Перспективные направления исследований в области компьютерной безопасности

И. В. Котенко, *д. т. н., профессор, руководитель группы компьютерной безопасности СПИИРАН*
Р. М. Юсупов, *д. т. н., профессор, директор СПИИРАН*

Одним из важнейших направлений исследований в области информационной безопасности являются работы, связанные с изучением различных аспектов обеспечения безопасности компьютерных сетей и систем. В статье рассматриваются основные направления научных изысканий в области компьютерной безопасности, выполняемых в Санкт-Петербургском институте информатики и автоматизации РАН.

Введение

Исследования в области компьютерной безопасности, выполняемые в СПИИРАН, проводятся в нескольких лабораториях института:

- лаборатории интеллектуальных систем;
- лаборатории информационно-вычислительных систем и проблем защиты информации;
- лаборатории прикладной информатики;
- лаборатории автоматизации научных исследований и др.

К основным направлениям научных исследований СПИИРАН в данной области следует отнести следующие направления.

- Научно-методологические основы информационной безопасности и информационного противоборства [1–4 и др.].
- Технологии построения и поддержки функционирования информационно-безопасных систем, основанных на политиках безопасности, включающие модели, методы и средства проектирования, создания и поддержания требуемого уровня безопасности распределенных компьютерных систем, основывающихся на механизмах спецификации и реализации верифицированных политик безопасности, непрерывного мониторинга их выполнения и адаптации к условиям применения [5–6 и др.].
- Применение интеллектуальных, в частности многоагентных технологий для исследования и реализации перспективных механизмов защиты информации, в том числе на основе использования собственного инструментария разработки многоагентных систем [7–12 и др.].
- Моделирование киберпротивоборства в сети Интернет:
  - методы моделирования атак на компьютерные сети с целью активного анализа уязвимостей в защите компьютерных сетей, обучения систем защиты и оценки уровня защищенности;
  - методы моделирования механизмов защиты;
  - разработка и использование компьютерных полигонов для отработки методов и средств информационного противоборства, сочетающего различные классы средств и моделей (от аналитических, аналитико-имитационных, имитацион-

ных и до полунатурных и натурных) и др. [13–14 и др.].

- Теоретические и практические основы построения систем обнаружения вторжений, основанных на перспективных подходах, в том числе машинного обучения, извлечения знаний, анализа и объединения данных и др. Методы обучения обнаружению вторжений в компьютерные сети, служащие для автоматической адаптации систем обнаружения вторжений к новым типам атак, реконфигурации компьютерных сетей и изменению профилей пользователей, сервисов и приложений [15–18 и др.].
- Теоретические и практические основы построения систем мониторинга сетевой безопасности и работы пользователей, а также анализа безопасности компьютерных систем на различных стадиях их жизненного цикла, основанные на:
  - комбинировании пассивных и активных методов;
  - использовании различных методов анализа уязвимостей (например, сетевого и хостового);
  - выявлении различий между специфицированной политикой безопасности и конфигурацией системы и текущим состоянием;
  - вычислении графов атак и выявлении уязвимых мест;
  - применения комплексной системы вычисления метрик безопасности, сравнения различных политик безопасности и формирования рекомендаций по увеличению уровня защищенности [20 и др.].
- Технологии построения обманных (ложных) информационных систем, предназначенных для введения злоумышленников (в том числе компьютерных террористов) в заблуждение, отслеживания их действий, распознавания их намерений и местоположения [21 и др.].
- Применение биологического подхода к обеспечению безопасности информации на основе иммунных сетей, направленного на получение формального описания иммунных сетей, создание программной реализации и программного эмулятора иммуночипа, а также электронной схемы иммуночипа [22 и др.].
- Методы стеганографии, в частности скрытого встраивания информации в цифровые файлы, в том числе использующие сингулярные разложения [23 и др.].
- Методы создания безопасного кода и противодействия несанкционированному использованию и изменению программного обеспечения.

Ниже некоторые из перечисленных направлений исследований раскрываются более детально.

Управление политиками безопасности

Современные средства обеспечения защищенности распределенных компьютерных систем в целом и их отдельные элементы отличаются широтой и многообразием применяемых технологий. Тем не менее с концептуальной точки зрения, основные требования к защите информационных ресурсов определяются следующими хорошо известными положениями:

- объекты системы должны быть защищены от несанкционированного доступа;
- должны быть разработаны механизмы поддержки целостности защищаемых объектов и самой системы защиты;
- должна обеспечиваться доступность информационных ресурсов.

Возникает противоречие между желанием управлять всей совокупностью применяемых методов обеспечения защиты и механизмами создания и поддержки отдельных компонентов защищенной информационной среды на различных этапах жизненного цикла (проектирования, конфигурирования, развертывания, функционирования и модификации).

Работы по преодолению указанного противоречия заключаются в проведении научных исследований, в разработке стандартов создания защищенных информационных систем и задания политик безопасности как совокупности правил обеспечения безопасности с последующей разработкой программно-аппаратных средств поддержки этих стандартов.

Используемым в настоящее время подходам присущ целый ряд недостатков, и, как показывают исследования, они оказываются не в состоянии эффективно и надежно решать задачу управления защищенностью сети в режиме реального времени. Эти недостатки обусловлены, главным образом, узкой специализацией отдельных средств обеспечения безопасности, неразвитыми механизмами верификации защиты на этапах создания и поддержки, неадекватными механизмами опреде-

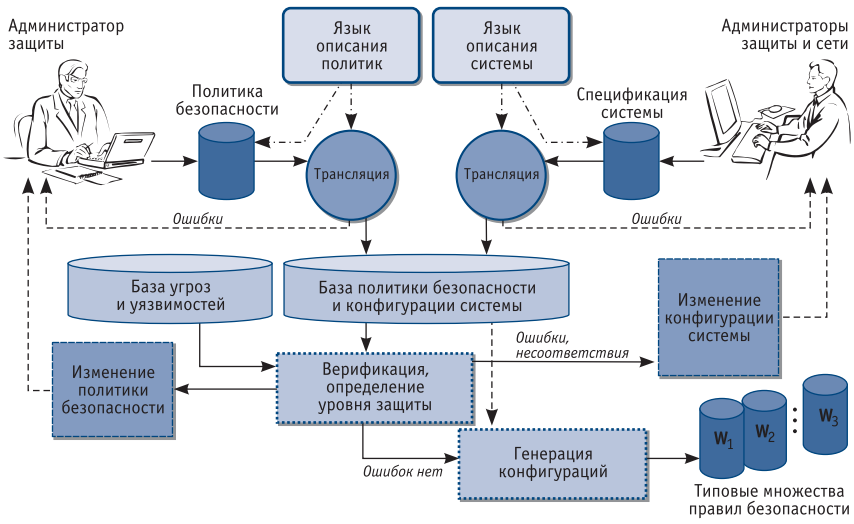

Рис. 1. ***Начальные этапы технологии разработки информационно-безопасных систем, основанных на политиках безопасности (от спецификации до трансляции сформированных правил безопасности в типовые множества правил)***

