Информационная безопасность и компьютерный терроризм

В. А. Васенин.

Статья из сборника "Научные и методологические проблемы информационной безопасности" (под ред. В. П. Шерстюка, М., МЦНМО, 2004 г.)

Введение

Терроризм, как выражение крайнего экстремизма, основанное на различного рода разногласиях (как национального, так и транснационального масштаба) в политике, экономике, на религиозной или криминальной почве, обсуждается и осуждается давно. При современном уровне развития высоких технологий расширяются возможности их использования для совершения террористических действий. Во многих странах сегодня ведется активная работа по анализу потенциальных возможностей подобных проявлений и выработке мер по борьбе с этим злом.

О понимании значимости, внимании к этой проблеме и попытках выработки такой системы мер на концептуально-теоретическом и практическом уровнях свидетельствуют, например, неоднократные обсуждения вопросов экстремизма на сетевой среде на межведомственном, междисциплинарном семинаре по научным проблемам информационной безопасности, проводимом в Московском университете под эгидой Совета Безопасности РФ и МГУ, доклады на российско-американском семинаре "Высокотехнологичный терроризм" [1], прошедшем Москве в июне 2001 года, а затем, его продолжении в декабре того же года в США, проводившемся Российской академией наук совместно с Национальными академиями США. На этом семинаре (еще до трагических событий сентября 2001 г.) рассматривались потенциально возможные направления использования различных технологий в террористических целях, включая химическое и бактериологическое, ядерное и компьютерное (кибертерроризм), возможные сценарии их использования, а также системы мер, как стратегического, так и оперативно-тактического характера.

Однако, и это следует отметить, многие из обсуждавшихся тогда предложений и сценариев не представлялись столь актуальными. После чудовищных по своему цинизму, масштабам и последствиям актов, совершенных 11 сентября 2001 года в Нью-Йорке и Вашингтоне, отношение мирового сообщества к этим проблемам стало более острым, а действия - более осознанными, скоординированными и последовательными. В последующие два года обсуждение вопросов терроризма вообще, и высокотехнологического терроризма в частности, проводились на различных форумах национального и международного масштабов, на всех уровнях представительства, - от консультаций специалистов в отдельных относительно "узких" областях до совещаний на уровне глав государств. Подписанные в ходе этих обсуждений документы создают благоприятные условия для активных действий, направленных на противодействие терроризму.

Одним из направлений, по которому на упомянутом российско-американском семинаре с российской стороны выступал автор настоящей публикации [2], был Кибертерроризм (кибернетический или компьютерный терроризм). Глобальное киберпространство и составляющая его основу сеть Интернет рассматривались при этом, как потенциально благоприятное поле для террористической деятельности. Уместно отметить, что компьютерный терроризм и соответствующая ему деятельность по целям и сути своей имеют смысл именно в рамках использования для этого крупной сетевой инфраструктуры или контроля над распределенными в сети важными информационными ресурсами. Данное обстоятельство указывает на типы сетевых объектов и инфраструктуры, которые следует рассматривать в качестве первоочередных объектов атаки террористов на Киберпространстве.

Несмотря на пристальное внимание к отмеченным выше вопросам (которые далее для краткости будет именовать "кибертерроризм" или "компьютерный терроризм"), на наличие документов международного и национального уровня, указывающих на необходимость активных действий на данном направлении,

реальных, опубликованных в доступной научно-технической литературе результатов исследований или разработок автору обнаружить не удалось. С одной стороны, это можно объяснить объемным и комплексным характером проблемы в целом, сложной организацией самих объектов первостепенного внимания на сетевой среде и отсутствием должным образом отработанных методологических подходов к анализу, управлению ими и защите. С другой стороны, это еще одно свидетельство недостаточного уровня понимания значимости и восприятия актуальности самой проблемы, отсутствия необходимых для начала таких работ побудительных мотивов, в том числе со стороны (а это национальная проблема) государственных ведомств.

