4. *Freeman E.* A3: An Agent Oriented Program. Architecture for Multi-agent Constraint Satisfaction Problem. *In Proceedings of the 2d International Conference on Tools for Artificial Intelligence*, IEEE Computer Press, 1990, pp.630-640.
5. *Guarino N.* Some organizing principles for a unified top-level ontology. *Working Notes of AAAI Spring Symposium on Ontological Engineering*, Stanford, 1997.
6. *Jennings N., Paratin P., Jonson M.* Using Intelligent Agents to Manage Business Processes. *In Proceedings of the First International Conference and Exhibition "The Practical Application of Intelligent Agents and Multi-Agent Technology"*, 22-24 April, 1996, London, UK, pp.345-376.
7. *Marik V., Pechoucek M., Stepankova O.* Proplant: Application of the multi-agent paradigm in production planning. *In Proceedings of Conference on Intelligent Information Processing*, Beijing, 2000
8. Proceeding of the Fifth International Conference *"The Practical Application of Intelligent Agents and Multi-agent Technology" (PAAM'2000)*, London, UK, 2000.
9. *Sandholm T.* An Implementation of Contract Net Protocol Based on Marginal Cost Calculations. *In Proceedings 11th AAAI*, pp.256-262, 1993.
10. *Smith R., Davis R.* Framework for Cooperation in Distributed Problem Solving. *IEEE Transactions on Systems, Man and Cybernetics, SMC-11*, pp.61-70, 1981.
11. *Smith R.* The Contract Net Protocol: High-Level Communication and Control in a Distributed Problem Solver, *IEEE Transactions on Computer*, vol. 29(12), pp.1104-1113, 1980.
12. *Conry S., Kuwabara K., Lesser V., and Meyer R.* Multistage negotiation for distributed constraint satisfaction. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-21 (6), Nov.1991.
13. *Wooldridge M., Jennings N.R.* Agent theories, Architectures, and Languages: A Survey. *Intelligent Agents. ECAI-94 Workshop on Agent Theories, Architecture and Languages.* Amsterdam, 1994.

УДК 681.3.053:681.32:007.5:519.71

И.В. Котенко, О.И. Карсаев

ИСПОЛЬЗОВАНИЕ МНОГОАГЕНТНЫХ ТЕХНОЛОГИЙ ДЛЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

1. Введение. В настоящее время в связи с бурным развитием задач распределенной обработки информации и использованием открытых сетей (Интернет), не приспособленных для защищенного обмена информации, вопросы защиты информационных ресурсов в компьютерных системах приобрели исключительную актуальность. Однако сложившееся состояние в области обеспечения безопасности этих систем, в том числе в области построения средств защиты компьютерных сетей, оставляет желать лучшего. Существующие системы защиты информационных ресурсов в компьютерных сетях, 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. [1]

Перспективным подходом к построению комплексных систем защиты информации в компьютерных сетях, позволяющим преодолеть некоторые из перечисленных недостатков, является использование интеллектуальных систем защиты

информации, базирующихся на *технологии многоагентных систем* [2]. Этот подход позволяет по сравнению с традиционными методами существенно повысить эффективность механизмов защиты информации, в том числе их оперативность, адекватность, отказоустойчивость, устойчивость к деструктивным действиям, гибкость и т.д.

К настоящему времени имеется большое число работ, посвященных созданию интеллектуальных систем защиты информации в компьютерных сетях. Для разработки распределенных систем обнаружения атак предлагаются различные инновационные подходы, например генетические алгоритмы [3], нейронные сети [4, 5], иммунные системы [6, 7].

В последнее время опубликовано большое количество исследовательских работ, в которых для проектирования систем обнаружения атак применяется многоагентный подход [8-17]. Однако хотя эти работы представлены относительно недавно, в них используется упрощенный вариант архитектуры агентов и кооперативного поведения. Среди общих недостатков предлагаемых решений необходимо выделить следующее: 1) реализуемые агенты выполняют, как правило, лишь задачи предобработки информации и не являются интеллектуальными, что существенно снижает качество механизмов защиты; 2) большинство систем базируются на иерархических структурах с одним центральным менеджером, что значительно ухудшает их собственную безопасность и надежность; 3) решается только одна из множества задач защиты информации – задача обнаружения вторжений, игнорируются все другие задачи; 4) недостаточное внимание уделяется вопросам кооперации агентов и использованию преимуществ многоагентных архитектур.

Задачей комплексного исследования, проводимого авторами настоящей статьи, является применение подхода, позволяющего преодолеть указанные недостатки.

В работе затрагиваются вопросы разработки архитектуры многоагентной системы защиты информации (СЗИ), создания моделей представления распределенных знаний, убеждений и намерений агентов защиты, определения обнаруживаемых СЗИ классов атак и действий агентов по их обнаружению. Описывается один из наиболее распространенных классов атак на компьютерные сети – комбинированная spoofing-атака, рассматриваются механизмы ее обнаружения при использовании СЗИ.

2. Архитектура многоагентной системы защиты информации. Компоненты предлагаемой многоагентной СЗИ (агенты защиты) представляют собой интеллектуальные автономные программы, реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности [2, 18, 19]. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств, операционных систем и приложений, повышая защищенность системы до требуемого уровня.

