5. Золотарев В.В. Метод исследования взаимного влияния внутренних параметров средств защиты информации и операционной среды / В.В. Золотарев / Проблемы правовой и технической защиты информации: сб. ст. / Под ред. В.В. Полякова, В.А. Мазурова. – Барнаул: Изд-во Алт. ун-та, 2008. – 180 с.

6. Золотарев В.В. Анализ информационных рисков при передаче данных по открытому каналу / В.В. Золотарев, О.Н. Жданов / Актуальные проблемы безопасности информационных технологий: Материалы I международной заочной научн.-практ. конф. / Под общ. ред. О.Н. Жданова, В.В. Золотарева; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2007. – С. 32-38.

7. Лубкин И.А. Защита программного кода от модификации и исследования методом использования в качестве адресов перехода значений хэш-функций / И.А. Лубкин / Информационная безопасность: Материалы IX Международной научн.-практ. конф. – Ч.1. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – С. 216-220.

УДК 681.3.053:681.32:007.5

А.М. Цыбулин, А.В. Никишова, М.Ю. Умницын

ИССЛЕДОВАНИЕ ПРОТИВОБОРСТВА СЛУЖБЫ БЕЗОПАСНОСТИ И ЗЛОУМЫШЛЕННИКОВ НА МНОГОАГЕНТНОЙ МОДЕЛИ

Пропасть между угрозами информационной безопасности и тем, что делается для защиты от них, становится все шире. Все это обуславливает чрезвычайную актуальность вопросов обеспечения информационной безопасности. Практически любая информационная система (ИС) представляет интерес для злоумышленника.

Специалист по защите информации разрабатывает и реализует ряд стратегий по защите ИС, однако оценка эффективности этих стратегий является насущной и острой проблемой.

Злоумышленник также разрабатывает и реализует ряд стратегий по проведению атак на ИС, используя ее уязвимости, и пытается максимизировать свой успех [1].

Существует множество моделей для исследования эффективности действий службы безопасности и злоумышленников. И, как правило, одна из противоборствующих сторон рассматривается упрощенно.

Исследование противоборства службы безопасности и множества злоумышленников проводится с помощью интеллектуальной многоагентной модели.

Модель включает множество агентов-нарушителей и агентов-системы безопасности, которые являются активными агентами, и агента ИС – пассивный агент. Активные агенты способны выбирать наиболее рациональные стратегии защиты и нападения в зависимости от располагаемых знаний об ИС и обучаться в процессе выполнения своих действий.

Формально агент описывается кортежем:

$$A = (K, B, T, З, И, C, П),$$

где К – класс агента; В – вид агента; Т – время жизни агента; З – совокупность знаний; И – множество инструментальных средств; С – множество стратегий; П – пользовательский идентификатор.

Выделяются следующие классы агентов: агенты службы защиты информации ($А_{сб}$); агенты ИС ($А_{ис}$); агенты злоумышленники ($А_{зл}$).

По месту действия агенты подразделяются на следующие виды: внутренний ($А^{вн}$), внешний ($А^{вш}$) и комбинированный ($А^{км}$).

Времена жизни агентов ИС и службы безопасности не ограничены, $Т_{ИС}=\infty$ и $Т_{СБ}=\infty$. Время жизни агентов злоумышленников ограничено, если злоумышленник не имеет свободного неограниченного доступа к ресурсам ИС.

Полный набор знаний $З=\{З_1,...З_n\}$ об уязвимостях аппаратных и программных средств ИС, полученный с применением всех возможных инструментов, и онтологию уязвимостей агент ИС размещает в своей базе знаний. На основе этих знаний агент ИС синтезирует дерево уязвимостей ИС, $G_{ис}$. Агент службы безопасности, исходя из конкретных возможностей и инструментария (средств обнаружения уязвимостей и средств защиты информации), и на основе своей базы знаний синтезирует дерево уязвимостей ИС, $G_{сб}$. Аналогично агент злоумышленник синтезирует дерево уязвимостей ИС, $G_{зл}$.