С учетом этих обстоятельств, отталкиваясь от основных положений, изложенных в [2], попробуем в данной работе кратко изложить основные концептуальные аспекты модели атаки (явления, феномена), проявления которой можно трактовать как кибертерроризм, а также предложить модель защиты (противодействия), как систему мер для предупреждения или пресечения подобных действий.

Общие положения

Кратко сформулируем основные (отправные, начальные) положения для формирования искомых моделей и системы мер, изложенных в [2].

Терроризм - совокупность противоправных действий, связанных с покушениями на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимуществ при решении политических, экономических или социальных проблем.

Направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов можно представить в виде следующих:

1. Разрушение инфраструктуры сети корпоративного, национального или транснационального масштаба посредством вывода из строя системы управления ею или отдельных подсистем.
2. Несанкционированный (неправомерный) доступ к сетевой информации, охраняемой законом и носящей высокий уровень секретности, нарушение ее целостности, конструктивной управляемости и защищенности.

Следует отличать террористические действия от действий террористов с использованием сетевых ресурсов (в том числе собственных в Интернет) в целях пропаганды своих взглядов, нагнетания обстановки страха, напряженности и т. д.

Ущерб от террористических действий на сетевой среде связан:

- с человеческими жертвами или материальными потерями, вызванными деструктивным использованием элементов сетевой инфраструктуры;
- с возможными потерями (в том числе гибелью людей) от несанкционированного использования информации с высоким уровнем секретности или сетевой инфраструктуры управления в жизненно важных (критических) для государства сферах деятельности;
- с затратами на восстановление управляемости сети, вызванными действиями по ее разрушению или повреждению;
- с моральным ущербом как владельца сетевой инфраструктуры, так и собственного информационного ресурса;
- с другими возможными потерями от несанкционированного использования информации с высоким уровнем секретности.

С учетом изложенных выше положений, анализа моделей нарушителя и моделей атак, рассматриваемых при разработке политик безопасности, при использовании критериальных подходов к оценке уровня защищенности других (в том числе традиционных) компьютерных комплексов, а также моделей гарантированно защищенных систем, в качестве исходной посылки к формированию модели противодействия кибертеррористическим действиям можно рассматривать следующую.

Направления действий на сетевой среде с целью использования их результатов для проведения террористических актов, как набор приемов и методов, представляют собой злоумышленные действия, традиционно рассматриваемые в моделях нарушителя и моделях атак. Такие модели являются необходимым условием для формирования политики информационной безопасности и разработки мер и средств ее реализации в любых ведомственных или корпоративных сетях.

Отличие подходов к предотвращению и реагированию на действия в случае террористического характера целей от других противоправных действий в сетях общего пользования связано с более высоким уровнем требований к безопасности систем, обусловленных их назначением, целями и средой безопасности, и, соответственно, величиной издержек от подобных злоумышленных действий.

О величине убытков от успешных атак на национально значимые сферы хозяйственного комплекса можно судить, например, по результатам инцидентов в 2003 году, связанных с перебоями в электроснабжении крупных регионов США и Канады или нарушениями в системе авиаперевозок в Англии. Потери измерялись сотнями миллионов долларов, а уровень социальной напряженности влиял на политическую обстановку в странах.

В качестве понятия, интегрирующего противодействия кибертерроризму, рассмотрим антитеррористическую информационную безопасность с тем, чтобы подчеркнуть отличие от традиционной информационной безопасности.

Антитеррористическая информационная безопасность - совокупность механизмов, инструментальных средств, методов, мер и мероприятий, позволяющих предотвратить, обнаружить, а в случае обнаружения, - оперативно реагировать на действия, способные привести:

- к разрушению инфраструктуры сети посредством вывода из строя системы управления ею или отдельных ее элементов;
- к несанкционированному доступу к информации, охраняемой законом и носящей высокий уровень секретности, нарушению ее целостности, конструктивной управляемости и защищенности.