Предполагается, что агенты распределены по хостам защищаемой сети, специализированы по типам решаемых задач и взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений (рис.1). В явном виде отсутствует “центр управления” семейством агентов – в зависимости от сложившейся ситуации ведущим может становиться любой из агентов, реализующий функции кооперации и управления. В случае необходимости агенты могут клони-

роваться и прекращать свое функционирование. В зависимости от ситуации (вида и количества атак на компьютерные сети, наличия вычислительных ресурсов для выполнения функций защиты) может генерироваться несколько экземпляров агентов каждого класса. Они адаптируются к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт [18, 20].

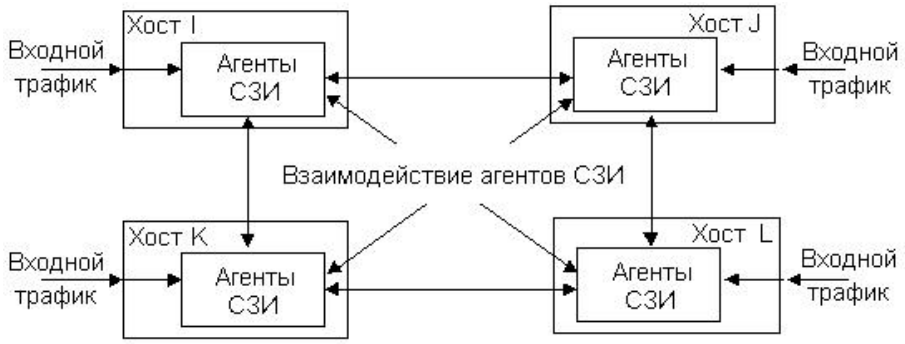


Рис.1. Обобщенное представление архитектуры СЗИ

Компонент архитектуры СЗИ, ассоциированный с некоторым хостом сети, может состоять из одного или нескольких экземпляров агентов каждого типа, специализированного на решение некоторой подзадачи общей задачи. В частности, выделяются следующие *базовые агенты* [2]: 1) агенты-демоны, выполняющие предобработку информации; 2) агенты обнаружения вторжения (агенты выявления атак и несанкционированного доступа); 3) агенты идентификации и аутентификации; 4) агенты разграничения доступа; 5) агенты подавления атакующего, ответственные за "преследование", идентификацию и обезвреживание атакующего; 6) агенты, которые осуществляют оценку возможного повреждения и восстановления целостности данных при несанкционированном доступе; 7) агенты криптографической и стеганографической защиты информации; 8) агенты обучения; 9) мета-агенты, ответственные за координацию работы СЗИ.

3. Модели представления распределенных знаний, убеждений и намерений агентов. Предлагаемые модели функционирования агентов СЗИ и решения по построению распределенной базы знаний предусматривают, что каждый агент “знает”, какие задачи он должен решать сам и к какому агенту он должен адресовать свой запрос на информацию или на решение подзадачи с целью получения такой информации, если это вне его компетенции. Сообщения одних агентов представляются в форме и терминах, понятных другим агентам.

Одним из наиболее перспективных подходов к структуризации распределенных баз знаний такого типа является использование онтологий, характеризующих предметные знания сами по себе, вне связи с конкретными структурами их представления, алгоритмами вывода в них или эвристиками, т.е. вне связи с тем, что привносится в задачу при ее формализации и программной реализации [21].

Как и для любой другой предметной области, онтология области защиты информации представляет собой описание частично упорядоченного множества понятий, которые должны использоваться соответствующими агентами защиты. Кроме отношения частичного порядка, на узлы этой структуры накладываются и

другие отношения, свойственные предметной области. Это различного рода ограничения, правила, количественные и качественные отношения, связывающие понятия защиты и т.п. Данная онтология определяет подмножество понятий, которые используют различные агенты СЗИ для кооперативного решения поставленных задач. Каждый агент использует определенный фрагмент общей онтологии предметной области.

Специализация каждого агента СЗИ отражается подмножеством узлов онтологии. Некоторые узлы онтологии могут быть общими для пары или большего количества агентов. Обычно только один из этих агентов обладает детально структурированным описанием этого узла. Именно этот агент является обладателем соответствующего фрагмента базы знаний. В то же время некоторая часть онтологических баз знаний является общей для всех агентов, в том числе и для мета-агента, и именно эта часть знаний является тем фрагментом, который должен играть роль общего контекста (общих знаний) СЗИ.

Предлагаемая формальная конструкция для представления распределенных знаний СЗИ предназначена для поддержки целостности распределенных баз знаний агентов, обеспечения возможности непротиворечивой модификации знаний отдельных агентов защиты, согласованного клонирования агентов и генерации агентов новых типов. Она используется в качестве базиса для декомпозиции общей задачи защиты информации на частные подзадачи и как основа применяемой методологии объектно-ориентированного проектирования многоагентной СЗИ.

Наиболее важными *“измерениями” общей онтологии* понятий и задач защиты информации являются (рис.2) [22]: 1) “предметная область агентов защиты”; 2) “цепочка понятий “сообщение – событие – атака””; 3) “типы частных атак”; 4) “значимые события”; 5) “агенты защиты – классы атак – значимые события”; 6) “функционирование агентов защиты”; 7) “сценарии атак – кооперация агентов”.

