УДК 004.94, 004.056

В.В. КАЗИМИР, А.А. СЕРАЯ

МЕТОД ПОСТРОЕНИЯ МОДЕЛЕЙ ИНФОРМАЦИОННЫХ АТАК

Анотація. *Розглянуті та проаналізовані існуючі підходи до побудови формальних моделей інформаційних атак. Сформульовані основні вимоги до моделей інформаційних атак. Запропоновано метод побудови моделей інформаційних атак на основі управляючих Е-мережевих переходів та багатоагентного керування з урахуванням сформульованих вимог.*
Ключові слова: *атака, моделювання, модель інформаційної атаки, управляюча Е-мережа, агент, багатоагентне керування.*

Аннотация. *Рассмотрены и проанализированы существующие подходы к построению формальных моделей информационных атак. Сформулированы основные требования к моделям информационных атак. Предложен метод построения моделей информационных атак на основе управляющих Е-сетевых переходов и многоагентного управления с учетом сформулированных требований.*
Ключевые слова: *атака, моделирование, модель информационной атаки, управляющая Е-сеть, агент, многоагентное управление.*

Abstract. *Existing approaches to the modelling the information attacks are considered and analysed. The basic requirements for information attacks model are formulated. Taking into account the formulated requirements the method is suggested for construction information attacks models based on control E-nets and multi-agent management.*
Key words: *attack, modelling, information attack model, control E-net, agent, multi-agent control.*

1. Введение

В настоящее время одним из наиболее актуальных направлений научных исследований в области обеспечения информационной безопасности является разработка методов и средств обнаружения атак и защиты от атак на компьютерные системы и сети. В процессе такой разработки необходимо постоянно проводить научно-исследовательские работы, включающие предварительное изучение и детальную проработку возможных вариантов реализации информационных атак. Как правило, эти работы осуществляются с использованием моделей, позволяющих воспроизвести необходимые свойства и характеристики информационной атаки, а также провести оценку уровня ее опасности для компьютерной системы (КС). Модели позволяют более точно определить эффективность существующих и разрабатываемых средств защиты от моделируемых информационных атак.

Созданные в настоящее время модели информационных атак могут быть классифицированы по следующим базовым критериям [1]:

– возможность расширения модели (модели с фиксированным количеством параметров и их значений, расширяемые модели с возможностью добавления новых параметров и их значений);

– возможность учёта в модели последовательности выполняемых действий в информационной атаке;

– уровень детализации модели (модели низкого, среднего и высокого уровня детализации).

Широкое распространение получила формализованная модель информационной атаки на основе деревьев атак, разработанная Б. Шнайером [2]. Деревья атаки представля-

ют собой концептуальные диаграммы, которые описывают угрозы системе и возможные атаки, направленные на их реализацию. В качестве основополагающей конструкции здесь выступает иерархическое дерево $G=(L,E)$, где $L=\{l_i\}$ – множество вершин дерева, $E=\{e_s\}$, $E\subset L^2$ – множество дуг дерева. Каждая вершина дерева G ассоциируется с определённым действием нарушителя, при этом корень дерева обозначает конечную цель информационной атаки, реализация которой может нанести значительный ущерб АС. Таким образом, на графе G имеется возможность составить множество возможных путей $Gp=\{gp_i\}$, где каждый путь gp_i представляет собой последовательность дуг $(e_1,e_2,...,e_n)$ вида $e_i=(l_i,l_j)$, $l_i,l_j\in L$. При этом конечная вершина дуги l_i одновременно является начальной вершиной дуги l_{i+1}. В качестве начальной вершины пути могут выступать листья дерева G, а в качестве конечной вершины – корень дерева. Модель деревьев атак Шнайера имеет несколько важных преимуществ:

– модель можно применять для описания атак на любые системы информационного или физического характера;

– благодаря наличию числовых значений у вершин и ребер модель предоставляет возможность для введения оценок каждого шага по некоторым критериям, например, по времени выполнения, числу операций, оценочной стоимости и т.д. Последовательность шагов может быть оценена на основании критериев каждого шага;

– расширение модели атаки осуществляется путём добавления новых элементов во множества вершин и дуг деревьев, описывающих атаку;

– имеется возможность моделирования сложных информационных атак, предусматривающих несколько вариантов реализации.