Основа антитеррористических действий с использованием сетевой среды - традиционная информационная безопасность, ее методология, модели, механизмы и инструментальные средства. Разработка, построение и сопровождение систем информационной безопасности для отдельных продуктов, изделий и комплексов на сетевой среде, особенно на сетях пакетной коммутации и Интернет, - сложная, многоплановая задача. Ее решения строятся с помощью конкретной системы мер, способов и механизмов их реализации на разных уровнях иерархии этой деятельности:

- законодательном;
- административном;
- операционном;
- программно-техническом.

Есть, и это отмечалось в [3], проблемы, связанные с реализацией конкретных мер, механизмов или инструментальных средств на каждом из перечисленных уровней. Степень разрешения этих проблем различна в различных странах и определяется разными факторами (научно-техническая база, уровень

развития сетевой инфраструктуры и т. п.), однако следует отметить, что в "среднем" проблемная область, общая методология информационной безопасности достаточно хорошо проработана и апробирована на традиционных комплексах. Существует, хотя и с разной степенью (и успехом) реализации на практике, необходимая законодательная база.

Вместе с тем, интегрированные распределенные системы информационно-вычислительных ресурсов, используемые для управления национально значимыми сферами хозяйственной деятельности (ведомственные или корпоративные), которые должны быть объектами первостепенного внимания с позиции разработки антитеррористических мер, по целому ряду причин более сложны для анализа и эффективного применения таких мер, чем системы, на которых меры информационной безопасности уже хорошо отработаны и апробированы.

Одной из причин является их сложная внутренняя структура, объективно различные требования, в том числе, по безопасности на отдельные элементы и ресурсы, трудности декомпозиции решений и средств их интеграции. Отмеченные обстоятельства очень затрудняют четкую формулировку политики безопасности для системы в целом и, как следствие, выбор и разработку адекватных средств ее реализации.

Оценка эффективности средств защиты, выполнения ими политики безопасности, обеспечивается либо на основе критериальных подходов [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20], либо с помощью средств их тестирования, надежной верификации или доказательства гарантированной защищенности для модели системы [21].

Для систем, потенциально уязвимых для кибертеррористических угроз, использование способов второго подхода затруднено и, это отмечалось выше, сложностью построения математических моделей, адекватно отражающих свойства исходной системы, и трудностями их анализа. Столь же сложен для использования критериальный подход к оценке подобных систем на всех этапах ее жизненного цикла. Однако, в отличии от аналогичных по сложности комплексов другого назначения, в силу изложенных выше обстоятельств, связанных с высокими требованиями к безопасности рассматриваемых систем, представляется целесообразным при оценке эффективности средств их защиты критериальный подход использовать в обязательном порядке, дополняя его, если это представляется возможным, способами тестирования, верификации и (или) формирования строгой доказательной базы.

Способы и механизмы операционного и программно-технического уровней на всех этапах жизненного цикла продукта или системы информационных технологий регламентируются требованиями, критериями и показателями информационной безопасности такого объекта оценки. Подобные показатели систематизированы государственными стандартами разных стран от "Оранжевой книги" до ее интерпретации для сетевых конфигураций в США [4, 5, 6, 7], "Канадские критерии оценки безопасности информационных технологий" [10], Руководящие документы Гостехкомиссии в России [12, 13, 14, 15, 16]. Более того, на этом направлении наблюдается явная, и правильная, по сути, тенденция к международной унификации этих стандартов (Гармонизированные европейские критерии [9] и Общие Критерии ИСО/МЭК 15408 [17, 18, 19]. На пути практического применения этих стандартов исследовательские коллективы многих стран активно работают над совершенствованием отдельных механизмов, позволяющих эффективно применять требования к системам информационной безопасности на разных уровнях. Например, в области законодательной - разумный баланс между конфиденциальностью персональной информации и широким доступом к данным общего доступа или международная унификация законодательных актов. В области программно-технической - механизмы ядра ОС для эффективной реализации основных (базовых) сервисов безопасности.

