего.

Не останавливаясь на более детальном анализе к числу макропроблем безопасности сетевых и информационных ресурсов в Интернет можно отнести

- изначально слабые ресурсы стека TCP/IP (v.4) для реализации механизмов ИБ;
- ошибки разработки и реализации аппаратно-программных средств в действующих системах ИБ;
- отсутствие математических моделей угроз безпасности и отдельных функционально важных подсистем (аутентификация, управление доступом и др.), составляющих систему ИБ типовой сети, позволяющих адекватно описать предметную область и строго оценить надежность такой системы;
- отставание уровня и темпов разработки и внедрения систем ИБ от уровня и темпов развития Интернет;

- недостаточное внимание к проблемам ИБ при разработке и реализации программных продуктов (как системных, так и общецелевых, прикладных) для их использования на сетях;
- незнание или пренебрежение пользователями основными принципами ИБ.

При формировании политики ИБ принято выделять следующие типы угроз:

- угроза конфиденциальности информации (защита от несанкционированного просмотра);
- угроза целостности информации (актуальность, непротиворечивость информации, защита от разрушения и несанкционированного изменения);
- - угроза доступности информации (возможность получить информацию за приемлемое время).

Основными составляющими деятельности при обеспечении информационной безопасности являются

- деятельность, направленная на ликвидацию возможностей осуществить атаку и, тем самым, на предотвращение ущерба; принятие мер по сокращению возможного ущерба (путем уменьшения объема информации и ресурсов, доступных злоумышленнику в случае успешной атаки; сокращения времени восстановления систем после атаки; раннего обнаружения факта атаки на систему);

- принятие мер, способствующих обнаружению злоумышленника после атаки.

Порядок перечисленных выше направлений деятельности отражает их важность для защиты интересов пользователей и сокращения ущерба от деятельности злоумышленников.

Многогранный характер самой задачи обеспечения информационной безопасности определяет несколько направлений (или уровней), скоординированные действия на каждом из которых в состоянии обеспечить ее комплексное решение. К таким уровням принято относить законодательный, административный, оперативный и программно-технический [8].

Законодательный, административный и операционный уровни (механизмы решения)

Законодательный уровень является базовым для создания стройной системы мер, обеспечивающих ИБ на всех остальных уровнях, так как определяет

- меры прямого законодательного действия, позволяющие квалифицировать нарушения и нарушителей, формирующие в обществе отрицательное отношение к нарушителям ИБ;

- меры направляющие и координирующие, способствующие разработке и распространению средств обеспечения ИБ, повышению образования в этой области;

Если говорить о России, то к первой группе мер можно отнести главу 28 «Преступления в сфере компьютерной информации» раздела IX новой редакции УК РФ, закон «Об информации, информатизации и защите информации» а также ряд других законов, которые находятся в стадии разработки («О праве на информацию», «О коммерческой тайне», «О персональных данных», «Об электронной цифровой подписи»).

Ко второй группе законодательных и нормативных актов относятся документы, регламентирующие процессы лицензирования и сертификации в области ИБ (ФАПСИ и Гостехкомиссия при президенте РФ), нормативные документы ведомств (руководящие документы Гостехкомиссии по требованиям к классам защищенности СВТ и АС, по межсетевым экранам и др.).

Однако необходимо отметить, что это пока только первые шаги в области приведения этого уровня в соответствие с требованиями сегодняшнего состояния Интернет и его ролью в государстве и обществе. Эти вопросы неоднократно обсуждались в Московском университете на "Круглом столе", посвященном проблемам информационной безопасности. Такой постоянно действующий "Круглый стол" организован по инициативе МГУ им. М.В.Ломоносова и поддержан Советом Безопасности России. Он активно работает уже более года, в его заседаниях участвуют ученые, технические специалисты разных научных направлений естественного и гуманитарного циклов.

Следует обратить внимание на важность согласованности этих мер с международной практикой и необходимость приведения российских стандартов и сертификационных нормативов в соответствие с международным уровнем информационных технологий. К числу важных на этом направлении следует отнести

вопрос о гармонизации российских стандартов в области ИБ с международными стандартами на основе спецификаций ISO 15408 («Общие критерии» [8]). Всесторонний анализ и принятие этих общеевропейских стандартов в качестве основы для разработки требований к системам обеспечения информационной безопасности в России могло бы стать заметным шагом на пути интеграции нашей страны в мировое информационное пространство на основе Окинанавской хартии 2000 г.

Политика безопасности представляет собой систему мер, предпринимаемых руководством организации или поддерживаемой ею сети на административном уровне. Эта система мер представляет собой совокупность документированных управленческих решений, направленных на

защиту как информации, так и поддерживающей ее сетевой инфраструктуры. Политика безопасности определяет стратегию организации в этой области и строится на основе анализа рисков, которые систематизируются и признаются реальными для информационной системы организации (или сети).

Осуществление политики безопасности можно разделить на две группы: меры верхнего и нижнего уровня. На верхнем уровне осуществляется управление рисками, координация деятельности, стратегическое планирование и контроль выполнения мероприятий в области информационной безопасности. На нижнем уровне происходит контроль реализации конкретных сервисов безопасности.