Данная модель имеет ряд недостатков, к которым следует отнести:

– в качестве основополагающей конструкции для моделирования атаки используется дерево, что налагает некоторые ограничения на структуру графического представления модели. Наличие циклов также создаёт определённые трудности при работе с этой моделью;

– модель атаки не включает в себя параметры среды АС, при которых возможна реализация моделируемой атаки;

– в модели отсутствуют средства, обеспечивающие динамическое моделирование.

В [3] предложен формальный метод моделирования атак, который представляет собой расширение и уточнение модели на основе дерева атак. Вводятся два атрибута: время жизни (отражает временные зависимости между этапами атаки) и степень уверенности (характеризует вероятность достижения цели атаки при достигнутых подцелях). Однако данная модель имеет те же недостатки, что и на основе дерева атак.

Модель графов атак [4] также основана на расширении модели деревьев атак. Графы атак являются специализированным средством для описания атаки. Узлы графа представляют не концептуальные действия, а узлы сети, процессы программы, конфигурационные файлы, участки кода и т.д. Модель получила широкое распространение, поскольку она основана на простой и хорошо исследованной математической базе – конечных автоматах, сама достаточно проста и очевидна. Переходы между узлами осуществляются на основе детерминированных правил, при этом может учитываться текущее значение некоторых параметров системы, переменных и т.д. Существующие модели графов хорошо подходят для описания последовательности действий злоумышленника и часто используются для оценки сложности нарушения безопасности информационной системы, а не для моделирования и исследования атак. К недостаткам данных моделей также можно отнести то, что они не содержат механизмов для организации управляемого ветвления и моделирования динамической составляющей атаки.

Модели информационных атак также строят на основе формальных языков и онтологий [5]. Формально, онтология – дерево, а угроза представляется последовательностью символов. Последовательности рассматриваются как слова формального языка, специфицируемого посредством некоторой формальной грамматики. Описание обобщенного сценария атаки посредством стохастической грамматики имеет следующий вид:

$$GA = \langle V_N, V_T, S, P \rangle, \quad (1)$$

где V_N – множество нетерминальных символов, которые обозначают шаги атаки микроуровня, V_T – множество терминальных символов, которые ставятся в соответствие верхним и промежуточным уровням представления шагов сценария атаки, S – начальный символ сценария атаки, P – множество правил вывода, описывающих операции детализации сценария атаки посредством замены символов. Каждая замена осуществляется с заданной вероятностью:

$$\alpha_i \xrightarrow{P_{ij}} \beta_{ij}, \quad i = 1,...,n_i, \quad i = 1,...,k, \quad (2)$$

где α_i – нетерминальный символ, β_{ij} – строка из терминальных и нетерминальных символов.

Характерно, что концептуальная модель информационной атаки на основе формальных языков и онтологий во многом аналогична рассмотренной выше модели, разработанной Б. Шнайером. Модель также представляется в виде графовой структуры и может быть расширена путём добавления новых элементов во множества терминальных и нетерминальных символов, а также посредством расширения правил вывода. Модель может быть представлена как в текстовом, так и в графическом виде. Основным недостатком такой модели информационной атаки является отсутствие параметра, характеризующего уязвимость КС, на основе которой выполняется действие нарушителя.

Среди других вариантов формализованных моделей информационных атак следует выделить модель, базирующуюся на математическом аппарате модифицированных сетей Петри, представляющих собой обобщенные стохастические сети Петри с задержками специального вида, сдерживающими дугами и взвешенными переходами [6]. Введение понятия задержанного перехода расширяет область практического применения сетей Петри и делает возможным не только проследить порядок событий, происходящих в системе, но и попытаться смоделировать их динамику. Пространство состояний модели определяется множеством позиций и множеством переменных состояния. Текущее состояние модели, т.е. фаза атаки, описывается расстановкой фишек в позициях сети и конкретными значениями переменных состояния. С переходами рассматриваемой сети Петри связано два события: изменение состояния модели и генерация очередного Ethernet-кадра атакующего воздействия. Содержимое генерируемого кадра определяется текущим состоянием модели.