Исходные положения к разработке модели атаки

Принимая как постулат утверждение о том, что традиционная информационная безопасность является основой антитеррористической информационной безопасности, следует отметить, что деятельность по предупреждению и пресечению терроризма на сетевой среде вообще и, особенно в Интернет, имеет свою специфику. Факторы, характеризующие ее, представляются важными для формирования рациональной программы действий специалистов на разных этапах построения системы защиты - от формирования политики безопасности до эксплуатации и поэтапной модернизации системы.

Сформулируем в самом общем и кратком виде положения, которые могут рассматриваться как отправные (начальные) для формирования модели атаки, проявления которой могут быть охарактеризованы как кибертерроризм.

Рассматривая набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих "типовой профиль" такого сценария можно выделить следующие:

- субъект действия - персона и (или) группа лиц, имеющих целью проведение террористических действий против объекта (объектов), и (или) совокупность их агентов на сетевой среде первичного объекта атаки (определение далее по тексту), действующих с использование скрытых каналов передачи информации [22];
- предмет действия - сетевая инфраструктура (физическая среда передачи данных, коммуникационные средства и программное обеспечение), предоставляющие доступ к информационно-вычислительным ресурсам системы;
- цель действий - использовать предмет действия (сетевую инфраструктуру) для деструктивного воздействия на объект (объекты), результатом которого будут различные последствия (почва для шантажа, покушение на жизнь людей, разрушение вторичных объектов и т. п.);
- первичный объект -
    - компьютерный комплекс для относительно узкой, но стратегически важной или, например, способной прямо влиять на здоровье людей, области применения;
    - большая интегрированная система распределенных информационно-вычислительных ресурсов для обслуживания национально значимой сферы деятельности (сектора экономики, промышленности, . . .), например энергетическая (в т. ч., атомная), транспортная (воздушная или железнодорожная) система или ее элементы (местные, региональные);
- вторичный объект - персона или группа людей, материальные объекты различного назначения, информационные системы, которые могут быть подвержены деструктивным воздействиям со стороны первичных объектов, вплоть до уничтожения.

Усредненный сценарий действий террористов при этом должен, как правило, содержать:

- действия, обеспечивающие неавторизованный доступ к информации с высоким уровнем секретности;
- уничтожение, модификацию или замену программного кода, обеспечивающего нормальное (регламентированное) функционирование системы;
- ограничение доступа внешних или внутренних агентов системы безопасности, способных оперативно предотвратить злоумышленные действия.

Конечно, представленные положения не позволяют сформулировать модель атаки с надлежащей степенью полноты. Это предмет более глубокого анализа специалистов разных (в том числе гуманитарного цикла) направлений. Однако, и они позволяют описать основные типы угроз, предсказать условия их реализации, а значит, и общие соображения, которые могут быть положены в основу модели противодействия атаке. Следует отметить, что налицо комбинация всех трех типов угроз, соответственно, - конфиденциальности, целостности и доступности, на предотвращение которых должны быть ориентированы системы информационной безопасности рассматриваемых комплексов. Важным

фактором эффективности противодействия выступает необходимость оперативной, в реальном времени реакции на последовательность вышеперечисленных действий с атакующей стороны.

К разработке модели противодействия

Рассмотрим общие положения модели защиты, как системы контрмер, которые необходимо предпринимать на всех уровнях реализации сетевой безопасности для предотвращения каждой из перечисленных выше угроз и их совокупности в контексте "среднего" сценария террористического акта. Главной задачей на административном уровне является выработка подходов к формированию политик безопасности для распределенных, вообще говоря, гетерогенных систем, интегрирующих в своем составе подсистемы с различными функциями и условиями эксплуатации.

В числе первых действий на операционном, а тем более, программно-техническом уровне обеспечения информационной безопасности, должна стать выработка (на основе анализа основных положений современных критериев оценки безопасности информационных технологий) заданий на безопасность и профилей защиты, которые отвечали бы политике безопасности систем, подлежащих защите от кибертеррористических атак.

