Информационная безопасность критически важных объектов

Васенин В. А.

Институт проблем информационной безопасности МГУ им. М. В. Ломоносова

1. Введение

Проблема обеспечения безопасности информации, технологий её обработки, средств и систем, как их носителей возникла задолго до появления электроники в её современном понимании. Передача информации в виде сведений всегда связана с её предварительным преобразованием в сообщение (обработкой), которое отчуждается от её источника, а, следовательно, может быть подвергнуто деструктивному воздействию. Такими могут быть как действия злоумышленника, так и другие причины, например, влияние со стороны среды окружения. Сообщение, зашифрованное с помощью желзла в виде кода Сцитала и передаваемое адресату в V веке до нашей эры, могло быть не только перехвачено и дешифровано злоумышленником, с помощью такого же жезла. В силу природных явлений или каких-либо иных причин мог быть поврежден или утрачен сам жезл.

С появлением электроники, средств вычислительной техники и систем телекоммуникаций вопросы защиты данных, информационных технологий, реализующих их средств и систем информатизации стали ещё более актуальны. Для относительно низкоскоростных сетей связи с коммутацией каналов, которые преобладали до середины 1980-х годов, определяющую роль в вопросах обеспечения информационной безопасности играли средства обеспечения конфиденциальности и целостности данных на основе методов криптографии. Заключительная четверть прошедшего столетия была ознаменована созданием и активным внедрением технологий передачи данных на основе пакетных коммуникаций. Развитие таких технологий, создание метасети Интернет на основе стека протоколов TCP/IP, её активное внедрение во все сферы человеческой деятельности, с одной стороны, сделано ещё более актуальной и обострило проблему информационной безопасности ресурсов, которые поддерживаются с помощью новых коммуникационных технологий, с другой – существенно усложнило её разрешение [1]. В связи с отмеченным обстоятельством особую важность приобретают вопросы защиты от деструктивных информационных воздействий больших и сложно организованных, значимых с позиций национальной безопасности объектов. В мировой практике такие объекты принято именовать критически важными.

Отправным мотивом и целью настоящей публикации является желание автора обратить внимание на существующие на этом пути задачи, отметить объективно существующие сложности, известные ему, и прошедшие предварительную апробацию подходы к их разрешению.

2. Безопасность информационных технологий и защита критически важных объектов

Сверхбыстрые темпы развития инфо-телекоммуникаций в последние 25 лет намного опережают темпы создания и совершенствования (обновления) отвечающих современным потребностям общества технологий, средств и систем защиты ресурсов, которые с их помощью поддерживаются. С учетом появления новых угроз, обусловленных использованием современных информационных технологий, таких как киберпреступность, кибервойны, кибертерроризм, последнее обстоятельство с полным основанием можно отнести к числу чрезвычайных. Оно не только влияет, но и во многом определяет состояние национальной безопасности отдельных государств мира, вопросы безопасности на транснациональном уровне.

Содержание традиционной системы мер и действий, направленных на обеспечение безопасности объекта от деструктивных информационных воздействий, зависит от целого ряда обстоятельств (факторов). К их числу относятся: назначение; свойства объекта и его среды окружения; активы, подлежащие защите; угрозы, которым они могут быть подвержены, и возникающие при этом риски; отношение администрирующей объект организации к предоставлению (использованию) активов и цели обеспечения их безопасности. В результате изучения, систематизации и формализации перечисленных факторов формируются требования к средствам обеспечения безопасности подконтрольного объекта как основа для программы практических действий на этом направлении.

Отмеченная выше система мер, направленных на обеспечение информационной безопасности объекта защиты, связана с решением целого ряда высокотехнологичных задач, предполагающих, как правило, использование современного математического аппарата, знание «тонких» архитектурно-технологических особенностей средств вычислительной техники и телекоммуникаций, наличие навыков программирования, в первую очередь – системного. Её выполнение требует значительных ресурсозатрат, которые иногда соизмеримы с затратами на создание самого объекта.