Административный уровень или уровень разработки и контроля соблюдения положений политики безопасности – это очень важный уровень, согласованные действия на котором позволяют унифицировать подходы, действия конкретных исполнителей по предотвращению, обнаружению, своевременному пересечению нарушений ИБ, в частности, уменьшению (минимизации) ущерба от них.

Опираясь на собственный опыт поставщика сетевого сервиса на российском сегменте Интернет, хотел бы обратить внимание на ряд проблем, присущих этому уровню. К сожалению, несмотря на имеющиеся (хотя и слишком общие) стандарты, которые существуют для разработки политики безопасности, в практическом плане большинство организаций, имеющих достаточно большие IP-сети, этих стандартов не придерживается. Более того, законодательный уровень не содержит материалов, стимулирующих деятельность на нижележащем административном уровне (обязывающих вести эту работу). Отсутствуют типовые стандарты на этот счет для различных организаций (сетей) с учетом специфики решаемых задач. Так, в научно-образовательных сетях обеспечение доступности информации, как правило, является приоритетной задачей, а обеспечение целостности и конфиденциальности – задачей второго уровня значимости. Другое распределение по приоритетам защиты от угроз информационной безопасности в сетях коммерческих структур, а тем более в сетях режимных государственных учреждений.

Создание дифференцированного перечня моделей угроз безопасности сетевых инфраструктур организаций с различными политиками безопасности, в том числе на основе строгих математических моделей, является одной из перспективных задач на этом уровне.

Операционный уровень - один из важнейших при реализации политики безопасности в любой компьютерной системе. Операционные регуляторы ориентированы прежде всего на людей, а не на технические средства. Они призваны сократить ущерб от деструктивных действий в первую очередь «изнутри», со стороны персонала или лиц, имеющих доступ к ресурсам, управляющим сетью, делегирующих или контролирующих делегирование тех или иных полномочий.

В качестве основных можно рассматривать следующие операционные меры:

- управление персоналом;
- физическое управление доступом и минимизация привилегий;
- поддержание работоспособности и восстановления сети или сетевых ресурсов после сбоев.

Однако практическая реализация перечисленных мер операционного уровня на сетях российского сегмента Интернет также вызывает ряд трудностей. Управление персоналом, например, наталкивается на отсутствие четких должностных инструкций и недостаток квалификации у специалистов, призванных осуществлять такое управление. По незнанию можно совершить ошибку, чреватую серьезными последствиями, например, получить «троянскую» программу, сказать пароль неавторизованному лицу, и т.п. Чтобы избежать подобных ошибок, нужно о них знать.

Применение мер физического управления доступом в рамках сети большой организации сложно реализуемо. Тем не менее, применение таких регуляторов к ряду ключевых узлов является необходимой мерой. Заблаговременная проработка вопросов реакции на нарушения режима информационной безопасности сети – в значительной степени связана с решением задач резервного копирования и восстановления сетевых ресурсов после сбоя.

Поддержание работоспособности и восстановление системы после сбоев остается узким местом даже для крупных российских ISP по причине отсутствия четкости в организации взаимодействия с канальными операторами, неукомплектованности штатным персоналом, отсутствия среднего звена специалистов надлежащей квалификации и еще целым рядом проблем. Реакция на нарушение режима безопасности вызывает трудности, как правило, из-за отсутствия какого-либо регламента взаимодействия ISP не только с государственными ведомствами, причастными к информационной безопасности (ФАПСИ, Гостехкомиссия, УВД и др.), но и с другими ISP, у которых может и не быть людей, которые такое взаимодействие обеспечивают. Сложившееся положение дел можно объяснить начальным этапом в развитии относительно молодого российского сегмента Интернет. Необходим поиск подходов к устранению отмеченных недостатков в каждой из сетей, представляющих отдельные организации.

Административные и операционные меры обеспечения информационной безопасности, например, существенно зависят от структуры организации и специфики решаемых задач, поэтому выработка общих рекомендаций в данных областях крайне затруднена. Однако работа в этом направлении проводится. В Центре телекоммуникаций и технологий Интернет Московского университета, напрмер, существует рабочая группа, в задачи которой входит создание методологии защиты открытых научно-образовательных сетей. В рамках этой деятельности затрагиваются и административные, и операционные регуляторы.

Программно-технический уровень (механизмы решения)

Интернет представляет собой совокупность взаимодействующих между собой отдельных сетей: от самых мелких – локальных – до крупных корпоративных сетей, национального или даже транснационального масштаба. Именно эту задачу межсетевого взаимодействия решает стек протоколов TCP/IP, и это обстоятельство стало одной из главных причин беспрецедентно быстрого развития и популярности Интернет. Каждая из этих сетей имеет (или должна иметь) собственную политику безопасности, исходя из которой она применяет свои операционные регуляторы и использует необходимые для этого программно-технические средства. Ключевыми в иерархии сетевых инфраструктур являются крупные ведомственные или корпоративные сети. Именно они, как правило, являются главными объектами потенциальных атак.