Каждому ребру дерева приписывается кортеж:

$$E=(P,T,R,L,D,F),$$

где $P=\max\limits_{i} P_i$ максимальная вероятность успешной реализации атаки (защиты) уязвимости. P_i, i=1..N – вероятность реализации данной уязвимости при использовании i-го инструмента атаки (защиты), где N – количество доступных инструментов. При этом инструменту, дающему максимальную вероятность, приписывается максимальный коэффициент качества;

T – время реализации атаки с использованием данной уязвимости. Данный показатель также учитывает применение неких средств защиты, увеличивая время реализации, а также то, что атака может быть ограничена во времени;

R – риск, R= Y*P, где Y – ущерб, который наносится реализацией данной атаки ИС;

L – уровень данной уязвимости в классификации модели OSI. Используется при построении дерева уязвимостей;

D – флаг, помечающий соответствующую уязвимость, как детектируемую системой диагностики атак. Агент службы безопасности будет получать сообщение, если злоумышленник будет пытаться использовать данную уязвимость в процессе атаки;

F – флаг, содержащий булевы пометки о факте реализации данной уязвимости.

При построении своего дерева агент $А_{ис}$ задает кортежам ребер начальные значения (значения по умолчанию).

После того как построены деревья ИС $G_{ИС}=(E^{ИС},\mathrm{V}^{\mathrm{ИС}})$ и службы безопасности $G_{СБ}=(\mathrm{E}^{\mathrm{СБ}},\mathrm{V}^{\mathrm{СБ}})$, с помощью наложения этих двух деревьев строится дерево политики безопасности $G_{ПБ}=(\mathrm{E}^{\mathrm{ПБ}},\mathrm{V}^{\mathrm{ПБ}})$, где $V_{ПБ}=\mathrm{V}_{\mathrm{ИС}}$, $E_{\mathrm{i}}^{ПБ}=\begin{cases}E_i^{\mathrm{СБ}}, \text{если } \mathrm{E}_{\mathrm{i}}^{\mathrm{ИС}}\in\mathrm{E}^{\mathrm{СБ}}\\ \mathrm{E}_{\mathrm{i}}^{\mathrm{ИС}}, \text{если } \mathrm{E}_{\mathrm{i}}^{\mathrm{ИС}}\notin\mathrm{E}^{\mathrm{СБ}}\end{cases}$, i=1..K – количество ребер в дереве $G_{ис}$.

В соответствии с выбранной стратегией агент $А_{зл}$ на основе своего дерева уязвимостей выбирает маршрут достижения цели. При переходе по соответствующему ребру выбранного маршрута атрибуты ребра (в частности, вероятность и время перехода) соответствуют атрибутам в дереве политики безопасности.

Действия злоумышленника являются случайными событиями, распределенными по закону Пуассона (закону редких событий) $P(x=k)=\frac{np^k}{k!}e^{-np}$,

где p – вероятность успеха (p<<1), n – число повторений (n>>1).

Затем осуществляется проверка условия: x<=P (вероятность реализации уязвимости). Если условие не выполняется, то считается, что злоумышленник не смог пройти по данному ребру.

Аналогично осуществляется проверка для атрибута времени перехода T кортежа ребра, генерируя экспоненциально распределенное число с плотностью распределения $f(x)=\lambda e^{\lambda x}$, где λ – параметр экспоненциальной функции.

Кроме того, при переходе осуществляется проверка флага D детектируемости уязвимости. Если реализация данной уязвимости детектируется, то переход не осуществляется.

Если маршрут с удовлетворительными показателями не найден, то агент может запросить данные о каком-либо маршруте или уязвимости у других агентов. Если при запросе сведений об уязвимости, данная уязвимость была пройдена или предпринималась попытка ее реализации, то сведения о данной уязвимости отправляются.

Агенты $А_{сб}$ используют системы диагностики атак. Для системного мониторинга используются сведения о событиях безопасности, зафиксированных в журналах безопасности операционной системы: тип события; код события; имя пользователя; время возникновения.

Для проведения мониторинга на сетевом уровне используются следующие сведения о пакетах, пересылаемых по сети: адрес источника; адрес получателя; протокол (следующий заголовок); время приема пакета.