Модель на основе сетей Петри обладает следующими преимуществами:

– содержит механизмы, необходимые для описания алгоритма действий злоумышленника, включая случайный выбор одной из равноценных альтернатив;

– позволяет описывать динамическую составляющую сетевого трафика атакующего воздействия в виде детерминированных и случайных задержек.

Недостатки данных моделей для исследования атак и проведения экспериментов вытекают из недостатков сетей Петри. Отсутствие условных переходов, разрешающих позиций, набора признаков у меток делает невозможным проведение вычислений и накопление статистики. Кроме того, данный подход ориентирован на моделирование сетевых атак, что не соответствует требованию универсальности методов моделирования.

Особое место в моделировании информационных атак занимает подход, основанный на многоагентных технологиях моделирования. В проводимых исследованиях, выполняемых группой Санкт-Петербургского исследовательского института Российской ака-

демии наук [7], такой подход предполагает, что кибернетическое пространство представляется в виде взаимодействия различных команд программных агентов, воздействующих на компьютерную сеть, а также друг на друга. При этом выделяются как минимум две команды агентов: агенты-злоумышленники и агенты-защиты. Такой подход к организации командной работы агентов базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и учитывает опыт программной реализации многоагентных систем. Данный подход позволяет учитывать сложный динамический характер кибернетического противоборства.

Рассмотренные подходы к моделированию позволяют с разной степенью детализации описать процесс информационной атаки. Модели используют разную математическую базу, но большинство из них основаны на конечных автоматах и представляют атаку как последовательность состояний автомата. Ни одна из моделей не позволяет учесть в комплексе уязвимость, активизируемую атакой, метод её реализации и возможные последствия [1, 8]. Другими словами, вопросы комплексности модели информационной атаки остаются неразрешенными и актуальными. Целью данной статьи является разработка метода построения моделей информационных атак, который исключит указанный выше недостаток и, таким образом, предоставит возможность проектировать и разрабатывать более эффективные комплексы средств защиты КС.

2. Требования к моделям информационных атак

Для эффективного использования в целях исследования вероятных действий нарушителя по отношению к КС разрабатываемая модель информационной атаки должна удовлетворять следующему минимальному набору требований:

– универсальность – позволяет использовать модель для представления различных типов атак, т.е. модель должна быть построена таким образом, чтобы она могла применяться в процессе моделирования как сетевых, так и локальных атак;

– расширяемость – обеспечивает возможность добавления в модель новых характеристик атаки, базирующихся на параметрах модели. Это свойство позволяет исследователю изменять характеристики моделируемой атаки в зависимости от среды КС, в которой она рассматривается;

– формализуемость – свойство, которое указывает на возможность использования математического аппарата при описании параметров модели;

– простота – позволяет эксперту легко воспринимать структуру и способы реализации моделируемой атаки. От этого свойства напрямую зависит, насколько эффективно можно использовать построенную модель;

– многофакторность – даёт возможность учитывать три основных параметра моделируемой информационной атаки: уязвимость, активизируемую атакой, способ реализации атаки и её возможные последствия.

3. Информационная атака как объект моделирования

Атакой на информационную систему называется действие или последовательность связанных между собою действий нарушителя, которые приводят к реализации угрозы путем использования уязвимостей системы. Под уязвимостью принято понимать слабое место КС, на основе которого возможна успешная реализация угрозы. В свою очередь, угроза – это потенциально возможное событие, действие, явление или процесс, который может вызвать нанесение ущерба ресурсу системы [9]. Таким образом, для того чтобы реализовать атаку, злоумышленник моделирует некоторое действие, которое приводит к искомому результату при помощи некоего средства, использующего уязвимости системы.

Информационная атака в общем случае может состоять из трех этапов [10]:

1. Сбор информации – основной этап. На данном этапе выбирается цель нападения, собирается информация о ней (ОС, конфигурация, сервисы), идентифицируются наиболее уязвимые места атакуемой системы, воздействие на которые приводит к нужному результату, выбирается тип реализуемой атаки.