Принимая во внимание изложенные выше обстоятельства, решение о создании системы обеспечения информационной безопасности объекта информатизации и определение её целей должно приниматься коллегией экспертов на основе анализа результатов предварительных (предпроектных) исследований. Основой для такого решения может быть определение категории анализируемого объекта в перечне (системе) уровней значимости объектов [2, 3] национальной информационно-

телекоммуникационной инфраструктуры (НИТИ). Самые общие подходы к подобной классификации информационных активов как объектов защиты от деструктивных воздействий диктуют правовые [4] и нормативно-регламентирующие документы, которые делят их на открытые и с ограниченным доступом, в том числе персональные данные, служебная тайна, секретные и государственная тайна. Аналогичные подходы к категорированию можно применить и в отношении классов объектов другой природы, например, к средствам вычислительной техники (СВ), к коммуникационному оборудованию, к автоматизированным системам (АС) [5, 6].

Отправным моментом в подходах к определению категории объектов НИТИ (в плане требований по их защите) выступает уровень (масштаб) ущерба, который может быть нанесен связанному с ним субъекту. В качестве такого субъекта может выступать отдельное физическое (персона) или юридическое лицо, элемент инфраструктуры, поддерживающий ту или иную сферу общественных отношений (материальную, политическую, духовную, социальную, информационную) в стране. Принимая во внимание декларируемое в Конституции Российской Федерации равенство и взаимообусловленность (гармонию) интересов личности, общества и государства, приоритет в этой иерархии интересов отдается национальным интересам, аккумулирующим в себе интересы отдельных граждан и общества в целом.

Главенствующую роль в перечне национальных интересов играет национальная безопасность в целом и информационная безопасность государства, как одна из её составляющих. Не останавливаясь на деталях её описания, которые подробно и систематизировано изложены в Доктрине информационной безопасности [7], отметим, что ключевое место в поддержании информационной безопасности страны играют системы, автоматизирующие технологические процессы, поддерживающие функционирование объектов, критически важных для государства инфраструктур по их назначению. Подобные системы, составляющие их средства вычислительной техники и телекоммуникаций, будем именовать критически важными объектами НИТИ.

К числу критически важных объектов (КВО) в контексте настоящей публикации относится объект, который в случае частичной деградации или полной потери функциональности способен прямо и в течение относительно короткого интервала времени влиять на состояние национальной безопасности, тех или иных её составляющих, например, управление энергоресурсами (атомными и гидроресурсами), оборонными системами, критическими производствами, транспортными потоками (железнодорожными, авиационными), информационными потоками государственных систем, поддерживающих межведомственное взаимодействие и другими, подобными им.

Принимая во внимание изложенные выше соображения, в качестве объектов, информационная безопасность которых является высшим приоритетом государства, рассматриваются КВО НИТИ.

3. Методология оценки уровня информационной безопасности критически важных объектов

Степень защищенности критически важных объектов от деструктивных информационных воздействий во многом определяется уровнем защищенности информационно-вычислительных и телекоммуникационных средств, составляющих системы, которые обеспечивают автоматизацию процессов управления такими объектами. Подобные системы, как уже отмечалось выше, сами являются критически важными объектами НИТИ. Именно они подлежат анализу при решении вопроса об оценке уровня защищенности КВО.

С позиции классических подходов уровень информационной безопасности подконтрольного объекта на разных этапах его жизненного цикла может оцениваться с использованием:

- аналитических математических моделей или путем имитационного моделирования;
- положений нормативных документов, стандартов и руководящих документов ФСТЭК (Федеральной службы технического и экспортного контроля) России;
- систематизированных согласно заранее разработанного регламента (схемы) тестовых испытаний.

Разработка **математических моделей** систем управления КВО, **доказывающих их гарантированную защищенность**, сталкивается с трудностями описания механизмов управления доступом к ресурсам таких систем. Трудности такого описания, в первую очередь, обусловлены, во-первых, многообразием механизмов управления доступом, включая сервисы идентификации (аутентификации, фильтрации, модели логического разграничения доступа, шифрования и другие), которые используются в комплексе средств защиты объекта. Обеспечивать учет и эффективное описание даже базовых из числа отмеченных особенностей подконтрольной системы в рамках одной аналитической модели, как правило, не представляется возможным. Тем не менее, это один из самых надежных способов построения систем с высоким уровнем доверия. Представляет безусловный интерес разработка подобных моделей для отдельных элементов сложно организованной системы обеспечения безопасности, поиск механизмов их взаимодействия в рамках единой большой модели.