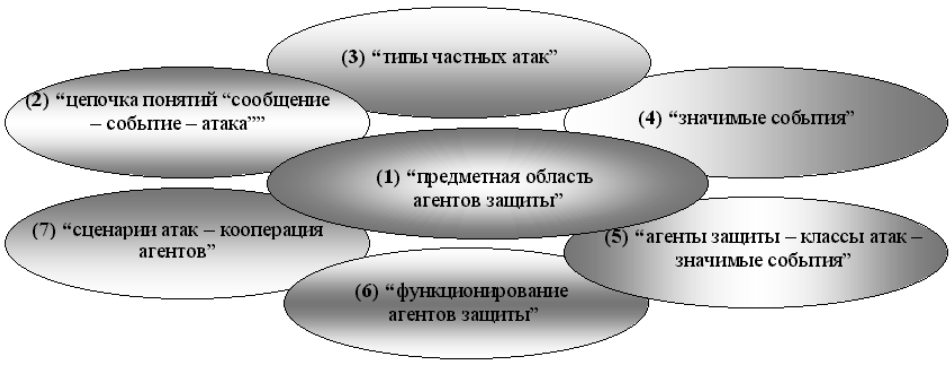


Рис.2. “Измерения” общей онтологии защиты информации

Онтология “предметная область агентов защиты” (рис.3) задает функциональности и области ответственности каждого агента защиты, а также этапы жизненного цикла проектирования компонентов СЗИ.

Онтология “цепочка понятий “сообщение – событие – атака”” определяет обработку сообщений в процессе выполнения агентами СЗИ задач защиты от нижнего до верхнего уровня обобщения и классификации. В качестве базовых частич-

но упорядоченных понятий выбраны: трафик сообщений, событие, значимое событие, критическое событие, данные аудита, паттерн, правила, сценарий деятельности, сценарий и атака.

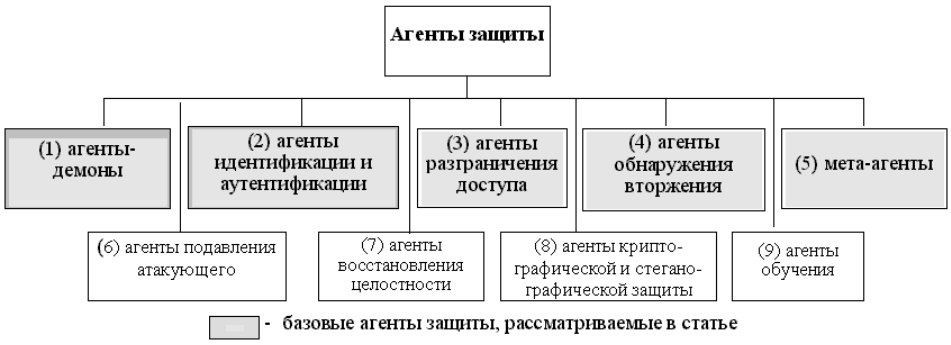


Рис.3. Верхний уровень онтологии "предметная область агентов защиты"

Онтология "типы частных атак" (рис.4) характеризует частные виды атак и упорядочивает классы сетевых и локальных атак. В соответствии с этой онтологией СЗИ обнаруживает восемь *типовых классов частных программных атак*: 1) анализ сетевого трафика; 2) сканирование сети; 3) подмена доверенного объекта сети; 4) внедрение ложного объекта сети; 5) отказ в обслуживании; 6) неавторизованный доступ с удаленного хоста посредством подбора пароля; 7) неавторизованное получение привилегий доступа; 8) удаленный запуск приложений.

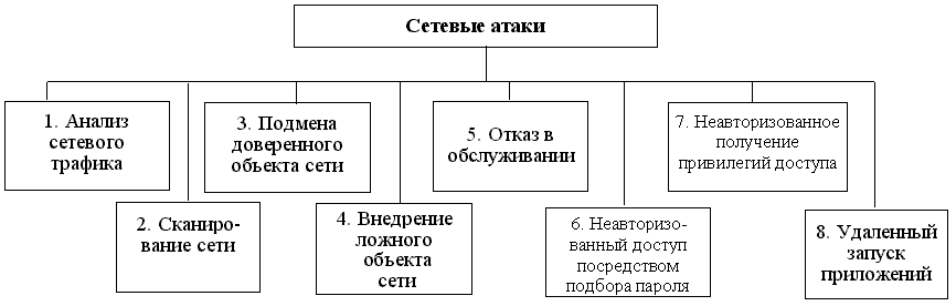


Рис.4. Верхний уровень онтологии "типы частных атак"

Онтология "значимые события" определяет иерархию уровней обработки событий, соответствующие сетевые протоколы и службы, команды операционной системы и приложения. Она играет важную роль для многоуровневой обработки данных, выполняемой агентами защиты. Иерархия используемых уровней обработки событий для протоколов Интернет представлена в табл.1. Значимое событие можно определить как событие, существенное для обнаружения атак (в частности) и для реализации процессов защиты информации (в целом). События можно разделить на сетевые и локальные. По существу сетевые события представляют собой прибытие на хост пакета трафика, а локальные – реализацию на хосте некоторой

операции (действия). Значимые события для конкретного сеанса работы пользователя находятся, как правило, на самом верхнем уровне обработки.