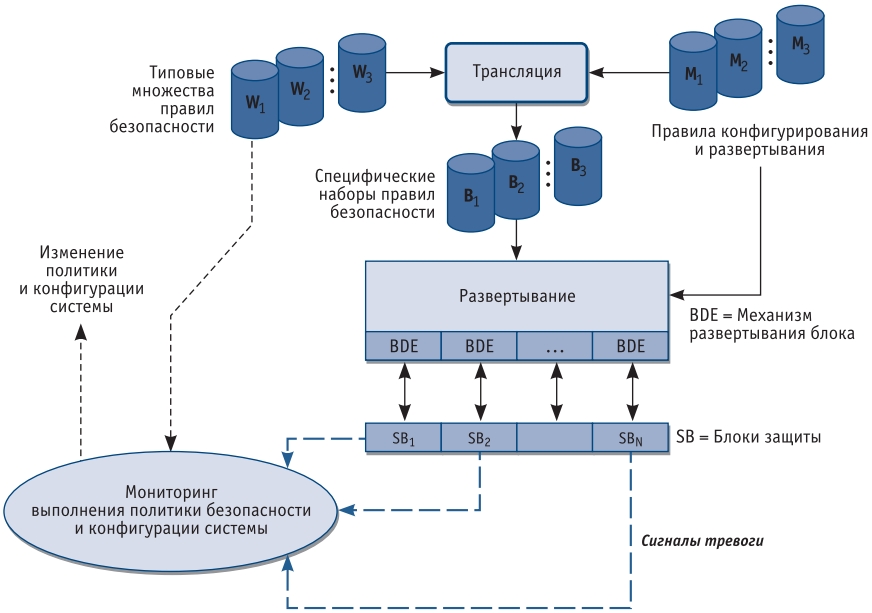

Рис. 2. ***Последующие этапы технологии разработки информационно-безопасных систем, основанных на политиках безопасности (от трансляции правил безопасности в параметры конфигурации и настройки программно-аппаратного обеспечения до мониторинга выполнения политик)***

ления уровня защищенности, анализа рисков, мониторинга состояния сетей, обнаружения вторжений и анализа уязвимостей.

Кроме необходимости разработки отдельных механизмов, в связи с отсутствием или неразвитостью соответствующих теоретических основ и технических решений чрезвычайно важной становится задача построения теоретических и практических основ создания единых унифицированных систем (сред), выполняющих комплекс задач по поддержке всего жизненного цикла распределенных защищенных компьютерных систем, включая адаптивное управление политиками безопасности.

Предлагаемая технология поддержки жизненного цикла распределенных защищенных компьютерных систем, основанных на политиках безопасности, позволяет преодолеть перечисленные выше недостатки.

Предполагается, что такая единая унифицированная система (среда), должна обеспечивать непрерывную цепочку различных этапов жизненного цикла распределенных защищенных компьютерных систем (с множеством прямых и обратных связей от одного этапа к другому) (рис. 1–2 [5, 6]):

- спецификацию политик безопасности и архитектуры (или конфигурации) защищаемой системы;
- трансформацию политик безопасности с целью их уточнения (детализации) с учетом описания защищаемой системы;
- верификацию политик безопасности (проверка правильности и устранение конфликтов на различных уровнях их детализации);
- определение уровня безопасности и анализ рисков;
- изменение политик и конфигурации системы в соответствии с требуемым уровнем безопасности и возможностями по использованию различных ресурсов и выделению финансовых средств и на защиту информации;
- реализацию политик безопасности в системе, в том числе трансляции сформированных правил безопасности в параметры конфигурации и настройки программно-аппаратного обеспечения;
- проактивный мониторинг выполнения политик безопасности и изменения конфигурации системы, в том числе обнаружение отклонений работы пользователей от политики безопасности, обнаружение вторжений и анализ уязвимостей;
- адаптацию поведения распределенных защищенных компьютерных систем и реализованных политик безопасности в соответствии с условиями функционирования.

Основной результат предлагаемых исследований и разработок – комплекс формальных методов, моделей, алгоритмов и построенных на их основе программно-аппаратных средств, направленных на разработку единой унифицированной интегрированной среды для проектирования, создания и управления безопасностью распределенных защищенных компьютерных систем, базирующихся на механизмах реализации верифицированных политик безопасности, непрерывного мониторинга их выполнения и адаптации к условиям применения.

В рамках данного направления ведется разработка следующих результатов:

- теоретические основы и концепция создания и использования единой унифицированной интегрированной среды для проектирования, создания и поддержания требуемого уровня безопасности распределенных защищенных компьютерных систем;
- методы, модели, алгоритмы и программные средства для спецификации политик безопасности и архитектуры защищаемой системы, трансформации политик безопасности с целью их уточнения (детализации) с учетом описания защищаемой системы, верификации политик безопасности (проверки правильности и устранения конфликтов), определения уровня безопасности и анализа рисков и изменения политик в соответствии с требуемым уровнем безопасности и возможностями по использованию различных ресурсов и выделению финансовых средств на защиту информации;
- методы, модели, алгоритмы и программные средства для реализации политик безопасности, в том числе трансляции сформированных правил безопасности в параметры конфигурации и настройки конкретного программно-аппаратного обеспечения, проактивного мониторинга выполнения политик

безопасности и изменения конфигурации системы, в том числе обнаружения отклонений работы пользователей от политики безопасности, обнаружения вторжений и анализа уязвимостей, а также адаптации поведения распределенных защищенных компьютерных систем и реализованных политик безопасности в соответствии с условиями функционирования.

К настоящему времени разработаны архитектура, модели и прототипы компонентов верификации политик безопасности, оценки уровня защищенности и мониторинга выполнения политик безопасности.

Механизмы защиты информации, основанные на многоагентных технологиях

Традиционные методы защиты компьютерных сетей в большей мере ориентированы на защиту от конкретных видов угроз и атак и, как правило, реализуются в виде набора программных и аппаратных компонентов, функционирующих относительно независимо друг от друга. Существующие системы защиты, как правило, имеют централизованную структуру, характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, большим процентом ложных срабатываний при обнаружении вторжений, значительной деградацией трафика целевых информационных потоков из-за большого объема ресурсов, выделяемых на защиту и т. п.

Перспективным подходом к построению комплексных систем защиты информации в компьютерных сетях, позволяющим преодолеть некоторые из перечисленных недостатков, является *технология интеллектуальных многоагентных систем*. Этот подход позволяет существенно по сравнению с традиционными методами повысить эффективность защиты информации, в том числе ее адекватность, отказоустойчивость, устойчивость к деструктивным действиям, универсальность, гибкость и т. д.

В соответствии с данным подходом предполагается, что компоненты систем защиты информации, специализированные по типам решаемых задач, тесно взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений, адаптируются к изменению трафика, реконфигурации аппаратного и программного обеспечения, новым видам атак [7–12].

В рамках предлагаемого подхода компоненты многоагентной системы защиты информации представляют собой интеллектуальные автономные программы (агенты защиты), реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств, операционных систем и приложений, повышая защищенность системы до требуемого уровня.

В настоящее время разработаны архитектуры, модели и программные прототипы нескольких многоагентных систем, в том числе агентно-ориентированная система моделирования атак, многоагентная система обнаружения вторжений, многоагентная система обучения обнаружению вторжений и др.

Согласно разработанной технологии процесс создания многоагентных систем для любой предметной области, в том числе защиты информации в компьютерных сетях, предполагает решение двух высокоуровневых задач:

- создание «системного ядра» многоагентной системы;
- клонирование программных агентов и отделение сгенерированной многоагентной системы от «системного ядра».

Для спецификации «системного ядра» используются два компонента программного инструментария создания многоагентных систем MASDK (Multi-agent System Development Kit), разработанного в лаборатории интеллектуальных систем СПИИРАН. Первый из них – это так называемый «Типовой агент» (Generic Agent), предназначенный для создания высокоуровневой спецификации класса агента. Второй – служит для формирования проблемно-ориентированной архитектуры приложения, заполнения данных, знаний, а также определения коммуникационного компонента.