В меньшей степени перечисленным выше трудностям подвержены подходы к анализу защищенности с использованием **методов имитационного моделирования**. К настоящему времени накоплен богатый опыт такого моделирования (например, [8, 9]) инструментальных средств разработки и реализации моделей применительно к сложным сетевым структурам и многопроцессорным вычислительным комплексам, на основе которых формируются КВО НИТИ. Однако адекватный учет

процессов информационного противоборства, возникающих в такого сорта объектах, может быть основан только на адекватных моделях атак, в том числе – многоагентных, распределенных на сетевой среде, расчитанных на отказ в обслуживании (Destributed Denial of Service DDoS), а также на моделях средств и систем защиты, противодействующих им. Их реализация не только сложна в плане построения формальных моделей, но и требует очень больших вычислительных ресурсов. Исследования и результаты на этом направлении представляют большой интерес.

Одним из важнейших факторов, способствующих совершенствованию практической деятельности в сфере обеспечения информационной безопасности любого государства, является эффективное **использование** сложившейся в мире и апробированной **системы стандартов и нормативно-регламентирующих** такую деятельность **документов**. Свидетельством осознания важности таких действий является широкое обсуждение в среде специалистов, и как результат – принятие в Российской Федерации в качестве рекомендаций ряда международных стандартов для их использования на этапах разработки, сопровождения и развития продуктов информационных технологий. Наиболее важными их них в контексте предметной области, которая рассматривается в настоящем издании, являются: ГОСТ Р ИСО/МЭК 15408–1,2,3–2002 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»; ГОСТ Р ИСО/МЭК 13335–1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»; ГОСТ Р ИСО/МЭК 17799–2005 «Информационные технологии. Практические правила управления информационной безопасностью».

К другим российским нормативно-регламентирующим документам, которые призваны регулировать аналогичную деятельность в Российской Федерации, в первую очередь относятся следующие:

1) специальные требования и рекомендации по технической защите сведений, составляющих государственную тайну (СТР);
2) специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);
3) ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
4) ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»;
5) ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»;
6) Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
7) руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения»;
8) руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
9) руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
10) руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации»;
11) руководящий документ «Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

Стандарты ГОСТ Р ИСО/МЭК 17799–2005, ГОСТ Р ИСО/МЭК 13335–1–2006, СТР, СТР-К и подобные им задают общие подходы к формированию политики безопасного использования ресурсов объектов, подлежащих защите, к оценке уровня их защищенности и рисков реализации деструктивных воздействий против них. Вместе с тем, положения этих стандартов в большей степени ориентированы на достаточно простые с архитектурно-технологических и организационно-административных позиций объекты. Группа мер обеспечения безопасности таких объектов на каждом из уровней комплексного подхода к ее реализации может быть определена в рамках требований одной организации, обслуживающей данный объект. В действительности КВО НИТИ, как правило, обслуживается несколькими взаимодействующими организациями, отношения которых к объекту в целом, к условиям использования отдельных его элементов и активов могут быть различны. Гармонизация таких отношений, унификация требований к обеспечению безопасности отдельных элементов КВО НИТИ с целью формирования единой политики информационной безопасности для объекта в целом – отдельная и очень важная задача. Способы ее решения в перечисленных выше документах не представлены. Некоторые подходы к ее решению и первые результаты в виде механизмов объединения моделей логического разграничения доступа к информационным активам в разных подсистемах сложно-организованного объекта, представлены в [10, 11].

Стандарт ГОСТ Р ИСО/МЭК 15408–2002 описывает систематизированный каталог требований к безопасности информационных технологий. Его положения определяют порядок и дают методиче-