Как результат более эффективных мер, которые будут способны противостоять (противодействовать) угрозе конфиденциальности (неавторизованному доступу к информации высокого уровня секретности или элементам управляющей инфраструктуры) могут рассматриваться:

- на операционном уровне - это обучение и управление персоналом, четкое распределение обязанностей и минимизация привилегий;
- на программно-техническом уровне - средства идентификации и аутентификации пользователей, учитывающие их индивидуальные особенности; управление ресурсами на основе комбинации традиционных и новейших моделей логического разграничения доступа, учитывающих различные требования по безопасности к разным компонентам системы, а также криптографическая поддержка и экранирование.

Угрозе целостности информации должны противодействовать специальные программно-технические меры, контролирующие целостность и согласованность данных при их хранении и передаче. Отражению атак (угроз) на доступность способствуют такие меры, как оперативная реакция на сбои и механизмы надежного восстановления - на операционном уровне, повышенные меры отказоустойчивости, распределение и квотирование ресурсов - на уровне программно-технических сервисов.

Для предотвращения всех трех типов угроз на операционном уровне очень важной является физическая защита (включая физическое управление доступом) ключевых элементов сетевой инфраструктуры, а на программно-техническом уровне - протоколирование и активный аудит системы на предмет обнаружения аномальных ситуаций, способных деструктивно повлиять на ее функциональность. Своевременное обнаружение, оперативное и адекватное реагирование на подобные ситуации обеспечивает более высокий уровень безопасности (защищенности).

Отдельного внимания в плане формирования общей модели противодействия кибертерроризму заслуживают примыкающие к программно-техническим сервисам вопросы, связанные с выработкой системы в организации аудита недоверенных технических средств и программного обеспечения.

Настоятельная потребность в аудите и сертификации аппаратных средств, которые используются в национально значимых компьютерных системах, объясняется отсутствием доверенных зарубежных или отечественных аналогов.

Внимание, особенно в последние годы, к верификации программ обусловлено не столько стремлением исправлять "ошибки" (хотя и этим обстоятельством), сколько широким использованием программных систем со свободно распространяемыми в Интернет кодами. Такое программное обеспечение (и системное, и прикладное), как правило, разрабатываемое с участием широкого круга специалистов из разных стран мира, либо напрямую используется в комплексах различного назначения, либо на его основе идет разработка доверенного программного обеспечения.

Замечу, что приведены не все основные меры, способные противодействовать перечисленным угрозам. Их сложно систематизировать и обобщить в одной статье. Отметим мероприятия, обобщающие их в рамках отдельных уровней.

К мерам общего характера на этом направлении можно отнести следующие:

- Разработка новых законодательных актов (национальных и международных) в области контроля над использованием систем сетевого управления национально значимыми сферами хозяйственного комплекса, оборонной промышленности и бизнеса с точки зрения возможного применения в отношении них террористических действий.
- Поиск типовых подходов к формированию
    - политик безопасности для стратегически важных объектов, управление которыми осуществляется с использованием сетевых структур, на основе анализа рисков, связанных с террористическими действиями (актами);
    - программ практической реализации политик безопасности и операционных регуляторов, ориентирующих персонал, обслуживающий системы управления такими объектами, на неукоснительное соблюдение правил, выработанных для их выполнения.
- Строгое следование требованиям и критериям стандартов (национальных и (или) международных) оценки продуктов или систем, предназначенных для эксплуатации на сетевой среде в условиях, предусматривающих оперативную реакцию на террористические действия.
- Анализ существующих показателей безопасности сетевых продуктов и систем с позиции их адекватной реакции на возможные сценарии террористических действий, развитие уже существующих стандартов в этой области на основе проведенного анализа.

Мировая сеть Интернет, построенная на основе стека протоколов TCP/IP, транснациональна по своей природе. Изначально рассчитанный на использование в открытых исследовательских и образовательных сетях, базовый в Интернет протокол межсетевого взаимодействия IPv.4, до настоящего времени имеет проблемы с защитой информационных ресурсов и защитой инфраструктур, поддерживающих такие сети. Несмотря на большую, многолетнюю (более 20 лет) работу, проводимую мировым сообществом математиков и программистов, исследователей и практиков, значительная их часть не устранена до настоящего времени.