Агенты, сгенерированные с использованием MASDK, имеют аналогичную структуру. Различия отражаются в содержании данных и баз знаний агентов. Каждый агент взаимодействует с другими агентами, средой, которая воспринимается и, возможно, изменяется агентами, а также пользователем, общающимся с агентами через пользовательский интерфейс.

В предложенной формальной модели и прототипе *агентно-ориентированной системы моделирования атак (АСМА)* распределенные скоординированные атаки на компьютерную сеть рассматриваются в виде последовательности совместных действий агентов-хакеров, которые выполняются с различных хостов [8, 9]. Предполагается, что хакеры координируют свои действия согласно некоторому общему сценарию. На каждом шаге сценария атаки они пытаются реализовать некоторую частную подцель. АСМА построена на основе предложенной формальной модели реализации атак.

Отличительные черты реализованного в АСМА подхода к моделированию атак:

- моделирование атак базируется на спецификации задач хакеров и иерархии их намерений;
- многоуровневое описание атаки представляется в последовательности «общий сценарий распределенной атаки → намерения хакеров → простые атаки → входной трафик или данные аудита»;
- разработка планов действий хакеров и моделей отдельных атак основывается на задании онтологии предметной области «Атаки на компьютерные сети»;
- формальное описание сценариев взаимодействия агентов и реализации распределенных атак выполнено на базе семейства стохастических атрибутных грамматик, связанных операциями подстановки;

- в алгоритмической интерпретации процедур генерирования атак каждой из грамматик ставится в соответствие автомат;
- генерирование действий (атак) хакеров происходит в зависимости от реакции атакуемой сети в реальном масштабе времени.

Разработанный к настоящему времени программный прототип АСМА состоит из следующих компонентов (агентов): множества агентов хакеров, каждый из которых реализует модель атакующего, агента – модели атакуемой компьютерной сети и генератора фонового «нормального» трафика. В процессе атаки агенты обмениваются сообщениями с целью координации своих действий.

Компоненты *многоагентной системы обнаружения вторжений (МСОВ)* – это взаимодействующие между собой агенты, совместно решающие общую задачу обнаружения вторжений в компьютерную сеть [10]. Архитектура МСОВ включает один или несколько экземпляров агентов разных типов, специализированных для решения подзадачи обнаружения вторжений. Агенты распределены по хостам защищаемой сети, специализированы по типам решаемых задач и взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений. В принятой архитектуре исследуемого прототипа МСОВ в явном виде отсутствует «центр управления» семейством агентов – в зависимости от сложившейся ситуации ведущим может становиться любой из агентов, инициирующий и (или) реализующий функции кооперации и управления. В случае необходимости агенты могут как клонироваться (образовывать новые сущности), так и прекращать свое функционирование. В зависимости от ситуации (вида и количества атак на компьютерные сети, наличия вычислительных ресурсов для выполнения функций защиты) может потребоваться генерирование нескольких экземпляров агентов каждого класса. Предполагается, что архитектура МСОВ может адаптироваться к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт.

Представляется, что наиболее действенный путь обнаружения распределенных многофазных атак, направленных на компьютерные сети, состоит в кооперации множества агентов защиты, распределенных по хостам сети. Поэтому основное достоинство МСОВ заключается в способности относительно «легких» компонентов системы к сотрудничеству и совместному решению сложной задачи обнаружения таких атак. Базовые черты подхода, реализованного в МСОВ, таковы:

- расширяемая и адаптивная многоагентная архитектура;
- центральное внимание уделяется обнаружению многофазных распределенных атак;
- обеспечение безопасности и робастности (обработка сетевых событий, важных с точки зрения защиты информации, и функции управления распределены среди множества агентов различных хостов).

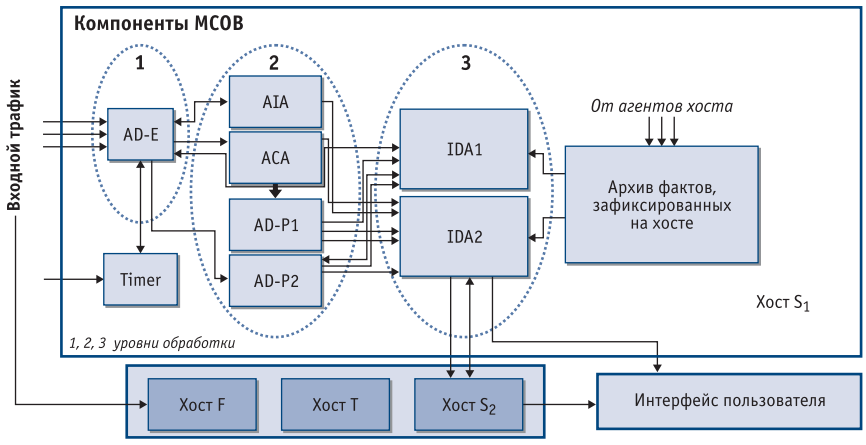

Рис. 3. ***Архитектура компонентов МСОВ на хосте***

Базовые типы компонентов разработанной МСОВ, размещаемые на каждом из хостов защищаемой компьютерной сети, представлены на рис. 3.

Агент-демон AD-E (AD-Events) осуществляет предварительную обработку поступающих на хост сообщений, фиксируя значимые для защиты информации события, и переадресует выделенные сообщения соответствующим специализированным агентам. *Агент-демон идентификации и аутентификации AIA* ответствен за идентификацию источников сообщений и подтверждение их подлинности. *Агент-демон разграничения доступа ACA* регламентирует доступ пользователей к ресурсам сети в соответствии с их правами и метками конфиденциальности объектов защиты. Агенты AIA и ACA обнаруживают несанкционированные действия по доступу к информационным ресурсам хоста, прерывают соединения и процессы обработки событий, отнесенные к числу несанкционированных, а также посылают сообщения агентам обнаружения вторжений. *Агенты-демоны AD-P1 и AD-P2 (AD-Patterns)* отвечают за обнаружение отдельных «подозрительных» событий или очевидных фактов вторжения и принятие решений относительно реакции на данные события (факты). *Интеллектуальные агенты обнаружения вторжений IDA1 и IDA2* реализуют более высокий уровень обработки и обобщения обнаруженных фактов. Они принимают решения на основе сообщений об обнаруженном подозрительном поведении и явных атаках как от агентов-демонов своего хоста, так и от агентов других хостов.

Возможными высокоуровневыми сценариями, обнаруживаемыми IDA2, являются:

- разведка – разведывательные действия атакующего (действия по определению конфигурации сети, обнаружению хостов, функционирующих на хосте сервисов, определению операционной системы, приложений и т. п.);
- внедрение в систему – действия злоумышленника по взлому хоста и внедрению в систему;

- повышение прав – попытки атакующего, направленные на получение повышенных прав по доступу к объектам хоста;
- распространение поражения на хосте – нелигитимное распространение злоумышленника по объектам хоста (каталогам, файлам, программам);
- распространение поражения по сети – распространение атакующего по защищаемой компьютерной сети и др.

Многоагентная система обучения обнаружению вторжений в компьютерные сети (МСООВ) является мультисенсорной системой объединения данных. Она формирует решения на основе многоуровневой модели обработки входных данных (входного трафика сети и данных аудита). На нижнем уровне решения принимаются так называемыми «*базовыми*» классификаторами. Их может быть несколько для одного и того же подмножества атак, но они должны обучаться на различных наборах обучающих и тестовых данных. На более высоком уровне они используются для принятия итогового решения метаклассификаторами.