ские рекомендации по его использованию при задании требований на стадиях разработки, сопровождения и развития, в ходе оценки и сертификации продуктов и систем информационных технологий с позиций их безопасности. Этот нормативный документ был принят в 2002 году. Он включает в себя требования, изложенные в целом ряде других аналогичных по назначению документов, разрабатываемых в разных странах мира ранее. В первой части данного документа определены основные понятия, используемые для описания и оценки таких систем (функциональные требования и требования доверия, профиль защиты, задание по безопасности и другие). Кроме того, в этой части приведены основные методические положения по оценке безопасности информационных технологий, включая реализующие их средства и системы, именуемые объектом оценки. Вторая часть документа содержит систематизированный набор функциональных требований безопасности к объекту оценки. Третья часть содержит описание требований доверия к безопасности такого объекта и описание оценочных уровней доверия к нему. Требования доверия включают меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем информационных технологий. В отмеченном контексте представляется целесообразным использовать положения стандарта ГОСТ Р ИСО/МЭК 15408–2002 для определения типовых угроз и требований безопасности функционирования для основных элементов, входящих в состав автоматизированных систем управления критически важными объектами. В качестве таких элементов могут, например, рассматриваться рабочие станции, оборудование для организации локальной вычислительной сети, аппаратно-программные средства для организации защищенных каналов, межсетевые экраны, прикладное программное обеспечение и ряд других. Предложения по решению задачи в такой постановке представлены и проиллюстрированы примерами в [12].

Вместе с тем, следует отметить, что существующие на этот счет, в том числе упомянутые выше, стандарты по ряду позиций не удовлетворяют современным требованиям, предъявляемым к сложным с точки зрения функциональности и в архитектурно-технологическом плане системам автоматизации и управления технологическими процессами, протекающими в объектах, подлежащих защите, в том числе тех, которые являются критически важными. В стандарте ГОСТ Р ИСО/МЭК 15408–2002, как и в Руководящих документах ФСТЭК России, рассматриваются вопросы обеспечения информационной безопасности с позиции обеспечения конфиденциальности и целостности информационных активов, защиты программного обеспечения от наличия недекларированных возможностей и в плане требований к определенным программно-техническим средствам защиты информации (например, межсетевым экранам). Следует, однако, отметить, что приведенным перечнем не исчерпывается весь список потенциально существующих, технически реализуемых с использованием современных информационных технологий угроз безопасности функционирования автоматизированных систем, в том числе и систем управления критически важными объектами. В настоящее время необходимо принимать во внимание классы угроз иного характера, наличие которых оказывает значительное влияние на состояние защищенности автоматизированной системы. К числу таких классов угроз можно отнести следующие:

- угрозы проведения распределенных атак на отказ в обслуживании;
- угрозы нарушения стойкости криптографических алгоритмов, активно используемых в том числе в подсистемах идентификации и аутентификации;
- угрозы реализации уязвимостей и недекларируемых возможностей другой природы при работе программного обеспечения;
- угрозы нарушения конфиденциальности при работе пользователя с сетевыми приложениями, например, распределенными базами данных, веб-браузерами.

В указанных выше нормативных документах отмечается необходимость проведения частичной верификации программного обеспечения, в том числе с использованием формальных методов. Реализация этих требований позволила бы устранить часть представленных выше угроз, однако вопросы их практической реализации не затрагиваются. Решению некоторых возникающих в связи с этим задач, основанных на верификации программного обеспечения с использованием формальных моделей, посвящены результаты, изложенные в [13-15]. Исследования на этом направлении имеют важное значения при разработке и внедрении программного обеспечения КВО НИТИ.

Отдельного внимания заслуживают методы и средства, направленные на предотвращение реализации угроз конфиденциальности и целостности данных. В плане защиты информационных активов больших и, как правило, распределенных на гетерогенной сетевой среде КВО, крайне важной является разработка механизмов, моделей и алгоритмов, использование которых позволило бы создать надежные криптографические протоколы, способные эффективно работать на скоростях, которые обеспечивают современные сети передачи данных.

Подходы, предлагаемые в ГОСТ Р ИСО/МЭК 15408–2002 [16–18] и в Руководящих документах ФСТЭК РФ [5, 6], позволяют в зависимости от области назначения анализируемого объекта, характера активов, подлежащих защите, угроз и отношения к ним со стороны сопровождающей объект организации, а также ряда других элементов среды окружения устанавливать цели безопасности и требования к средствам, которые обеспечивают их достижение. Таким образом поддерживается высокий уровень универсальности при установлении оценок безопасности информационных технологий, средств и систем, которые их реализуют, по сравнению с подходами, которые использовались