2. Этап реализации атаки. На этом этапе нарушитель получает несанкционированный доступ (НД) к ресурсам тех узлов КС, по отношению к которым осуществляется атака. Если по характеру воздействия атака является активной [11], то данный этап сопровождается также реализацией тех целей, ради которых предпринималась атака. Результатом таких действий может являться нарушение конфиденциальности, целостности и доступности информации. Кроме того, на данном этапе может происходить скрытие источника и факта атаки, так называемое «заметание следов».

3. Этап дальнейшего развития атаки – выполняются действия, которые направлены на продолжение атаки на ресурсы других узлов КС. В случае пассивных атак [11] данный этап является этапом завершения атаки.

На рис. 1 схематично представлены этапы жизненного цикла типовой информационной атаки.

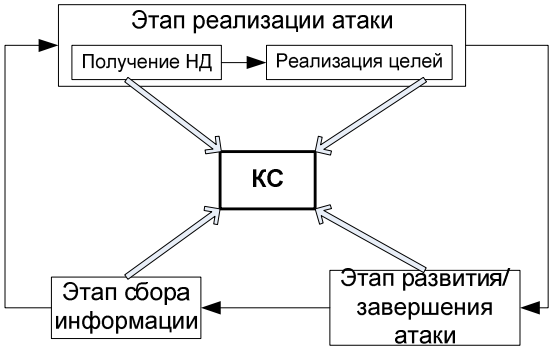

Рис. 1. Жизненный цикл типовой информационной атаки на ресурсы КС

При моделировании информационной атаки необходимо определять ее параметры и характеристики. Основными параметрами атаки являются:

– время действия;

– кратность;

– список уязвимостей, используемых атакой.

Заметим, что моделирование некоторых типов атак, например, «распределенный отказ в обслуживании» – DDoS требует определения дополнительных параметров атаки, таких как [12]:

– тип атаки (семантическая атака (TCP SYN, Incorrect packets, Hard request и др.) или атака типа «грубая сила» – такие как UDP/ICMP flood, smurf/fraggle и др.);

– темп атаки (может быть постоянным или переменным. В последнем случае интенсивность атаки меняется во времени. Изменение темпа может быть нарастающим или колеблющимся);

– влияние на цель атаки (можно выбрать «подрывную» атаку, когда распределенная атака будет осуществляться сразу со всех атакующих узлов, или ухудшающую – число атакующих узлов включается в атаку постепенно. Первый вариант атаки легче обнаружить);

– постоянство набора атакующих узлов (набор может быть постоянным (атакуют одни и те же узлы) или переменным);

– степень автоматизации (автоматическая или автоматизированная).

4. Предлагаемый метод моделирования атак

Учитывая недостатки существующих аналогов, в качестве модели информационной атаки будем использовать управляющие Е-сети (Control E-Nets – CEN) [13, 14], которые представляют собой модификацию Е-сетей и удовлетворяют всем требованиям к моделям атак, описанным выше. Вопросы комплексности модели атаки (учет этапа поиска уязвимостей в модели атаки, метода реализации и развития атаки) будем решать, используя систему многоагентного управления, модули которой работают на принципах интеллектуальных агентов. Каждый агент будем описывать с помощью модели реализации, представленной в ви-

де управляющей Е-сети. Моделирование атак будем производить в специально разработанной среде, в основу которой положены принципы инвариантности к предметной области, уровню моделирования, проводимому эксперименту и уровню подготовленности пользователя. Рассмотрим более детально механизмы работы управляющих Е-сетей, системы многоагентного управления и среду моделирования информационных атак.

4.1. Управляющие Е-сети как функциональная основа моделей атак

Е-сети [15], применение которых было ориентировано только на задачи моделирования, являлись, по сути, автономными, т.е. они не взаимодействовали со своим окружением, в данном случае с КС, на которую направлена атака. В управляющих Е-сетях, исполняющих роль моделей реализации атак, все действия, выполняемые сетью, должны быть согласованы с текущим состоянием объекта атаки и КС. Взаимодействие с объектом атаки осуществляется через соответствующие переменные сети V. Причем для входных дискретных сигналов используется обозначение *DI*, для входных аналоговых сигналов – *AI*, выходных дискретных – *DO*, выходных аналоговых – *AO*, так что $V_I = DI \cup AI$ и $V_O = DO \cup AO$. Дискретные сигналы могут принимать значения из множества $\{0,1\}$, а аналоговые – из множества $\Re$ действительных чисел.