Применительно к такому взгляду на обучаемую систему предложена архитектура многоагентной системы обучения обнаружению вторжений. Эта система имеет многоагентную архитектуру, реализующую многоуровневое обучение на основе имеющихся интерпретированных данных из тех же источников и представленных в тех же структурах, которые используются МСОВ. Типовыми классами агентов МСООВ являются:

- класс агентов управления данными обучения;
- класс агентов тестирования классификаторов;
- класс агентов подготовки метаданных;
- класс обучающих агентов.

В качестве методов (алгоритмов) обучения, которые позволяют решать рассматриваемую задачу обучения, используются методы ID3, C4.5, бустинг, мета-классификации, FP-growth, метод визуальной классификации, GK2, INFORM и др.

Моделирование кибер-противоборства

В настоящее время актуальным направлением научных исследований в области обеспечения безопасности компьютерных систем является формализация сложных процессов, которые происходят в сети Интернет с целью выработки адекватных механизмов защиты от существующих и вновь появляющихся угроз. В данном контексте эта задача может рассматриваться как задача формализации организационного и технического компьютерного противоборства между системами защиты информации и системами нападения злоумышленников, которая базируется на исследовательском моделировании указанного комплекса процессов на основе использования семейства различных моделей (от аналитических до полунатурных и натурных) [13].

В проводимых исследованиях развивается агентно-ориентированный подход к моделированию противоборства злоумышленников и систем защиты в виде антагонистического взаимодействия команд программных агентов, сформулированный в [26]. Выделяется, по крайней мере, две команды агентов, воздействующих на компьютерную сеть, а также друг на друга [29–31] (рис. 4): команда агентов-злоумышленников и команда агентов защиты. Агенты различных команд соперничают для достижения противоположных намерений. Агенты одной команды сотрудничают для осуществления общего намерения.

Цель команды агентов-злоумышленников состоит в определении уязвимостей компьютерной сети и системы защиты и реализации заданного перечня угроз информационной безопасности (конфиденциальности, целостности и доступности) посредством выполнения распределенных скоординированных атак. Цель команды агентов защиты состоит в защите сети и собственных компонентов от атак.

Команда агентов-злоумышленников реализует развитые стратегии, включающие сбор информации о системе:

- цели нападения;
- обнаружение уязвимостей и используемых средств защиты;
- моделирование способов преодоления защиты;
- подавление, обход или обман средств защиты (например, посредством реализации «растянутого» во времени скрытого сканирования, выполнения отдельных скоординированных действий (атак)

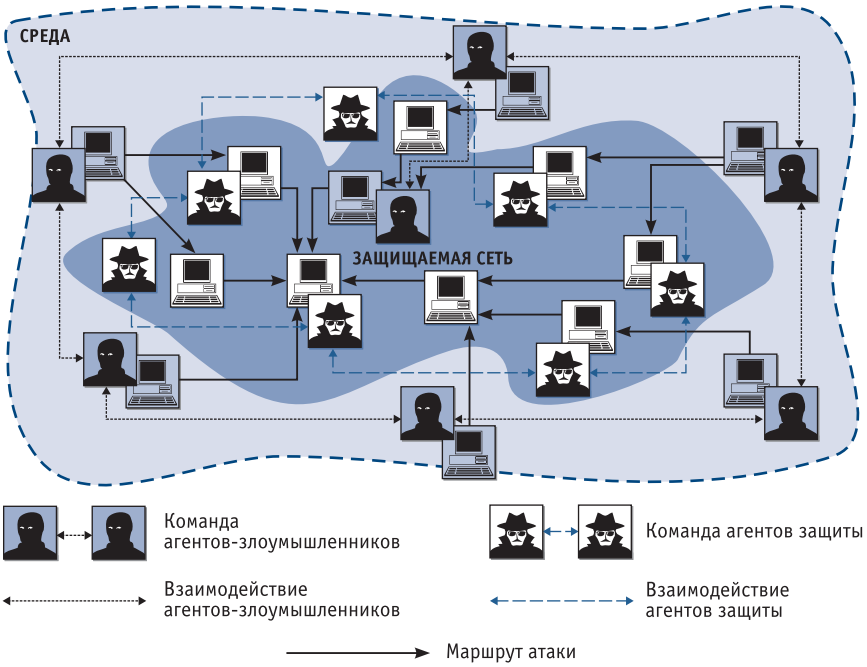

Рис. 4. ***Представление кибернетического противоборства в виде взаимодействия команд агентов***

из нескольких различных источников, вместе составляющих сложную многофазную атаку и др.);
- использование уязвимостей и получение доступа к ресурсам;
- повышение полномочий;
- реализацию определенной угрозы;
- скрытие следов своей деятельности и создание «черных ходов» для использования их при последующем вторжении.

Примером автоматической стратегии является поражение сети Интернет, возникающее в результате распространения сетевых вирусов и червей, в том числе недавние эпидемии, высвечивающие тенденцию сращивания вирусных и спам-технологий и формирования объединенной, мотивированной сети агентов-злоумышленников.

Команда агентов защиты выполняет в режиме реального времени последовательность следующих действий:
- реализацию механизмов защиты, соответствующих установленной политике безопасности (в том числе проактивного препятствования вторжениям, блокирования атак и их обнаружения);
- сбор информации о состоянии защищаемой системы и анализ обстановки;
- предсказание намерений и возможных действий злоумышленников;
- заманивание злоумышленников с использованием ложных информационных компонентов с целью введения в заблуждение и уточнения их целей;
- непосредственное реагирование на вторжения, в том числе усиление критичных механизмов защиты;
- устранение последствий вторжения, выявленных уязвимостей и адаптация системы обеспечения информационной безопасности к последующим вторжениям.

Структура команды агентов описывается в терминах иерархии групповых и индивидуальных ролей. Конечные узлы иерархии отвечают ролям индивидуальных агентов, промежуточные узлы – групповым ролям. Механизмы взаимодействия и координации агентов базируются на трех группах процедур:
- обеспечение согласованности действий;
- мониторинг и восстановление функциональности агентов;
- обеспечение селективности коммуникаций (для выбора наиболее «полезных» коммуникационных актов).

Спецификация иерархии планов действий осуществляется для каждой из ролей. Для каждого плана описываются:
- начальные условия, когда план предлагается к исполнению;
- условия, при которых план прекращает исполняться;
- действия, выполняемые на уровне команды, как часть общего плана (для групповых планов явно выражается совместная деятельность).

Команда агентов-злоумышленников эволюционирует посредством генерирования новых экземпляров и типов атак с целью преодоления подсистемы защиты. Команда агентов защиты адаптируется к действиям злоумышленников путем формирования новых экземпляров механизмов и профилей защиты.

Взаимодействие между агентами разных команд представляется как игра двух соперников, в которой целью агентов является поиск стратегии, максимизирующей ожидаемый интегральный выигрыш в игре.

Для того чтобы справиться с гетерогенностью и распределенностью источников информации и используемых агентов, применяется основанный на онтологии подход и специальные протоколы для спецификации распределенного согласованного тезауруса понятий. Онтология предметной области обеспечения безопасности компьютерных сетей реализуется на базе стандартных языковых средств RDF или DAML+OIL.

Проектирование и реализация рассмотренной многоагентной системы были осуществлены на базе нескольких различных инструментариев: MASDK, JADE, OMNeT++ INET Framework [14]. В настоящее время разработка ведется на базе пакета моделирования OMNeT++ INET Framework.