Однако темпы роста метасети Интернет огромны. Сегодня она объединяет более 200 млн. сетевых ЭВМ в почти 250 странах мира на всех континентах. Эта сеть "де-факто" или потенциально имеет связность с любыми сетями от локальных бытовых и исследовательских до сетей силовых ведомств или сетей, которые используются для управления национально значимыми отраслями или сферами деятельности. Это безусловно инфраструктура, которая потенциально может быть задействована террористами для реализации своих целей в каждой из перечисленных выше сфер и отраслей человеческой деятельности. Более того, чем выше уровень развития сетевых технологий, шире спектр их использования в различных сферах человеческой деятельности, тем вероятнее внимание к ним со стороны террористов и более изощренны могут быть их действия. Сегодня, например, не выглядит нереализуемым намеренно организованный отказ бортовой системы управления транспортным средством в воздухе, на земле или на воде, выдача управляющих воздействий, которые могли бы перенацелить боевые снаряды (ракеты) на другие цели. К сожалению, такие примеры можно продолжить. С этим нужно считаться и предвосхищать подобные действия.

Проблемы реализации

Представленные в настоящей работе идеи и положения следует рассматривать как результат начального осмысления очень важной и трудной для решения проблемы. Исходная посылка о том, что в методическом плане традиционные подходы к разработке и построению систем информационной безопасности остаются неизменными при создании систем и сценариев противодействия кибертерроризму, не только не отменяются, а наоборот, требует более серьезного осмысления этой базы. В данном контексте совершенствование критериальной основы оценки безопасности информационных технологий, разработка новых конструктивных моделей для тестирования, верификации средств защиты сложно организованных распределенных компьютерных систем, формирование доказательной базы их гарантированной защищенности, совершенствование программно-технических сервисов безопасности - это движение в правильном направлении. Однако трудности на этом пути есть. Приведу лишь две из них, которые указывают на стратегический и даже глобальный характер проблемы.

- Многие из обсуждаемых выше положений, призванных сформировать адекватные подходы к описанию политики безопасности, моделей (профилей) атаки и атакующего, модели защиты в условиях противодействия кибертерроризму, пока не обеспечены соответствующими технологическими средствами. Трудность состоит не только в разработке упомянутых конструктивных моделей (что представляет большую комплексную задачу), но и в поиске теоретических подходов к созданию технологий и инструментальных средств для реализации отдельных механизмов этих моделей. Работа на этих направлениях потребует привлечения современных математических методов и совместной, скоординированной работы математиков, специалистов в области информационной безопасности и сетевых технологий.
- Ряд крупных, рассматриваемых в качестве потенциально уязвимых для кибертерроризма, национально значимых систем взаимосвязаны на основе современных магистральных сетевых инфраструктур транснационального масштаба. Это обстоятельство делает потенциально более подверженными в отношении указанных угроз страны с низким уровнем развития сетевой инфраструктуры. Во-первых, эти страны уязвимы к подобным действиям на их собственной территории. Во-вторых, как в случае с традиционным "хакерским" приемом, когда в качестве "транзитного" для атаки используется какой-то третий компьютер со слабой системой защиты. В качестве таковых для крупных террористических действий (включая их подготовку) могут использоваться элементы сетевой инфраструктуры слаборазвитых в сетевом отношении стран. Такое развитие событий возможно, оно требует осмысления и выработки программы действий на международном уровне. Это не простое механическое переосмысление, например, политики, проводимой ЮНЕСКО в рамках соответствующей программы по выравниванию сетевых инфраструктур различных стран за счет помощи странам, слабым в этом отношении. Проблема информационной безопасности (сетевой в том числе) более тонкая и серьезная. Она, кроме общих (в методологическом, техническом, правовом и т. п. плане) межнациональных, затрагивает и национальные интересы. Поэтому их реализация потребует выработки некоторых сбалансированных в этом отношении мер и программы. Однако тот факт, что такая программа необходима, сомнений не вызывает и это прекрасное поле для активных совместных действий на международной арене.