в других документах, предшествующих Руководящим документам ФСТЭК РФ и ГОСТ Р ИСО/МЭК 15408. Однако следует отметить, что наряду с этим достоинством одновременно снижается информативность оценки, так как при некотором изменении задач или условий окружения результаты оценки, в строгом понимании, теряют применимость. Анализ сложных с позиций функциональности и в архитектурно-технологическом плане систем автоматизации и управления технологическими процессами, протекающими в объектах, в том числе тех, которые являются критически важными, показывает, что данные системы следует рассматривать не в качестве типовых изделий, а как комплексы, функционирующие в перманентно изменяющихся условиях. Структура и набор компонентов в такой системе может меняться на протяжении ее жизненного цикла. В связи с изложенным актуальными являются: разработка моделей и алгоритмов, учитывающих перечисленные факторы; создание на их основе средств автоматизации процедур анализа состояния сложно организованного объекта на предмет его защищенности от деструктивных информационных воздействий.

Защищенность системы зависит не только от свойств механизмов обеспечения безопасности ее компонентов, но и в не меньшей степени от способов их объединения и средств, поддерживающих взаимодействие между ними. В связи с отмеченными обстоятельствами, необходимо построение некоторой модели более высокого уровня, задающей «мета-требования» по разработке требований безопасности к отдельным компонентам системы. В ходе исследований таких компонентов вполне можно ориентироваться на положения Руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [5]. Такие компоненты входят в сферу действия положений данного документа, что может позволить получить равномерную силу средств защиты, распределенных по структурным элементам большой системы. Такой подход учитывает особенности, присущие сложным распределенным информационно-телекоммуникационным комплексам. Вместе с тем, он позволяет использовать положительные стороны российских и международных стандартов.

Принимая во внимание изложенные выше соображения относительно стандартов и нормативно-регламентирующей базы безопасности информационных технологий с позиций их применения к КВО НИТИ, следует еще раз подчеркнуть высокую важность решения вытекающих отсюда задач.

Одним из подходов к оценке степени защищенности КВО НИТИ является их **тестирование**. Недостатком такого подхода применительно к технологически сложным объектам является отсутствие строгой математической основы регламентов проведения тестовых испытаний, средств их автоматизации и, как следствие отсутствие доказательной базы и низкая надежность получаемых результатов. В этой связи особую важность и значимость приобретает исследование подходов к тестированию больших аппаратно-программных комплексов, обслуживающих объекты подобные КВО НИТИ, на основе строгих формальных моделей. Исходные посылки для работ на этом направлении представляет методология тестирования на основе математических моделей, которая в 1980-1990–х годах начала складываться в ходе исследований, направленных на повышение эффективности коммуникационных протоколов стека TCP/IP. Эффективность таких моделей тестирования во многом определяется их четкой систематизацией, декомпозицией на взаимосвязанные компоненты, набор которых адекватно отражает свойства тестируемой системы.

4. Заключение

Эффективное решение практических задач в сфере защиты критически важных объектов от деструктивных информационных воздействий во многом зависит от обоснованности, адекватности требованиям времени поддерживающих такие системы технологий, аппаратно-программных средств и систем. Добиться этого можно только путем упреждающего проведения научных исследований как фундаментальных, так и прикладных. Решение практических задач противодействия проявлениям киберугроз объектам критически важных инфраструктур, в первую очередь, следует искать:

- на проведении фундаментальных и прикладных исследований, результаты которых обеспечат четкую систематизацию и формализацию базовых положений, идентифицирующих и классифицирующих объекты и субъекты деструктивных кибервоздействий, характеристики среды окружения, уровни организации защиты и меры противодействия на каждом из этих уровней, которые, в свою очередь, позволят создать основу для дальнейших эффективных исследований как теоретического, так и практического плана;
- на изучении и критическом анализе зарубежного опыта, на создании передовых по мировым стандартам технологий и инструментальных средств, способных обеспечить опережающие темпы решения новых задач по защите объектов критически важных инфраструктур, уязвимых в плане деструктивных кибервоздействий.