На основе OMNeT++ INET Framework разработана среда для многоагентного моделирования атак «Распределенный отказ в обслуживании» (DDoS) и механизмов защиты от них [13, 14]. Для этого система INET Framework подверглась нескольким модификациям. Так, были созданы: таблица фильтрации пакетов на сетевом уровне для моделирования действий стороны защиты, модуль, позволяющий просматривать весь трафик данного узла для ведения статистики и для моделирования действий стороны защиты. Подверглись изменению модули, отвечающие за работу Sockets, для моделирования механизмов атаки. Ядра агентов были выполнены на основе сопрограмм, так как это удобно для реализации протоколов взаимодействия, на которых основана командная работа агентов. Остальные модули выполнены как обработчики сообщений от ядра и внешней среды.

Пример пользовательского интерфейса среды моделирования показан на рис. 5.

На основном окне визуализации (рис. 5, справа вверху) отображается компьютерная сеть для проведения моделирования. Окно управления процессом моделирования (рис. 5, внизу посередине) позволяет просматривать и менять параметры моделирования. Для отображения текущего состояния команд агентов служат соответствующие окна состояний (рис. 9, сверху посередине). Можно открывать различные окна, характеризующие функционирование (статистические данные) отдельных хостов, протоколов и агентов, например, на рис. 9 внизу слева отображено окно функционирования одного из хостов.

Компьютерная сеть для проведения моделирования состоит из трех подсетей:
- подсеть защиты, на K узлах которой устанавливаются агенты защиты и в которой можно выделить защищаемые серверы;
- промежуточная подсеть, состоящая из N хостов с типовыми клиентами, генерирующими нормальный трафик;
- подсеть атаки, включающая M узлов с демонами и один узел с мастером (характеристики подсетей

задаются соответствующими параметрами моделирования).

На примере моделирования процессов реализации распределенных атак «отказ в обслуживании» проведен ряд экспериментов, показавших эффективность предлагаемого подхода и возможность его использования для исследования перспективных механизмов защиты и анализа уровня защищенности проектируемых сетей. В дальнейшем планируется реализация большего количества механизмов защиты и атак, а также исследование механизмов внутрикомандного взаимодействия агентов.

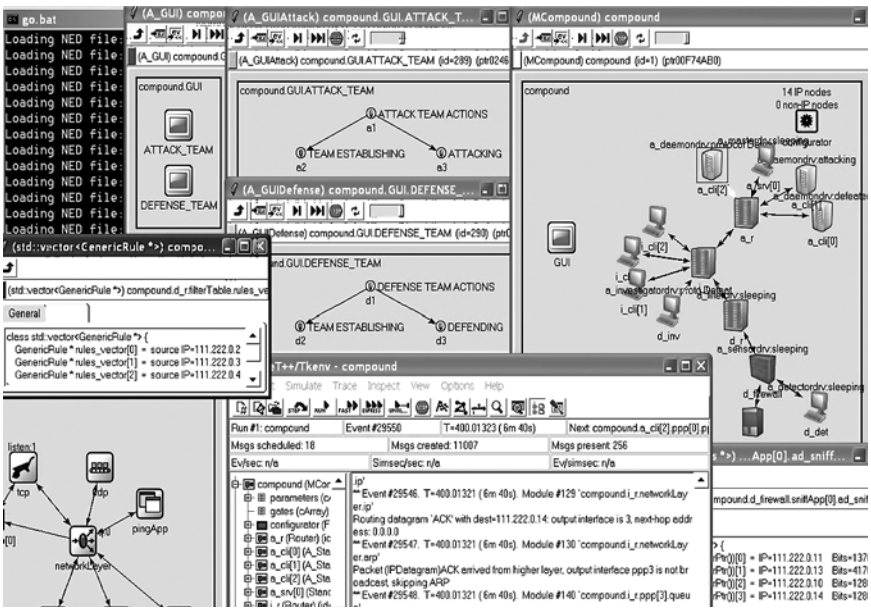

Рис. 5. ***Пример пользовательского интерфейса среды моделирования***

Анализ безопасности компьютерных систем и сетей

В настоящее время актуальной задачей в области компьютерной безопасности является обнаружение уязвимостей и оценка уровня защищенности компьютерных систем и сетей. Для решения данной задачи служит специальный класс систем, называемых системами анализа защищенности (САЗ). Современные САЗ предназначены для проверки защищаемой системы на соответствие заданной системной конфигурации и политике безопасности, определения уязвимостей для их дальнейшего устранения и уменьшения рисков, вызванных наличием данных уязвимостей.

Проводимые в СПИИРАН исследования в области анализа безопасности компьютерных систем и сетей посвящены разработке моделей, архитектур и прототипов интеллектуальных компонентов анализа уязвимостей и определения уровня защищенности, которые позволят расширить функциональные возможности существующих САЗ как за счет активных методов, реализуемых на основе имитации действий злоумышленников, так и на основе пассивных методов, осуществляемых посредством анализа журналов регистрации событий, настроек программного и аппаратного обеспечения и т. п. Важной особенностью предлагаемых решений является возможность их применения на различных этапах жизненного цикла компьютерных систем, включая этапы проектирования и эксплуатации.

Подход к построению САЗ на основе активных методов базируется на механизме автоматического генерирования и выполнения распределенных сценариев атак с учетом разнообразия целей и уровня знаний злоумышленника [20]. В основе рассматриваемого подхода – комплексное использование основанных на экспертных знаниях моделей злоумышленника, вероятностных моделей компьютерной сети, генерации комплекса сценариев атак и оценки уровня защищенности.

Система анализа защищенности, использующая предложенный подход, предназначена для функционирования на различных этапах жизненного цикла компьютерной сети, включая этапы проектирования и эксплуатации. На этапе проектирования САЗ оперирует с моделью анализируемой компьютерной сети, которая базируется на заданной спецификации компьютерной сети и реализуемой политики безопасности. На этапе эксплуатации САЗ взаимодействует с реальной компьютерной сетью.

Результаты генерируемых атак позволяют определить уязвимости, построить трассы (графы) возможных атак, выявить «узкие места» в компьютерной сети, вычислить различные метрики безопасности, которые могут быть использованы для оценки общего уровня защищенности компьютерной сети (системы) и ее компонентов.

Полученные результаты обеспечивают также выработку обоснованных рекомендаций по устранению выявленных «узких мест» и усилению защищенности системы. На основе данных рекомендаций пользователь САЗ вносит изменения в конфигурацию реальной сети или в ее модель, а затем, если необходимо, повторяет процесс анализа уязвимостей и оценки уровня защищенности. Таким образом, требуемый уровень защищенности компьютерной сети (системы) обеспечивается на всех этапах ее жизненного цикла.

Обобщенная архитектура предлагаемой системы активного анализа защищенности представлена на рис. 6. Модуль реализации модели злоумышленника обеспечивает определение уровня умений злоумышленника, выбор стратегии поведения и определение цели атаки. Хранилище данных и знаний состоит из базы знаний (БЗ) об анализируемой системе, базы правил функционирования САЗ и базы данных (БД) эксплоитов (программ реализации атак). Хранилище содержит данные и знания, используемые злоумышленником для планирования и реализации атак. База знаний об анализируемой системе содержит знания и данные об архитектуре

и конкретных параметрах компьютерной сети, которые необходимы для генерирования сценариев и выполнения атак (например, для конкретного хоста эти данные могут задавать тип и версию операционной системы, список открытых портов, запущенные приложения и т. п.). Эти данные обычно могут быть получены злоумышленником при реализации этапа разведки с помощью программных средств и методов социальной инженерии.