Динамические свойства сети определяются изменением маркировки сети и зависят от значений компонентов управляющего отображения. Маркировкой управляющей Е-сети будем называть вектор $M = (M(p_1), M(p_2), ..., M(p_n))$, где $n = |P_S|$. Позиция $p_i \in P_S$ называется свободной (не содержит метку), если $M(p_i) = 0$, в противном случае, при $M(p_i) = 1$ позиция считается занятой. Для заданной маркировки M множество маркированных позиций будем определять как $P_M = \{p \in P_S \mid M(p) > 0\}$.

Как и в обыкновенных Е-сетях, каждой метке, находящейся в позиции CEN, ставится в соответствие описатель, или кортеж числовых атрибутов, определяющий информационное содержание метки $d_i = (d_{i1}, d_{i2}, ..., d_{ij}, ..., d_{iN})$, где d_{ij} – значение j-го атрибута i-й метки. Во время перемещения меток по сети значения их атрибутов могут изменяться. При выполнении сети метки могут переходить из входных позиций переходов в выходные, изменяя маркировку сети. Поскольку число позиций CEN конечно, то и число возможных ее маркировок также конечно и равно $2^{|P_S|}$, включая начальную маркировку $M_0 = (M_0(p_1), M_0(p_2), ..., M_0(p_n))$.

Множеством достижимости CEN будем называть конечное непустое множество RS всех маркировок, достижимых из начальной маркировки M_0, включая начальную маркировку, т.е. $RS \subseteq M$. Графом достижимости CEN будем называть граф $RG = (RS, G \subseteq RS \times RS)$, включающий в качестве вершин достижимые маркировки. Дуги $g \in G$, где $g = (M_i, M_k)$, показывают, что маркировка M_i непосредственно достижима из маркировки M_k. Структурным компонентом управляющей Е-сети, определяющим ее динамику, является множество управляющих отображений $U = (r, \sigma, \alpha, \tau, z)$, включающее пять функций, ассоциированных с переходами сети:

- r – решающая функция перехода;
- σ – функция готовности перехода к срабатыванию;
- α – функция активации перехода;
- τ – функция задержки перехода;
- z – функция преобразования перехода.

Решающая функция

$$r : P_R \to \{1,2,3,...\} \quad (3)$$

ассоциируется с решающими позициями, которые не содержат меток и управляют работой связанных с ними переходов типов T_X и T_Y посредством вычисления значений так называемых решающих функций $r : P_R \to \{1,2,3,...\}$. Решающая функция может быть рассчитана, в том числе, и с учетом значений атрибутов меток и переменных сети, т.е. $r(q) = f(d_p, V_I), q \in P_S, p \in P_R$.

Значение решающей функции определяет направление перемещения метки при срабатывании перехода. Границы возможных значений решающих функций зависят от числа позиций, инцидентных переходу, по умолчанию $r_0(q) = 1$.

Функция готовности есть предикат

$$\sigma : T \to \{0,1\}, \quad (4)$$

который определяет готовность перехода к срабатыванию: если $\sigma(t) = 0$, то переход $t \in T$ к срабатыванию не готов, иначе, если $\sigma(t) = 1$, то переход t к срабатыванию готов. Каждому типу перехода соответствует свое определение функции готовности. Значение предиката (4) зависит от маркировки простых позиций, инцидентных переходу, а также значения решающей позиции перехода, если таковая имеется, и вычисляется каждый раз при изменении маркировки сети. Таким образом, $\sigma(t) = f[M(p), r]$, если $r \in \{\bullet t, t\bullet\}$ для переходов, где $p \in \{\bullet t, t\bullet\}$. Маркировки входных и выходных позиций, при которых происходит срабатывание переходов, будем называть допустимыми.