Таблица 1

Иерархия уровней значимых событий

N	Уровень	Основные протоколы / Команды / Службы
5	Операционная система и приложения	Команды операционной системы и выполняемые приложения
4	Прикладной (Application)	FTP, SFTP, TFTP; TELNET; SMTP, POP3, IMAP4; NNTP; HTTP; NFC; r-service;X-Windows; SNMP; DNS; RPC; RIP
3	Транспортный (Transport)	TCP; UDP; RIP, EGP, BGP, OSPF
2	Сетевой (Network)	IP; ICMP, IGMP; ARP, RARP
1	Канальный (Channel)	Ethernet; Token Ring; FDDI; Frame Relay; SMDS; ATM; Gigabit Ethernet; X.25; ISDN; PPP

Онтология "агенты защиты – классы атак – значимые события" задает области ответственности агентов обнаружения вторжения. Эта онтология фиксирует иерархию уровней обработки событий, отображенную на классы агентов обнаружения вторжения. Взаимосвязь понятий онтологий "агенты защиты – классы атак – значимые события" и **"**предметная область агентов защиты" показана на рис.5.

Онтология "функционирование агентов защиты" определяет, каким образом агенты защиты должны реализовывать обнаружение атак, защиту от них и противодействие им.

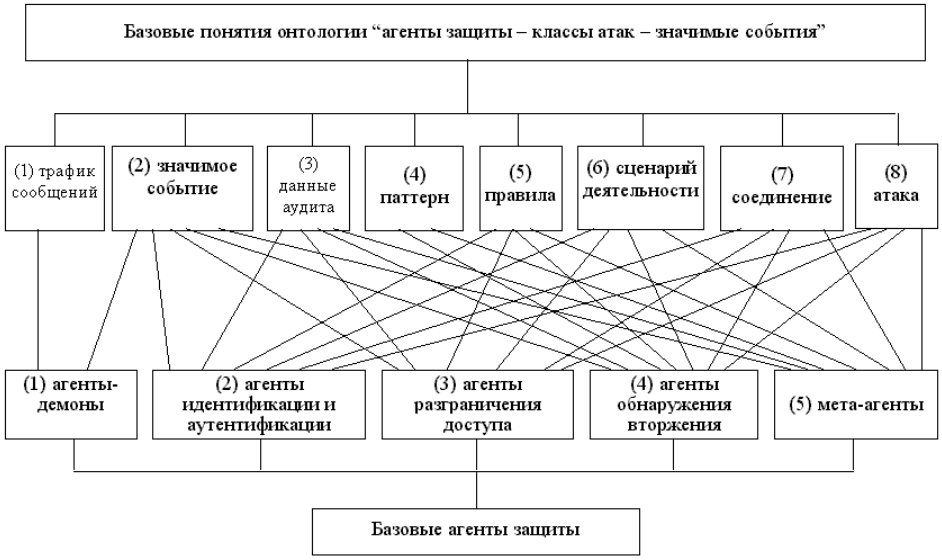


Рис.5. Взаимосвязь понятий онтологий "агенты защиты – классы атак – значимые события" и "предметная область агентов защиты"

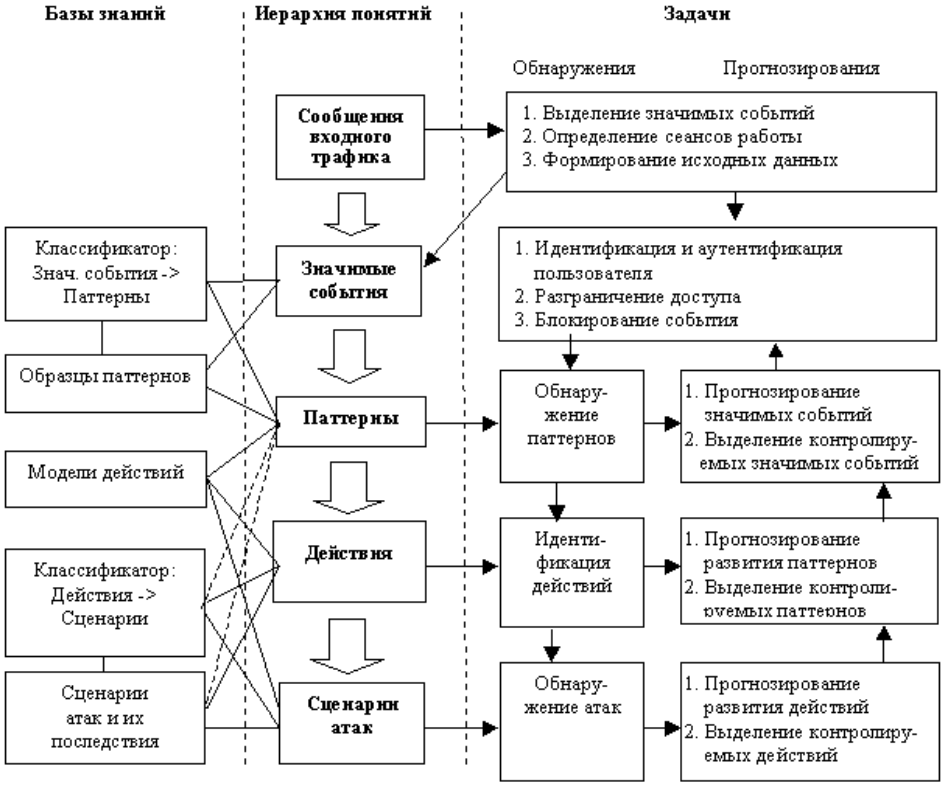


Рис.6. Фрагмент онтологии "функционирование агентов защиты"

Фрагмент этой онтологии, соответствующий задаче обнаружения атак по их сигнатурам (паттернам), представлен на рис.6.