Заключение

В заключении хотелось бы заметить, что описанные выше сценарии действий могут быть обусловлены не только террористическими целями. Однако проблема в целом и условия ее разрешения при этом не изменяются.

Представленные в настоящей работе материалы не претендуют на полноту изложения и отточенность формулировок. Это в большей степени "эскизный проект" или предложения для активных действий на новом, актуальном и продиктованном самой жизнью направлении.

Основные идеи, положения и оценки прошли осмысление и некоторую апробацию при обсуждении вопросов на семинарах и "круглых столах" по проблемам информационной безопасности в Московском университете, на конференциях "Московский университет и развитие криптографии в России" и "Математика и безопасность информационных технологий" (МаБИТ-03). Все эти обсуждения стали возможны благодаря тому, что тематика информационной безопасности была принята, получила одобрение и развитие в научном и образовательном плане в МГУ им. М. В. Ломоносова. Инициатором этого процесса с 1997 года стал ректор Московского университета академик Виктор Антонович Садовничий. Благодаря его поддержке, участию в исследованиях и активной позиции в плане развития учебного процесса, к данной тематике привлечены математики и специалисты в области кибернетики, физики и экономисты, психологи, юристы и политологи. Такое положение дел является гарантией новых, интересных, в том числе - междисциплинарных результатов, на которые в значительной степени рассчитана программа действий, кратко изложенная в данной работе.

Литература

1. Высокотехнологичный терроризм. Материалы российско-американского семинара. Москва, 4-6 июня 2001 г., Российская академия наук в сотрудничестве с Национальными академиями США, 320 с.
2. *Васенин В. А., Галатенко А. В.* Компьютерный терроризм и проблемы информационной безопасности в Интернет. В кн. Высокотехнологичный терроризм. Материалы российско-американского семинара РАН в сотрудничестве с Национальными академиями США. Москва, 4-6 июня 2001 г., М., 2002, с. 211-225.
3. *Васенин В. А., Галатенко А. В.* О проблемах информационной безопасности в сети Интернет. Глобальная информатизация и безопасность России. Материалы круглого стола "Глобальная информатизация и социально-гуманитарные проблемы человека, культуры и общества". МГУ, октябрь 2000 г., М.: Изд-во МГУ, 2001, с. 199-214.
4. Trusted Computer System Evaluation Criteria, US DOD 5200. 28-STD, December 1985.
5. National Computer Security Center. A Guide to Understanding Audit in Trusted Systems // NCSC-TG-001, 1987.
6. National Computer Security Center. A Guide to Understanding Audit in Trusted Systems // NCSC-TG-003, 1987.
7. National Computer Security Center. Trusted Network Interpretation // NCSC-TG-003, 1987.
8. Security Architecture for Open Systems Interconnection for CCITT Applications / Recommendation X.800 // CCITT. Geneva, 1991.
9. Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom // Department of trade and Industry. L., 1991.
10. Canadian Trusted Computer Product Evaluation Criteria. Version 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada. January, 1993.
11. Information Technology Security Evaluation Criteria. Version 1.2. Office for Official Publications of the European Communities. June 1991.
12. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от несанкционированного доступа к информации. М., 1992.
13. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.
14. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.
15. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. М., 1992.

16. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.
17. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. - ISO/IEC 15408 - 1.1999.
18. Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements. - ISO/IEC 15408 - 2.1999.
19. Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements. - ISO/IEC 15408 - 3.1999.
20. Проект Госстандарта РФ ГОСТ Р ИСО/МЭК 15408 "Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий." Части 1, 2, 3 М.: Изд-во Госстандарта России, 2002.
21. *Грушо А. А., Тимонина Е. Е.* Теоретические основы защиты информации. М.: Изд-во агентства "Яхтсмен", 1996. 192 с.
22. *Грушо А. А., Тимонина Е. Е.* Языки в скрытых каналах. Труды международной конференции "Информационные технологии в науке, образовании, телекоммуникациях, бизнесе". Украина, Крым, Ялта - Гурзуф, 19-29 мая 2003 г.