Функция активации отсутствует в определении переходов обыкновенной E-сети. Ее использование в CEN вызвано необходимостью учета состояния объекта атаки при определении условий срабатывания перехода дополнительно к анализу допустимой маркировки. Функция активации является предикатом

$$\alpha : T \to \{0,1\}, \quad (5)$$

который вычисляется для каждого перехода и определяет возможность его активации: если $\alpha(t) = 0$, то переход $t \in T$ остается неактивным, иначе, если $\alpha(t) = 1$, то переход t активизируется. При вычислении функции активации учитываются значения входных сигналов сети V_I, т.е. $\alpha(t) = f(DI, AI)$. По умолчанию функция активации равна 1, при этом переход активизируется при любых значениях входных сигналов.

Функция задержки вычисляет время задержки на переходе τ на основании значений атрибутов меток, находящихся в позициях сети, а также значений переменных сети, т.е. $\tau(t) = f(d_p, V_I), p \in P_S$. Как частный случай, по умолчанию может быть задано нулевое время задержки. В общем виде функцию задержки можно представить в виде отображения:

$$\tau : T \to \Re^+, \quad (6)$$

где T – множество переходов сети;

$\Re^+$ – множество положительных действительных чисел, включая ноль.

Функция преобразования перехода

$$z : T \to \delta \quad (7)$$

задает последовательность операций $\delta : \{d_p \bigcup V\} \to \{d_p \bigcup V\}, p \in P_M \bigcap P_t$, которые выполняются над переменными сети и атрибутами меток при перемещении их из входных позиций в выходные позиции перехода. При задании стандартной функции преобразования z_0, которая выполняется по умолчанию, значения атрибутов меток не изменяются.

С учетом управляющих отображений выполнение любого перехода $t \in T$ включает последовательное прохождение следующих четырёх фаз:

• *готовности*, когда переход не находится в задержке и выполнено условие его срабатывания $\sigma(t)=1$, определяемое конкретным типом перехода;

• *активности*, когда наступила фаза готовности и $\alpha(t)=1$;

• *задержки*, когда идет отсчет времени до момента срабатывания перехода; длительность фазы определяется временем задержки на переходе τ(t), которое должно быть вычислено до входа в фазу задержки; состояние позиций перехода до окончания фазы задержки не изменяется;

• *срабатывания*, когда по истечении времени задержки происходит мгновенное изменение маркировки позиций перехода путем перемещения меток из его входных позиций в выходные в соответствии с правилами срабатывания переходов данного типа; одновременно значения атрибутов меток, помещаемых в выходные позиции, изменяются в соответствии с заданной процедурой преобразования перехода.

Традиционные для Е-сетей динамические свойства, определяемые способностью меток перемещаться по позициям и правилами срабатывания переходов, в управляющих Е-сетях расширены за счет возможности динамического изменения управляющих функций переходов. Решающая функция, функции активации, задержки и преобразования являются функциями времени, способными изменяться в процессе выполнения сети.

4.2. Многоагентное управление

Моделирование всех трех этапов атаки будем производить на основе интеллектуальных агентов, взаимодействие которых организовывается в рамках многоагентной системы. Подробно вопросы теории многоагентных систем освещены во множестве работ, которые проанализированы в [16]. Основываясь на этих работах, можно заключить, что в общем случае система с многоагентным управлением может быть рассмотрена, как кортеж

$$S =< W, A, \Omega, \Lambda, K >, \qquad (8)$$

где W – множество объектов управления;

A – множество управляющих агентов;

Ω – множество связей ответственности;

$\Lambda : A \to W$ – локализация агентов по объектам управления;

K – информационные каналы между агентами.

Среди множества известных архитектур агентов наиболее подходящей в плане обеспечения их взаимодействия является InterRap-архитектура [17], которая включает три уровня управления: реактивный, плановый и кооперативный. На уровне планирования выполняется первый этап моделирования атаки – этап сбора информации об объекте моделирования. На этом этапе осуществляется поиск уязвимостей КС, определяется состояние объекта атаки, выбирается тип реализуемой атаки, задаются ее параметры. На реактивном уровне заданные значения начальных параметров атаки корректируются в соответствии с состоянием объекта атаки. На данном уровне выполняются второй и третий этапы атаки – ее реализация и развитие (завершение), которые производятся в цикле по мере поступления данных от уровня планирования. На кооперативном уровне решаются задачи обмена информацией между агентами.