Онтология "сценарии атак – кооперация агентов защиты" задает сложные комбинированные сетевые и локальные атаки, отображенные на сценарии взаимодействия и кооперации агентов защиты.

Распределенная база знаний СЗИ структурируется в соответствии с онтологией предметной области защиты информации, которая определяет в том числе классы атак и действия агентов по их предупреждению, обнаружению и противодействию.

Согласно онтологии "сценарии атак – кооперация агентов защиты" по признаку сложности обнаружения атак и привлекаемым агентам обнаружения, выделено три класса возможных комбинированных программных атак:

1) атака реализуется в рамках одного сеанса работы пользователя;

2) атака реализуется в процессе последовательности нескольких сеансов работы различных пользователей с одним хостом;

3) атака имеет распределенный характер (отдельные действия одного сценария атаки направлены на различные хосты) и реализуется в течение нескольких сеансов с нескольких хостов.

Согласно онтологии "функционирование агентов защиты" задается упорядочение процессов обработки данных в процессе защиты информации, в том числе

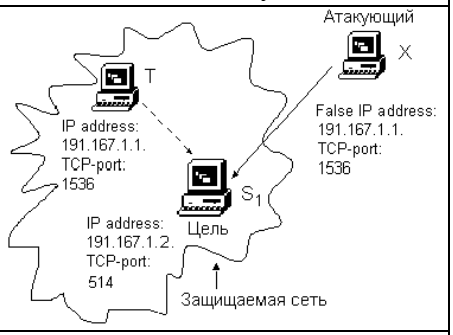
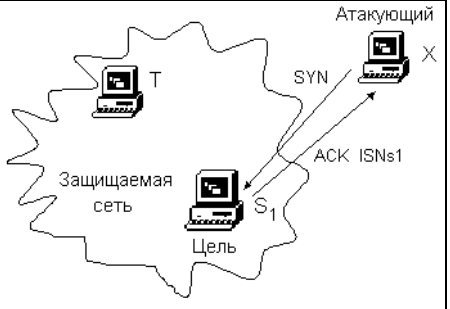
определяются соответствующие базы знаний агентов защиты, справочники понятий, иерархия базовых понятий, задачи защиты, форматы исходных и промежуточных данных и результатов.

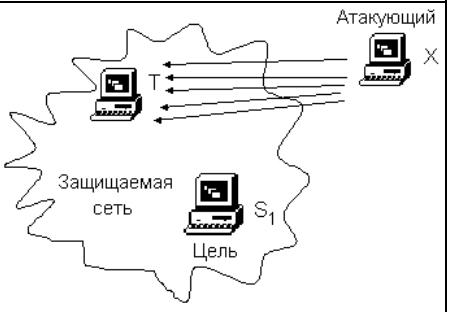
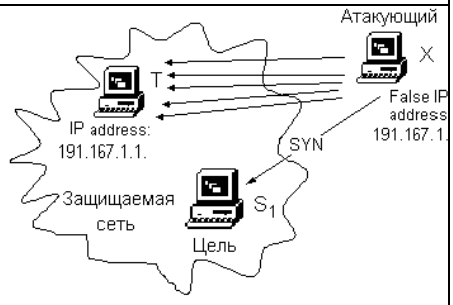
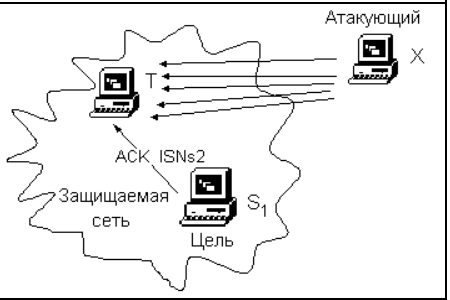
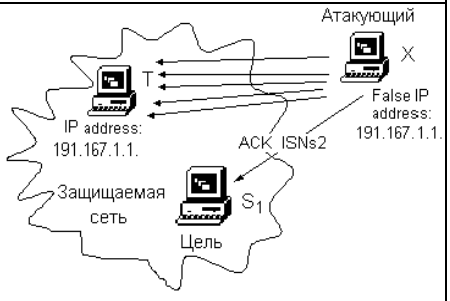
4. Пример распределенной атаки и действия агентов защиты по ее обнаружению. Для иллюстрации предлагаемой многоагентной технологии защиты рассмотрим пример комбинированной spoofing-атаки и возможных действий агентов СЗИ. *Спуфинг* – тип сетевой атаки, основанной на подмене адресов IP-пакетов. Для его осуществления используются два уровня значимых событий: сетевой (IP) и транспортный (TCP). На сетевом уровне происходит подмена адресов IP-пакета, а на транспортном – подбор начального номера последовательности TCP-сегментов и задание портов адресации. Конечным результатом спуфинга является возможность посылки данных (в том числе выполняемых команд) в выбранный злоумышленником порт атакуемого хоста. Спуфинг обычно используется как первая часть плана по несанкционированному получению прав администратора атакуемого компьютера.