В качестве основных направлений научных исследований и опытно-конструкторских работ, позволяющих найти адекватные меры и средства противодействия проявлениям киберугроз критически важным объектам, должны рассматриваться следующие:

- Разработка и совершенствование основных положений, идентифицирующих киберпреступления, кибертерроризм и информационные войны, их объекты, субъекты и среду окружения, которые должны составить (сформиро-

вать) методологическую базу как для проведения исследований (систематизации и анализа фактов), так и для выполнения практических работ.

- Создание взаимоувязанного, систематизированного набора моделей и сценариев реализации компьютерных атак на объекты, потенциально уязвимые с точки зрения киберпреступлений, кибертерроризма и информационных войн, а также разработка и внедрение эффективного комплекса механизмов, моделей и сценариев организации противодействия подобным акциям.
- Подготовка предложений по системе мер и мероприятий на законодательном, административном и операционном уровнях реализации информационной безопасности, а также правовых и нормативных актов для эффективного противодействия проявлениям киберугроз.
- Реализация программно-технических средств, поддерживающих достаточно представительный и полный (покрывающий потенциальные проявления угроз) набор механизмов, моделей и сценариев противодействия кибератакам.

Литература

1. Васенин В.А. Проблемы математического, алгоритмического и программного обеспечения компьютерной безопасности в Интернет. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 23-24 октября 2003 г.- М.: МЦНМО, 2004.-с.11-143.
2. Васенин В.А. Научные проблемы противодействия терроризму. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 2-3 ноября 2005 г.- М.: МЦНМО, 2006, с. 49-63.
3. Климовский А.А., Большаков М.В., Пучков Ф.М. Объекты критически важных инфраструктур: анализ защищенности и риски успешной реализации компьютерных атак. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25-26 октября 2006 г., – М.: МЦНМО, 2007, с.315-333.
4. Стрельцов А.А. Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации. // Сборник «Научные и методологические проблемы информационной безопасности» под. ред. В.П. Шерстюка.- МГУ, 2004. – с. 67-83.
5. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ ФСТЭК от 30 марта 1992 года / ФСТЭК.- 1992.
6. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ ФСТЭК от 30 марта 1992 года / ФСТЭК. – 1992.
7. Доктрина информационной безопасности Российской Федерации. Электрон. текст. дан. – Режим доступа: http://www.scrf.gov.ru/documents/5.html, свободный. – Электрон. текст. док.
8. Котенко И.В., Уланов А.В. Программный полигон и эксперименты по исследованию противоборства агентов нападения и защиты в сети Интернет. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 2-3 ноября 2005 г.- М.: МЦНМО, 2006, с.78-91.
9. Батов И.С. К разработке средств имитационного моделирования для решения задач обеспечения безопасности информационных технологий. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 2-3 ноября 2005 г.- М.: МЦНМО, 2006, с.397-413.
10. Васенин В.А., Шапченко К.А., Андреев О.О. Математические модели и механизмы логического разграничения доступа в операционной системе Linux: текущее состояние и перспективы. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25-26 октября 2006 г., – М.: МЦНМО, 2007, с.495-507.
11. Шапченко К.А. К вопросу о средствах ОС Linux для управления доступом при использовании ролевых политик безопасности. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 2-3 ноября 2005 г.- М.: МЦНМО, 2006, с. 257-281.
12. Савкин В.Б. Профили защиты элементов критически важных объектов и меры по поддержанию доверия. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25-26 октября 2006 г., – М.: МЦНМО, 2007, с. 336-348.
13. Пучков Ф.М., Шапченко К.А., Андреев О.О. К созданию автоматизированных средств верификации программного кода. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25-26 октября 2006 г., – М.: МЦНМО, 2007, с.401-439.
14. Несов В.С., Маликов О.Р. Использование информации о линейных зависимостях для обнаружения уязвимостей в исходном коде программ // Труды ИСП РАН, № 9, с. 51-57, 2006.
15. Маликов О.Р. Исследование и разработка методики автоматического обнаружения уязвимостей в исходном коде программ на языке Си, диссертация на соискание ученой степени кандидата физико-математических наук, Московский государственный университет, факультет вычислительной математики и кибернетики, Москва, 2006.
16. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.- М.: ИПК Издательство стандартов, 2002.
17. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.- М.: ИПК Издательство стандартов, 2002.
18 ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.- М.: ИПК издательство стандартов, 2002.