4.3. Построение модели распределенной атаки «Отказ в обслуживании»

Для примера создадим модель информационной распределенной атаки типа отказ в обслуживании (Distributed Denial of Service – DDoS), так как этот класс атак является наиболее критичным по своим последствиям [18]. Целью атаки является нарушение доступности информационных ресурсов с помощью программных средств, расположенных на уже удачно атакованных (скомпрометированных) узлах Internet. Суть атаки состоит в том, что одновременно (либо с указанным интервалом времени) со всех скомпрометированных уз-

лов на объект атаки отправляется большое количество ложных запросов и, как следствие, парализуется работа объекта. Во время проведения атаки DDoS создается иерархичная структура объектов атаки – кластер DDoS. Объект иерархии атаки типа 1 координирует работу объектов иерархии атаки типа 2, которые, в свою очередь, и выполняют атаку.

Имитационная модель атаки DDoS в виде управляющих E-сетей представлена на рис. 2. Модель состоит их трех уровней:

1. На кооперативном уровне происходит организация «команды» атаки: объекты типа 2 посылают сообщение объекту типа 1 о своем состоянии готовности к атаке. В свою очередь, объекты типа 1 сохраняют информацию о состоянии готовности объектов атаки 2, а также распределяют нагрузку между ними и формируют команды для агентов типа 2, в которых указывают способ, темп, интенсивность, время и другие параметры (разд. 3) для проведения атаки. В ходе выполнения атаки объекты типа 1 периодически получают сообщения от объектов типа 2 и таким образом контролируют заданный режим выполнения атаки.

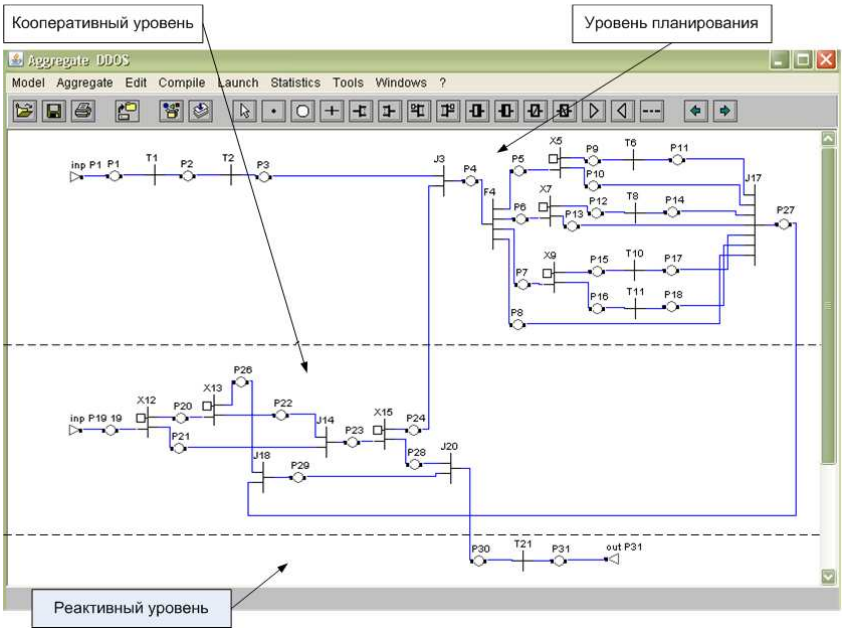

Рис. 2. Имитационная модель атаки DDoS

2. На уровне планирования происходит определение параметров атаки, выполняется поиск уязвимостей объекта атаки, выбирается тип атаки, происходит передача установленных параметров атаки в другие агенты.

3. На реактивном уровне выполняется сама атака DDoS согласно данным, полученным от других агентов.

5. Выводы

Предложен метод построения информационных атак на основе управляющих E-сетей и многоагентного управления. Использование данного метода позволяет создавать модели на основе простых, легко воспринимаемых конструкций для представления различных типов атак. Благодаря использованию механизма управляющих E-сетей, метод позволяет учитывать текущее состояние КС и объекта атаки во время моделирования – обеспечивается динамическое моделирование. Кроме того, управляющие E-сети позволяют использовать математический аппарат при описании параметров модели – обеспечивается свойство формализуемости модели. Применение многоагентного подхода позволяет решить проблему многофакторности (комплексности) атаки, выделяя этап поиска уязвимостей объектов атаки (уровень планирования), этапы реализации атаки и определения ее возможных последствий (реактивный уровень); для обмена информацией между агентами разных уровней существует кооперативный уровень.