База правил функционирования содержит мета- и низкоуровневые правила вида «ЕСЛИ-ТО», определяющие действия САЗ на различных уровнях детализации. Метаправила определяют сценарии атак на высоком уровне, низкоуровневые – атакующие действия на основе внешней базы уязвимостей. Часть «ЕСЛИ» каждого правила содержит цель действия и (или) условия его выполнения. Цель выбирается согласно типу сценария и высокоуровневой цели, определяемой метаправилом более высокого уровня. Условия выполнения действия сравниваются с данными, хранимыми в базе знаний об анализируемой системе. Часть «ТО» содержит идентификатор атаки, которая может быть выполнена при данных условиях, и (или) ссылку на эксплоит. Низкоуровневые правила данной базы создаются на основе одной из баз данных уязвимостей, например OSVDB (Open Source Vulnerability Database). База данных эксплоитов содержит программы реализации действий злоумышленника и параметры их использования.

Модуль генерирования комплекса сценариев производит выбор данных об анализируемой системе из хранилища данных и знаний, генерирует комплекс сценариев атаки с использованием базы правил функционирования САЗ, осуществляет контроль выполнения комплекса сценариев и его изменение в процессе работы, а также выполняет обновление данных об анализируемой системе.

Модуль выполнения этапа сценария осуществляет выбор следующего действия и эксплоита, прогнозирует ожидаемый отклик анализируемой компьютерной сети, реализует запуск эксплоита и распознавание отклика сети. В случае взаимодействия с компьютерной сетью генерируется реальный сетевой трафик.

При работе с моделью анализируемой системы обеспечивается два уровня эмуляции атак:

- на первом уровне каждое низкоуровневое действие представляется идентификатором, описывающим тип атаки и (или) используемый эксплоит, а также параметрами атаки;
- на втором (низком) уровне каждое действие представляется множеством сетевых пакетов.

Сетевой интерфейс обеспечивает:

- в случае работы с моделью анализируемой системы – передачу идентификаторов и параметров атак (или сетевых пакетов в случае моделирования с большей степенью детализации), а также получение результатов атак и реакции системы;
- при взаимодействии с реальной компьютерной сетью – передачу, захват и анализ сетевого трафика.

Модуль определения уровня защищенности использует разработанную таксономию метрик безопасности. Это основной модуль, который фиксирует сценарии атак в виде трасс прохождения различных компонентов системы, производит подсчет метрик безопасности, основываясь на информации о результате атак, и определяет «узкие места».

Модуль обновления баз данных и баз знаний использует открытые базы данных уязвимостей (например, OSVDB) и транслирует их в базу правил функционирования САЗ на низком уровне.

Окно интерфейса пользователя одного из разработанных прототипов САЗ (рис. 7) разделено на четыре функциональные части.

Левая верхняя часть (Network Model) отображает в виде дерева заданную системным администратором конфигурацию анализируемой компьютерной сети. Данная конфигурация изменяется в процессе выполнения атак (например, отображается остановка сетевого сервиса), и возвращается в исходное состояние после окончания каждого сценария. Правая верхняя часть (Malefactor's Network Model) отображает в виде дерева конфигурацию компьютерной сети так, как ее представляет себе злоумышленник. Изначально она пуста и заполняется в процессе выполнения атак. Эта конфигурация может иметь различия с заданной администратором конфигурацией, так как злоумышленник, как правило, обладает не всей информацией о сети. Например, злоумышленник может узнать, что в сети функционирует 4 компьютера, а не 5, как задано в спецификации. Левая нижняя часть (Attack Tree) представляет собой сгенерированный системой сценарий выполнения атаки. Правая нижняя часть содержит три вкладки: журнал выполняемых действий и результатов атак (лог), обнаруженные уязвимости и трассы успешных атак, вычисленные метрики безопасности.

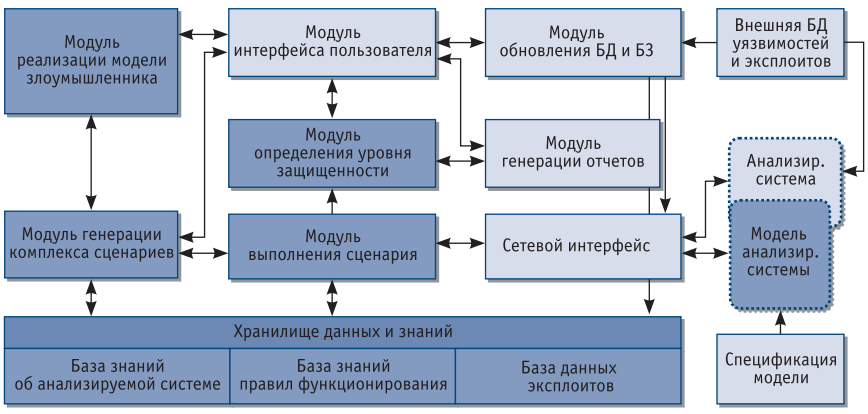

Рис. 6. ***Обобщенная архитектура системы активного анализа защищенности***

В рамках работ по созданию архитектур, моделей и прототипов, осуществляющих *пассивный анализ уязвимостей*, ставится задача разработки компонентов, выполняющих следующие функции:

- захват сетевого трафика и его анализ;
- анализ учетных записей (выявление учетных записей со слабыми паролями, количество пользователей с правами администратора, активен ли пользователь guest и т. п.);
- анализ установленного программного обеспечения (определение версий ПО и наличие программных коррекций);
- анализ журналов регистрации событий (операционной системы и приложений);
- анализ состояния файловой системы (проверка прав доступа и целостности файлов);
- обнаружение несоответствий с заданной политикой безопасности и конфигурацией сети;
- в случае обнаружения последних – генерирование сигнала тревоги;
- определение уровня защищенности и выдача рекомендаций по его повышению;
- коррекция обнаруженных уязвимостей и отклонений от заданной политики безопасности;
- создание отчетов.

Архитектура компонентов пассивного анализа уязвимостей состоит из единой консоли управления и программных агентов, функционирующих на каждом устройстве сети (рис. 8).