Примем, что в сети существует доверительный хост T, пользователи которого имеют доступ к хосту S_1, а X – это хост злоумышленника. Для доступа к S_1 злоумышленник осуществляет имитацию хоста T, обращаясь от его имени к S_1, тем самым “притворяясь” хостом, которому “доверяет” система-жертва. Описание комбинированной spoofing-атаки дано в табл.2. Описание реализуемых действий, используемых агентов, паттернов и значимых событий комбинированной spoofing-атаки представлено в табл.3.

Таблица 2

Описание комбинированной spoofing-атаки

Описание	Иллюстрация
Спуфинг-атака – злоумышленник имитирует хост T, обращаясь от его имени к хосту S_1 . *Цель злоумышленника* – “притвориться” хостом, которому "доверяет" хост-жертва.	
[.] X определяет IP-адрес T (например, методом социальной инженерии). 1. X легальным образом устанавливает связь с S_1 и получает начальный номер ISNs1 соединения "X – S_1". Этот номер необходим для того, чтобы вычислить начальный номер ISNs2 соединения "S_1 – T" . Начальный номер последовательности носит не случайный характер, а изменяется по строго определенному закону. Поэтому, зная начальный номер последовательности одного соединения, можно вычислить начальный номер последовательности	

другого соединения.	
2. X временно выводит из строя T, используя атаку “отказ в обслуживании” (DoS), например, направленным штормом запросов (SYN-flooding), делая это для того, чтобы в дальнейшем не дать T послать S_1 пакет о том, что соединение от имени T (на самом деле инициированное X) не было запрошено, иначе S_1 закроет соединение, установленное X .	
3. X инициирует связь с S_1 от имени T (в заголовке IP-пакетов в поле отправителя сообщения проставляется адрес T) и вычисляет начальный номер ISNs2 соединения "S_1 – T": X → S_1: SYN(ISNx), (обратный адрес: T) .	
[.] S_1 шлет ответный сигнал T с подтверждением ISNx и своим начальным номером ISNs2 : S_1 → T: SYN(ISNs2), ACK(ISNx).	
4. X, вычисливший ISNs2, отвечает вместо T : X → S_1: ACK(ISNs2), (обратный адрес: T). Если защита отсутствует или не срабатывает, то X получает одностороннюю связь с выбранным портом S_1 и может “дистанционно управлять” S_1, но он должен посылать подтверждения S_1 о непреходящих к нему данных, увеличивая каждый раз на единицу значение ISNs2.	

Примечания: [.] – действия, выходящие за рамки рассматриваемого сценария атакующего или относящиеся к действиям атакуемых хостов.

Таблица 3

Описание действий, используемых агентов, паттернов и значимых событий комбинированной spoofing-атаки

Действия злоумышленника	**Задействуемые агенты и их действия**	**Паттерны**	**Значимые события (в форме сообщений tcpdump)**
1. X устанавливает связь с S_1 и получает начальный номер ISNs1 последовательности "X – S_1"	Агенты граничного хоста и хоста S_1. Агенты обнаружения S_1 фиксируют попытку соединения без дальнейшего продолжения сеанса работы со стороны X	Адрес отправителя находится за пределами внутренней (защищаемой) сети (не всегда “срабатывает”, так как атакующий может задать адрес источника в пределах защищаемой сети – тогда справедливо правило, приведенное ниже) Адрес хоста источника находится в защищаемой сети, но (по сообщению граничного хоста) пакет пересек границу сети извне В трехшаговой последовательности установления соединения (“рукопожатия”) отсутствует пакет подтверждения (жирным выделены наиболее показательные паттерны): 4:00:00.259810 187.102.1.1.1057 > 191.167.1.2.21:. ack 1 win 8576 (DF)	1)4:00:00.083238 187.102.1.1.1057 > 191.167.1.2.21: S 1484414:1484414(0) win 8192 <mss 536,nop,nop,sackOK> (DF) 2) 4:00:00.250587 191.167.1.2.21 > 187.102.1.1.1057: S 3037133697:3037133697(0) ack 1484415 win 9112 <mss 536> (DF)
2. X выводит из строя T DoS- атакой, например, штормом запросов (SYN-flooding)	Агенты хоста T и (или) граничного хоста. Агенты обнаружения T фиксируют атаку DoS со стороны X и передают соответствующую информацию агентам защиты других хостов (в том числе и на S_1)	Адрес отправителя находится за пределами внутренней (защищаемой) сети (не всегда “срабатывает”, так как атакующий может задать адрес источника в пределах защищаемой сети – тогда справедливо правило, приведенное ниже) Адрес хоста источника находится в защищаемой сети, но (по сообщению граничного хоста) пакет пересек границу сети извне Большое число SYN-пакетов (несколько десятков - сотни), направленных на хост-жертву за малый промежуток времени (доли секунды). При этом адрес отправителя – ложный (spoofed). Атака продолжается в течение действий 2 - 4	1) 4:01:14.212003 spoofed.ip.one.1053 > 191.167.1.1.23: S 322286:322286(0) win 8192 <mss 536, nop, nop, sack-OK> (DF) 2) 4:01:14.598008 spoofed.ip.one.1054 > 191.167.1.1.23: S 322286:322286(0) win 8192 <mss 536, nop, nop, sack-OK> (DF) 3) 4:01:14.975522 spoofed.ip.one.1055 > 191.167.1.1.23: S 322286:322286(0) win 8192 <mss 536, nop, nop, sack-OK> (DF) … n) 4:01:14.975732 spoofed.ip.one.1055 > 191.167.1.1.23: S 322286:322286(0) win 8192 <mss 536, nop, nop, sack-OK> (DF)
3. X инициирует связь с S_1 от имени T и вычисляет начальный номер ISNs2 соединения "S_1 – T"	Агенты хоста T (если удалось нейтрализовать атаку SYN-flooding), граничного хоста и S_1. Агенты обнаружения S_1 фиксируют попытку соединения со стороны T.	Хосту S_1 поступил начальный пакет синхронизации с хоста T, но T находится под атакой DoS Хосту T поступил пакет с подтверждением TCP-соединения с хоста 4:02:00.250587 191.167.1.2.21 >191.167.1.1.1057:S 3037133697:3037133697(0) ack 1484415 win 9112 <mss 536> (DF), но начального пакета синхронизации с хоста T не передавалось Адрес хоста источника находится в защищаемой сети, но (по сообщению	1) 4:02:00.083238 191.167.1.1.1057 > 191.167.1.2.21: S 1484414:1484414(0) win 8192 <mss 536,nop,nop,sackOK> (DF) 2) 4:02:00.250587 191.167.1.2.21 > 191.167.1.1.1057: S 3037133697:3037133697(0) ack 1484415 win 9112 <mss 536> (DF)