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

- экранирования, предназначенные для регулирования потоков между внутренней и внешней частью сети на различных (сетевом, транспортном и прикладном) уровнях модели открытых систем, включая средства протоколирования потоков;
- 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);
- криптографической защиты, в том числе, вспомогательные для других регуляторов, например, аутентификации;
- управления доступом (логическим), позволяющие специфицировать и контролировать действия, которые субъекты могут выполнять под объектами, включая квотирование ресурсов как частный случай;
- протоколирования и аудита, обеспечивающие мониторинг сети на всех уровнях, выявляющие подозрительную активность и реализующие оперативное реагирование;
- централизованного администрирования сети.

Совокупность этих средств призвана в значительной степени покрыть потребности защиты корпоративной IP-сети на программно-техническом уровне. Кратко остановимся на некоторых проблемах их реализации.

К перспективным системам экранирования следует отнести многокомпонентные комплексы, включающие экранирующие маршрутизаторы, экраны транспортного уровня и шлюзы. Их взаимодействие позволит не только обеспечить эффективное функционирование данного вида сервиса, но и собрать информацию, важную для других программно-технических регуляторов.

Исследования, связанные с идентификацией аутентификацией в Интернет, направлены на создание механизмов, обеспечивающих их централизацию, целостность и гибкость, портабельность хотя бы на ограниченный набор «надежных» ОС.

Перспективы логического управления доступом в значительной степени могут быть обеспечены переходом на более эффективные схемы и модели как произвольного, так и принудительного управления [9], включая решение проблемы квотирования ресурсов, как частный случай, в расчете на предотвращение атаки на доступность (отказа в предоставлении сервиса).

Здесь хотелось бы обратить внимание на необходимость и важность поиска подходов к созданию математически строгих моделей, позволяющих описывать (и строить) монитор безопасности (обращений) с учетом не только современных представлений о таких моделях, но и в расчете на возможность их использования для получения надежных оценок степени безопасности (надежности) системы на основе современных критериев. Пока можно констатировать только подходы к созданию таких систем [10].

Криптографические механизмы в Интернет призваны обеспечить защиту сетевых ресурсов от всех видов угроз, не только традиционные конфиденциальность и целостность данных, но и защиту от отказа в предоставлении сервиса. Перспективы здесь связаны с объединением преимуществ высокого быстродействия при реализации алгоритмов симметричного шифрования с эффективностью

асимметричных методов для различных прикладных сервисов и (или) программно-технических регуляторов.

Активный аудит – один из самых сложных, но важных и необходимых регуляторов на программно-техническом уровне. Существующие на сегодня комплексы своих функций в полном объеме не выполняют. Будущее на этом направлении определяется необходимостью решения целого ряда научных, технических и технологических задач, оно связано с поиском новых архитектурных решений, использованием перспективных математических моделей [9,11].

В заключение необходимо отметить, что динамика развития российского сегмента Интернет на ближайшие годы во многом будет определяться решением как перечисленных выше, так и целого ряда других задач, направленных на защиту информационных ресурсов и сетевой инфраструктуры. Учитывая всю важность проблемы и последствий ее разрешения для будущего страны, разработка государственной политики, подкрепленной системой практических мер в этой области, должна стать одним из приоритетов государства.

Литература

1. Крол Э.. Всё об Internet: Пер. с англ. – К.: Торгово-издательское бюро BHV, 1995. 592с.
2. Васенин В.А. Internet: от настоящего к будущему. - "Открытые системы", N12, 2000, с.36-44.
3. Кан Р. Е.. Эволюция сети Интернет. Всемирный доклад ЮНЕСКО по коммуникациям и информации. 1999 – 2000 гг., «Бизнес–Пресс», М.: 2000 г.
4. Васенин В.А. Высокопроизводительные научно-образовательные сети России. Настоящее и будущее.М: Изд-воМоск.ун-та, 1999,32 с.
5. Васенин В. А.. Российские академические сети и Интернет (состояние, проблемы, решения) / Под ред. В. А. Садовничего. – М.: РЭФИА, 1997, 173 с.
6. 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.
7. Васенин В.А., Галатенко А.В. О проблемах информационной безопасности в сети Интернет. Материалы круглого стола. "Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества (МГУ, октябрь 2000 г.)/ Под ред.проф.В.И.Добренькова.-М.:Изд-во Моск.ун-та, 20001, с.199-214.
8. Галатенко В.А. Информационная безопасность: практический подход. М.: Изд-во "Наука", 1998 г., 301 с.
9. Галатенко А.В. Об автоматной модели защищенных компьютерных систем. - "Интеллектуальные системы", т.4, вып.3-4, 1999г., Москва, с.263-270.
10. Кривонос Ф. В. О подходе к обоснованию корректности проектирования монитора безопасности.
11. Галатенко А. В. Активный аудит. – Jet Info, информационный бюллетень, №8 (75)/1999.
12. Корнеев В. В. Мониторинг угроз компьютерного нападения на информационно-телекоммуникационные системы.
13. Бетелин В. Б., Галатенко В. А. Информационная (компьютерная) безопасность с точки зрения технологии программирования.