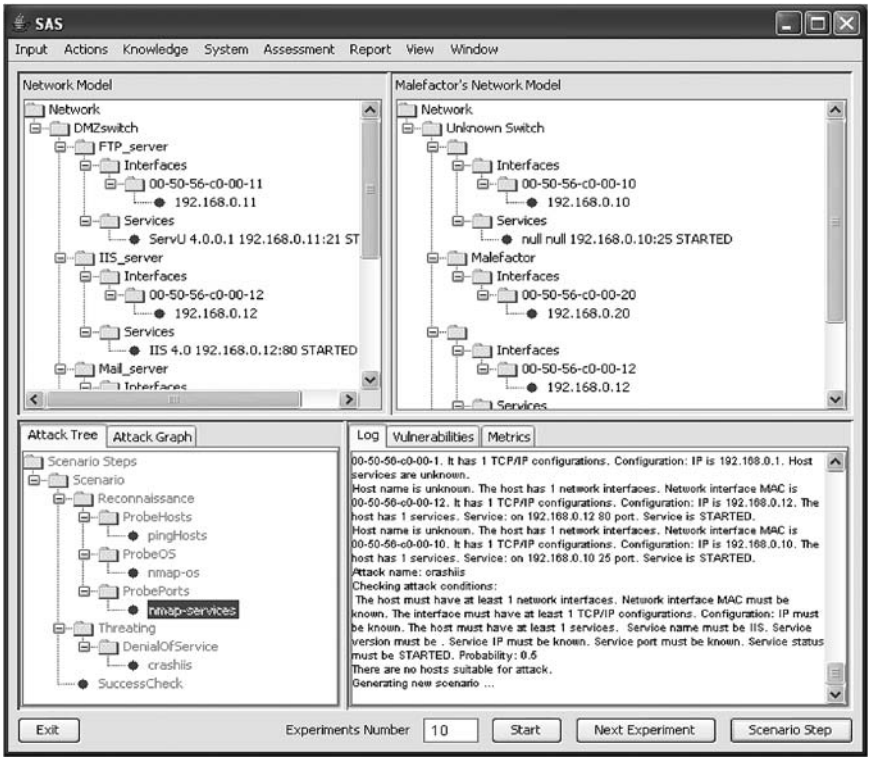

Рис. 7. ***Окно прототипа САЗ***

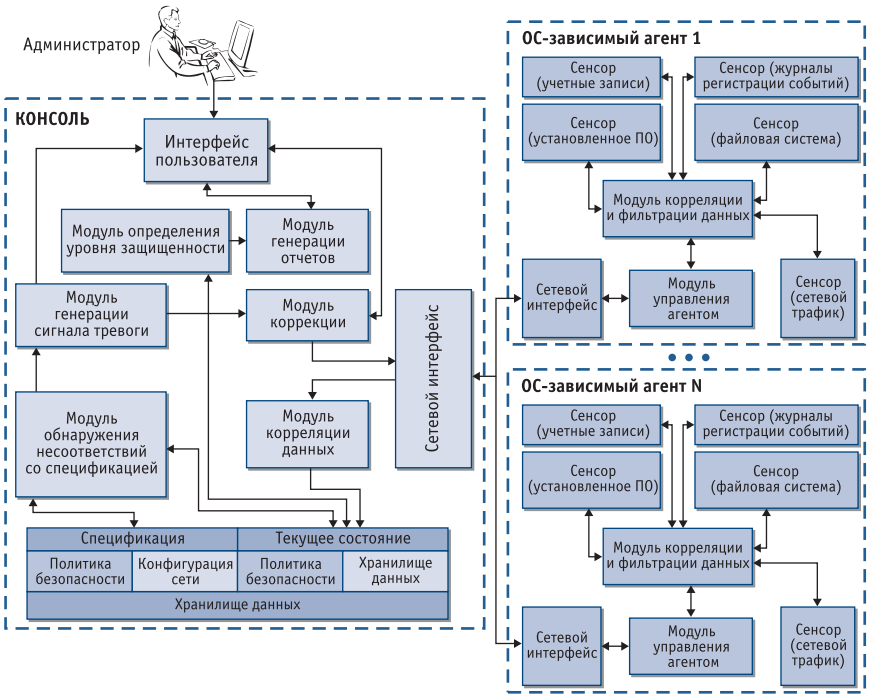

Рис. 8. ***Обобщенная архитектура компонентов пассивного анализа уязвимостей***

Введение злоумышленников в заблуждение

Для защиты информационных ресурсов компьютерных сетей необходимо не только предупреждать, блокировать, обнаруживать действия нарушителей и реагировать на них, но и отвлекать злоумышленников от основных целей, заманивая на ложные информационные объекты, производить сбор информации об их приемах, тактике и мотивации, осуществлять идентификацию и разоблачение атакующих. Для выполнения этих подзадач могут быть использованы так называемые ложные информационные системы (ЛИС), называемые также системами-имитаторами, обманными системами или системами-ловушками [21].

ЛИС представляют собой программно-аппаратные средства обеспечения информационной безопасности, реализующие функции сокрытия и камуфляжа защищаемых информационных ресурсов, а также дезинформации нарушителей.

На основании анализа работ в указанной области в качестве основных функций, которые должны быть реализованы в перспективных ЛИС, можно выделить следующие:

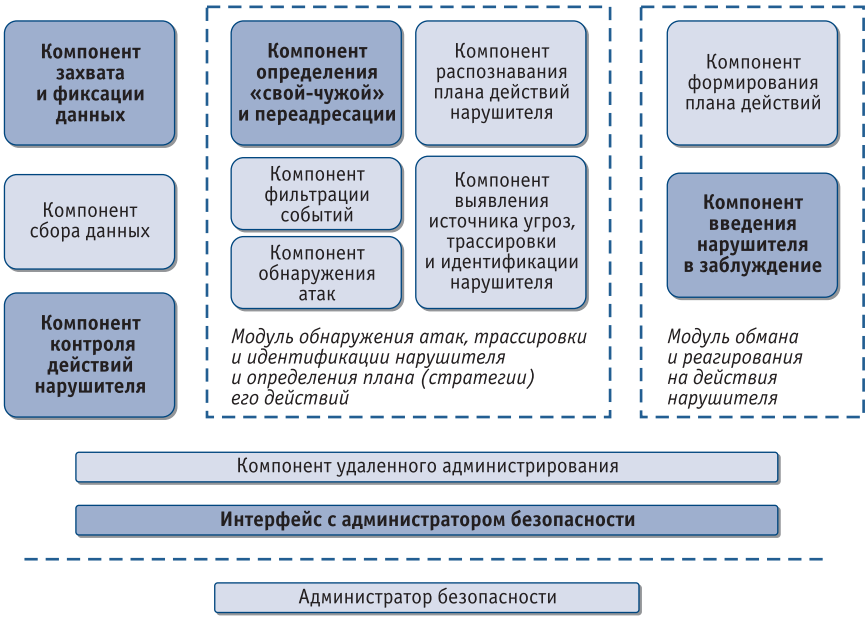

Рис. 9. ***Обобщенная функциональная структура ЛИС***

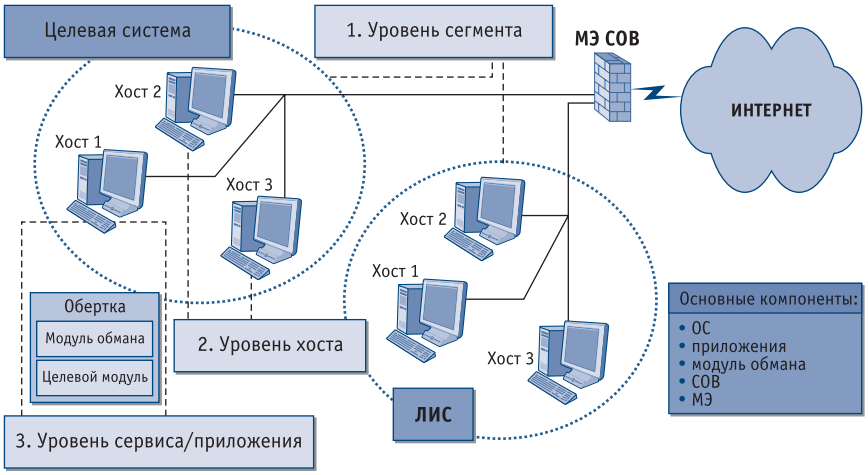

Рис. 10. ***Обобщенная архитектура ЛИС и реализуемые уровни введения в заблуждение***

- захват данных («прослушивание» сетевого трафика и фиксация данных для последующего анализа);
- сбор и объединение данных от различных программных и аппаратных компонентов компьютерной сети, в частности сенсоров, межсетевых экранов, систем обнаружения вторжений, маршрутизаторов и др.;
- определение «свой-чужой» и переадресация несанкционированных запросов на ложные компоненты;
- фильтрация событий (для автоматической отбраковки несущественных и фокусировки на значимых событиях);
- обнаружение действий нарушителя;
- выявление источника угроз, трассировка и идентификация нарушителя (определение типа, квалификации и др.);
- обеспечение невозможности использования скомпрометированных компонентов (ресурсов) для атаки или для нанесения вреда другим системам после проникновения нарушителя в ЛИС;
- распознавание плана (стратегии) действий нарушителя; контроль его действий и реагирование на них – оповещение администратора о компрометации, блокирование действий нарушителя и др.;
- формирование плана действий компонентов ЛИС по имитации целевой информационной системы;
- заманивание и обман нарушителя (привлечение внимания, сокрытие реальной структуры защищаемой системы и ресурсов, камуфляж, дезинформация) за счет эмуляции сетевых сегментов, серверов, рабочих станций, в том числе – передаваемого трафика, и их уязвимостей, автоматическое реагирование на действия нарушителя, в том числе – оповещение администратора;
- удаленное администрирование, документирование, ввод сигнатур, профилей и другое (обеспечивает централизованное управление ЛИС, основанную на правилах безопасности реакцию системы, подготовку отчетов и анализ тенденций), обеспечение интерфейса с администратором безопасности.