	Имея данные об атаке на T, они делают предположение о spoofing-атаке со стороны X.	граничного хоста) пакет пересек границу сети извне	
4. X, вычисливший ISNs2, отвечает вместо T на сообщение хоста S_1 к хосту T, содержащее подтверждение ISNx с начальным номером ISNs2	Агенты граничного хоста и S_1 Агенты обнаружения S_1 фиксируют подтверждение со стороны T. Теперь они уже однозначно определяют spoofing-атаку со стороны X.	Адрес хоста источника находится в защищаемой сети, но (по сообщению граничного хоста) пакет пересек границу сети извне Если X не смог сразу правильно определить ISNs2+1 на хост S поступает несколько подтверждений с хоста T с неверным ISN	1) 4:02:00.259810 191.167.1.1..1057 > 191.167.1.2.21: . ack 3037133698 win 8576 (DF)

Заключение. Основное внимание в данной работе было уделено архитектуре и моделям представления распределенных знаний, убеждений и намерений агентов многоагентной СЗИ, а также описанию одной из широко используемых атак на компьютерные сети (распределенной комбинированной spoofing-атаки) и рассмотрению действий агентов защиты по ее обнаружению.

Базовые черты предлагаемого подхода: 1) расширяемая и адаптивная многоагентная архитектура СЗИ, элементами которой являются интеллектуальные агенты; 2) центральное внимание уделяется защите от атак, состоящих из последовательностей операций, распределенных по множеству хостов и проводимых в течение длительного времени; 3) обеспечение безопасности и робастности СЗИ (обработка событий, важных с точки зрения защиты информации, распределена среди множества хостов; функции управления СЗИ распределены между мета-агентами различных хостов; в зависимости от ситуации мета-агент любого хоста может выполнять роль мета-агента сети.

Описанные “измерения” онтологии защиты информации в телекоммуникационных сетях отражают взгляд авторов на сложность модели предметной области защиты и функционирования СЗИ, а также на разработанный программный прототип СЗИ, который позволяет представить преимущества, недостатки и проблемы применения технологии интеллектуальных агентов для обеспечения интегрированной защиты информации в телекоммуникационных сетях.

В рамках будущих работ предполагается сосредоточить внимание на задаче моделирования сетевых атак и задаче обучения агентов для обеспечения адаптации к новым видам атак и расширяемости системы.

ЛИТЕРАТУРА

1. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под ред. И.В. Котенко. СПб.: ВУС, 2000.
2. *Городецкий В.И., Котенко И.В.* Архитектура базовых агентов многоагентной системы защиты информации в компьютерных сетях // Известия ТРТУ, 2. 2000. С.38-51.