Полученные имитационные модели информационных атак могут быть использованы для построения синтетического окружения систем информационной безопасности с це-

лью уточнения их особенностей и характеристик с помощью метода полунатурного моделирования.

СПИСОК ЛИТЕРАТУРЫ

1. Сердюк В.А. Анализ современных тенденций построения моделей информационных атак / В.А. Сердюк // Информационные технологии. – 2004. – № 5. – С. 94 – 101.
2. Schneier B. Attack Trees [Електронний ресурс] / B. Schneier. – Режим доступу: http://www.schneier.com/paper-attacktrees-ddj-ft.html.
3. Campete S. A Formal Method for Attack Modeling and Detection: [Електронний ресурс] / S. Campete. – Режим доступу: http://citeseer.ist.psu.edu/751069.html.
4. Shener O. Automated Generation and Analysis of Attack Graphs / O. Shener. – Oakland, CA, USA, 2002. – P. 273 – 284.
5. Gorodetski V. Attacks against Computer Network: Formal Grammer-based Framework and Simulation Tool / V. Gorodetski, I. Kotenko I. // Труды международной конференции RAID. – Санкт-Петербург, 2002. – С. 219 – 238.
6. Хорьков Д.А. О возможности использования математического аппарата сетей Петри для моделирования компьютерных атак / Д.А. Хорьков // Доклады ТУСУРа. – 2009. – № 2. – С. 49 – 50.
7. Уланов А.В. Система многоагентного моделирования механизмов защиты компьютерных сетей [Электронный ресурс] / А.В. Уланов, И.В. Котенко. – Режим доступа: http://www.raai.org/resurs/papers/kii-2006/vistavka/Ulanov.doc.
8. Тумоян Е.П. Методы формального моделирования сетевых атак / Е.П. Тумоян // Известия Южного федерального университета. Технические науки. – 2007. – № 1. – С. 108 – 113.
9. Лукацкий А.В. Обнаружение атак / Лукацкий А.В. – СПб.: БВХ-Петербург, 2001. – 624 с.
10. Сердюк В.А. Информационная безопасность автоматизированных систем предприятий / В.А. Сердюк // Бухгалтер и компьютер. – 2007. – № 1. – С. 104 – 107.
11. Натров В.В. Классификация сетевых атак / В.В. Натров // Информационные технологии в управлении и моделировании: сб. докладов. – Белгород, 2005. – С. 128 – 132.
12. Котенко И.В. Моделирование противоборства программных агентов в Интернете: общий подход, среда моделирования и эксперименты / И.В. Котенко, А.В. Уланов // Защита информации. INSIDE. – 2006. – № 5. – С. 2 – 10.
13. Казимир В.В. Моделирование синтетического окружения для реактивных систем / В.В. Казимир // Математичне моделювання. – 2003. – № 2 (10). – С. 24 – 32.
14. Казимир В.В. Модельно-ориентированное управление интеллектуальными производственными системами: дис… доктора техн. наук: 05.13.06 / Казимир Владимир Викторович. – К., 2006. – 301 с.
15. Nutt G. Evaluation Nets for Computer Systems Performance Analysis / G. Nutt // FJCC, AFIPS PRESS. – 1972. – P. 279 – 286.
16. Городецкий В.И. Многоагентные системы (обзор) / В.И. Городецкий, М.С. Грушинский, А.В. Хабалов // Новости искусственного интеллекта. – 1998. – № 2. – С. 64 – 116.
17. Muller J.P. Modelling Reactive Behaviour in Vertically Layered Agent Architecture / J.P. Muller, M. Pishel, M. Thiel // Intellegent Agents. Proc. of ECAI–94. – Berlin: Springer Verlag , 1994. – P. 261 – 276.
18. Сабанов С.Г. Анатомия хакерской DDoS-атаки [Электронный ресурс] / С.Г. Сабанов. – Режим доступа: http://www.klubok.net/reviews93.html.

Стаття надійшла до редакції 11.05.2010