В институте проводятся исследования в области разработки и совершенствования моделей и алгоритмов реализации различных функций ЛИС, в частности по выявлению источника угроз, трассировке и профилированию нарушителя, идентификации плана действий нарушителя, формированию плана действий компонентов ЛИС по имитации целевой информационной системы, сокрытию реальной структуры защищаемой системы и дезинформации злоумышленника и др.

Обобщенная функциональная структура разрабатываемой перспективной ЛИС представлена на рис. 9. Жирным шрифтом выделены базовые компоненты ЛИС.

В общем случае предлагаемая ЛИС может обеспечить три уровня введения в заблуждение нарушителя (рис. 10):

- уровень сегмента (основных компонентов целевой системы) – на данном уровне ЛИС имитирует защищаемую целевую систему в целом, и при обнаружении атаки злоумышленник перенаправляется с целевой системы на компоненты ЛИС;
- уровень хоста – данный уровень предполагает размещение компонентов ЛИС, имитирующих отдельные хосты, в компьютерной сети целевой системы;

- уровень сервиса/приложения – в рамках хоста целевой системы каждое приложение/сервис формируется следующим образом: целевой модуль сервиса/приложения вместе с модулем обмана «вкладывается в обертку», в режиме санкционированного использования при вызове сервиса/приложения управление передается целевому модулю, при обнаружении несанкционированного обращения управление передается модулю обмана.

Для исследования возможностей перспективных ЛИС разработаны их прототипы и ведутся эксперименты с различными компонентами этих систем [21].

Заключение

В работе рассмотрены перспективные направления исследований в области компьютерной безопасности, выполняемые в Санкт-Петербургском институте информатики и автоматизации РАН (СПИИРАН). Из-за ограниченности объема статьи детально охарактеризованы лишь некоторые их них:

- информационно-безопасные системы, основанные на политиках;
- интеллектуальные механизмы защиты информации, в том числе многоагентные технологии;
- моделирование киберпротивоборства в сети Интернет;
- анализ безопасности компьютерных систем;
- обманные (ложные) информационные системы.

Представленные в настоящей работе результаты были разработаны коллективом ученых СПИИРАН. Отраженные в работе исследования проведены или выполняются в настоящее время в рамках ряда научно-исследовательских работ: проекта шестой рамочной программы Европейского сообщества, гранта Российского фонда фундаментальных исследований, программы фундаментальных исследований отделения информационных технологий и вычислительных систем Российской академии наук, проекта, поддерживаемого Федеральным Министерством образования и науки Германии, проектов МНТЦ и Европейского офиса аэрокосмических исследований и разработок, а также ряда других проектов. ■

ЛИТЕРАТУРА

1. Юсупов Р. М. Информационная безопасность и ее влияние на важнейшие компоненты национальной безопасности. В кн. «Наука и безопасность России», М.: Наука, 2000.

2. Юсупов Р. М., Заболотский В. П. Научно-методологические основы информатизации. СПб.: Наука, 2000.

3. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под ред. И. В. Котенко. СПб.: ВУС, 2000.

4. Gorodetski V., Kotenko I., Skormin V. (Editors). Computer Network Security. Lecture Notes in Computer Science, Vol. 3685, Springer Verlag, 2005.

5. Policy-based Security Tools and Framework. http://www.positif.org.

6. Tishkov A., Kotenko I. Security Checker Architecture for Policy-based Security Management // Lecture Notes in Computer Science, Springer-Verlag, V.3685. The Third International Workshop «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-05). 2005.

7. Gorodetski V., Karsayev O., Kotenko I., Khabalov A. Software Development Kit for Multi-agent Systems Design and Implementation // Lecture Notes in Artificial Intelligence, Vol. 2296, Springer Verlag, 2002. P.121–130.

8. Gorodetski V., Kotenko I. Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // A.Wespi, G. Vigna, L. Deri (Eds.). Recent Advances in Intrusion Detection. Fifth International Symposium. RAID 2002. Zurich, Switzerland. October 2002. Proceedings. Lecture Notes in Computer Science, V. 2516.

9. Kotenko I. Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated Distributed Attacks on Computer Networks // Lecture Notes in Artificial Intelligence, Springer-Verlag, V. 2691. 2003.

10. Gorodetsky V., Kotenko I., Karsayev O. The Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. The International Journal of Computer Systems Science & Engineering, № 4, 2003.

11. Kotenko I. V. Modeling and Simulation of Attacks for Verification of Security Policy and Vulnerability Assessment // Seventh International Symposium on Recent Advances in Intrusion Detection. RAID 2004. Abstract and Poster sessions. Sophia-Antipolis, French Riviera, France, 2004.

12. Котенко И. В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Защита информации. Конфидент, № 2–3, 2004.

13. Kotenko I., Ulanov A. Multiagent modeling and simulation of agents' competition for network resources availability // Second International Workshop on Safety and Security in Multiagent Systems. SASEMAS'05. Utrecht, The Netherlands. 2005.

14. Kotenko I. V., Ulanov A. V. Agent-based simulation of DDOS attacks and defense mechanisms // Journal of Computing, V. 4, Issue 2, 2005.

15. Городецкий В. И., Котенко И. В., Карсаев О. В. Интеллектуальные агенты для обнаружения атак в компьютерных сетях // КИИ-2000. VII Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. М.: Издательство Физико-математической литературы, 2000.

16. Gorodetski V., Karsayev O., Khabalov A., Kotenko I., Popyack L., Skormin V. Agent-based Model of Computer Network Security System: A Case Study // Lecture Notes in Computer Science, V. 2052. 2001.

17. Laskov P., Schafer C., Kotenko I. Intrusion detection in unlabeled data with one-class Support Vector Machines // Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2004), Lecture Notes in Informatics (LNI), No. 46, Dortmund, Germany, July 2004.

19. Gorodetski V., Karsayev O., Kotenko I., Samoilov V. Multi-Agent Information Fusion: Methodology, Architecture and Software Tool for Learning of Object and Situation Assessment // The 7th International Conference on Information Fusion. Proceedings. Stockholm, Sweden. June 28 – July 1, 2004.

20. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science, Springer-Verlag, V. 3685. The Third International Workshop «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-05). 2005.

21. Котенко И. В., Степашкин М. В. Использование ложных информационных систем для защиты информационных ресурсов компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2005, №. 1.

22. Tarakanov A., Skormin V. and Sokolova S. Immunocomputing: Mathematical Basis and Applications. Springer, New York, 2003.

23. Gorodetski V., Popyack L., Skormin V., Samoilov V. SVD-based Approach to Transparent Embedding Data into Digital Images. Proceedings of the International Workshop «Mathematical Methods, Models and Architectures for Computer Network Security». Lecture Notes in Computer Science, V. 2052, Springer Verlag, 2001.