3. *Crosbie M., Spafford G.* Applying Genetic Programming to Intrusion Detection // Proceedings of the AAAI Fall Symposium on Genetic Programming. Cambridge, 1995. Menlo Park, CA: AAAI Press, 1995.
4. *Bonifácio J. et al.* An Adaptive Intrusion Detection System Using Neural Networks // Proceedings of the IFIP World Computer Congress "Security in Information Systems" (IFIP-SEC `98). Viena, Austria, August/September 1998.
5. *Bonifácio J et al.* Neural Networks Applied in Intrusion Detection Systems // Proceedings of the IEEE World Congress on Computational Intelligence (WCCI `98). Anchorage, AK, May 1998.
6. *Forrest S., Hofmeyr S., Somayaji A.* Computer Immunology // Communications of the ACM, 40, 10, 1997, P.86-96.
7. *Somayaji A., Hofmeyr S., Forrest S.* Principles of a Computer Immune System // Proceedings of the 1997 New Security Paradigms Workshop. 1998. P.75-82.
8. *White G., Fisch E., Pooch U.* Cooperating Security Managers: A Peer-Based Intrusion Detection System // IEEE Network, 10, 1, 1996. P.20-23.
9. *Karjoth G., Lange D., Oshima M.* A Security Model for Aglets // IEEE Internet Computing, August 1997. P.68-77.
10. *Balasubramaniyan J. et al.* An Architecture for Intrusion Detection Using Autonomous Agents. Coast TR 98-05. West Lafayette, IN: COAST Laboratory, Purdue University, 1998.
11. *Helmer G., Wong J., Honavar V., Miller L.* Intelligent Agents for Intrusion Detection // Proceedings of the 1998 IEEE Information Technology Conference, Environment for the Future. Syracuse. NY: IEEE, 1998. P.121-124.
12. *Asaka M., Okazawa S., Taguchi A., Goto S.* A Method of Tracing Intruders by Use of Mobile Agents // INET'99, June 1999.
13. *Queiroz J., Carmo L., Pirmez L.* Micæl: An Autonomous Mobile Agent System to Protect New Generation Networked Applications // Proceedings of Second International Workshop on the Recent Advances in Intrusion Detection (RAID'99). West Lafayette, Indiana, USA. 1999.
14. *Conner M., Patel C., Little M.* Genetic Algorithm/Artificial Life Evolution of Security Vulnerability Agents // Proceedings of 3rd Annual Symposium on Advanced Telecommunications & Information Distribution Research Program (ATIRP). Army Research Laboratory Federal Laboratory. February 1999.
15. *Jacobs S., Dumas D., Booth W., Little M.* Security Architecture for Intelligent Agent Based Vulnerability Analysis // Proceedings of 3rd Annual Symposium on Advanced Telecommunications & Information Distribution Research Program (ATIRP). Army Research Laboratory Federal Laboratory. February 1999. P.447-451.
16. *Jansen W., Karygiannis T.* Mobile Agents and Security // NIST Special Publication 800-19, September 1999.
17. *Jansen W., Mell P., Karygiannis T., Marks D.* Mobile Agents in Intrusion Detection and Response // Proceedings of the 12th Annual Canadian Information Technology Security Symposium, Ottawa, Canada, June 2000.
18. *Gorodetski V., Kotenko I., Popyack L., Skormin V.* Integrated Multi-Agent Information Security System: Mechanisms of Agents' Operation and Learning // Proceedings of PAAM' 2000. Manchester. UK. Practical Application Company Ltd. 2000. P.151-154.
19. *Gorodetski V., Kotenko I., Skormin V.* Integrated Multi-Agent Approach to Network Security Assurance: Models of Agents' Community // Information Security for Global Information Infrastructures. IFIP TC11 Sixteenth Annual Working Conference on Information Security / Ed. by S.Qing, J.H.P.Eloff. Beijing. China. 2000. P.291-300.
20. *Городецкий В.И., Котенко И.В., Карсаев О.В.* Многоагентная система защиты информации в компьютерных сетях: механизмы обучения и формирования решений для обнаружения вторжений // Проблемы информатизации, № 2, 2000. С.67-73.

21. Guarino N. Formal ontology, conceptual analysis and knowledge representation // *Int. J. Human-Computer Studies*, No.43, 1995.
22. *Gorodetski V., Kotenko I., Karsaev O.* Framework for Ontology-based Representation of Distributed Knowledge in Multiagent Network Security System // Proceedings of the 4th World Multi-conference on Systems, Cybernetics and Informatics (SCI-2000), Vol. III: "Virtual Engineering and Emergent Computing". Orlando, USA, July 2000. P.52-58.
23. *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. С.771-779.

УДК 007:681.51

Е.Н. Филинов, А.В. Бойченко, Ю.Ф. Тельнов, А.В. Данилов[1]

ПОСТРОЕНИЕ ПРОФИЛЕЙ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ЗАПАСАМИ НА БАЗЕ КОНКРЕТИЗАЦИИ И РАЗВИТИЯ ЭТАЛОННОЙ МОДЕЛИ OSE/RM

1. Введение. В последние годы значительно усилился интерес пользователей к построению корпоративных информационных систем (КИС), в которых реализуются современные достижения технологий искусственного интеллекта. Общая тенденция в развитии новых информационных технологий состоит в их интеллектуализации. Интеллектуальные технологии реализуются системами, основанными на представлении и обработке знаний.

В современные КИС как их органическая часть встраиваются приложения, поддерживающие многоаспектный анализ данных, принятие решений в сложных ситуациях, управление корпоративными знаниями, экспертные системы, распознавание "образов" и обучение.

Между этими приложениями и средой КИС необходимо иметь программные средства промежуточного слоя (middleware), обеспечивающие функционирование базы знаний, логический вывод на базе знаний, естественно-языковый пользовательский интерфейс для формирования запросов к БЗ и взаимодействие с внешней средой.

Для реинжиниринга бизнес-процессов и для построения КИС, основанных на знаниях, требуются инструментальные комплексы разработки динамических интеллектуальных систем для решения задач управления и моделирования. В качестве примера таких средств могут быть названы системы ReThink и G2 фирмы Gensym (США), лидера на мировом рынке систем этого класса.

2. Задача построения профилей интеллектуальных КИС. Встраивание в КИС компонентов, обладающих функциями поддержки интеллектуальных технологий, следует с самого начала ориентировать на соблюдение стандартов открытых информационных систем. Это позволит обеспечить независимость, по возможности, от применяемых вычислительных и телекоммуникационных платформ,

[1] Работа выполнена при поддержке РФФИ, грант №98-01-00978.