Для анализа этих сведений используется универсальный тип нейронной сети многослойный персептрон. Считается, что многослойные персептроны имеют хорошую обобщающую способность [2]. Функционирование нейросетей описывается следующими формулами:

$$NET_{jl}=\sum_i w_{ijl}x_{ijl},$$

$$OUT_{jl}=F(NET_{jl}-\Theta_{jl}),$$

$$x_{ij(l+1)}=OUT_{jl},$$

где i – номер входа, j – номер нейрона в слое, l – номер слоя; x_{ijl} – i-й входной сигнал j-го нейрона в слое l; w_{ijl} – весовой коэффициент i–го входа нейрона j в слое l; NET_{jl} – взвешенная сумма сигналов на входе j-го нейрона в слое l; OUT_{jl} – выходной сигнал j-го нейрона в слое l; Θ_{jl} – пороговый уровень нейрона j в слое l.

Для обучения используется алгоритм обучения с помощью процедуры обратного распространения [3].

Агенту во время его жизни доступно множество инструментальных средств $И = \{И_1,...,И_k\}$. Инструментарий может изменяться и пополняться, в частности, при повторных атаках или если агент получил сведения от других агентов. Характеристики инструментария хранятся в базе знаний, в которой устанавливается соответствие между знаниями об уязвимости и инструментами, необходимыми для реализации этой уязвимости. В базе знаний хранятся сведения, необходимые для реализации некоторых уязвимостей (например, подобранный пароль). Также в базе знаний инструменты ранжируются по приоритету, который указывает на то, что именно этим средством агент будет пользоваться в первую очередь.

Каждому инструменту приписан весовой коэффициент $\alpha \in [0,1]$, который постоянен для этой уязвимости и определяет качество данного инструмента. Соответственно приоритетным будет тот инструмент, у которого это значение выше.

Множество стратегий $C = \{C_1,...,C_m\}$ определяет последовательность действия и решений для участников. Для ИС $C_{ИС} = \varnothing$.

Агенты $А_{зл}$, исходя из наличия инструментальных средств, возможностей их наращивания и построенного дерева атак, выбирают:

- путь с максимальной вероятностью успешного преодоления защиты:

$$\max \prod_{i=1}^{L} P_i ,$$

$$\text{при} \quad \sum_{j=1}^{N} И_{Cj} \le И_{СД} ,$$

$$\sum_{i=1}^{L} T_i \le T_{ЗЛ} ,$$

где L – количество ребер в соответствующем пути в дереве, N – количество инструментальных средств, $И_{Cj}$ – стоимость j-го инструментального средства, $И_{СД}$ – допустимые затраты на приобретение инструментальных средств, T_i – время реализации i-й уязвимости, $Т_{ЗЛ}$ – время жизни агента злоумышленника;

- путь с минимальным временем взлома:

$$\min \sum_{i=1}^{L} T_i ,$$

$$\text{при} \quad \prod_{i=1}^{L} P_i > P_{доп} ,$$

где L – количество ребер в соответствующем пути дерева, P_i – вероятность реализации i-й уязвимости, $Р_{доп}$ – нижнее допустимое значение вероятности прохождения маршрута.

Агенты $А_{СБ}$, исходя из наличия инструментальных средств, возможностей их наращивания и построенного дерева уязвимостей атак, определяют наиболее вероятный путь злоумышленника. На основании этого пути формируются приоритетные стратегии усиления защиты, стремясь сделать все пути в дереве равновероятными. Однако такой вариант требует больших финансовых ресурсов. Поэтому на

практике реализуется в первую очередь защита наименее защищенного пути в дереве, с учетом ограничений на стоимость инструментальных средств защиты:

$$\min \prod_{i=1}^{K} P_i ,$$

$$\text{при} \qquad \sum_{j=1}^{J} И_{Cj} \le И_{СД} ,$$

где J – количество инструментальных средств, необходимых для повышения защищенности, K – количество ребер в соответствующем пути в графе, $И_{Cj}$ – стоимость j-го инструментального средства, $И_{СД}$ – допустимые затраты на приобретение инструментальных средств.

Кроме уменьшения вероятности реализации уязвимости, агент службы безопасности может:

- понизить время жизни уязвимости;
- выключить или остановить службу, содержащую данную уязвимость, тем самым удалив вершину из графа.

Стратегия может изменяться в течение атаки, тем самым выбор следующего шага не определен заранее.

Разработана архитектура интеллектуальной многоагентной модели (см. рис.1), алгоритмы модулей. Программная реализация модели выполнена на объектно-ориентированном языке C#.

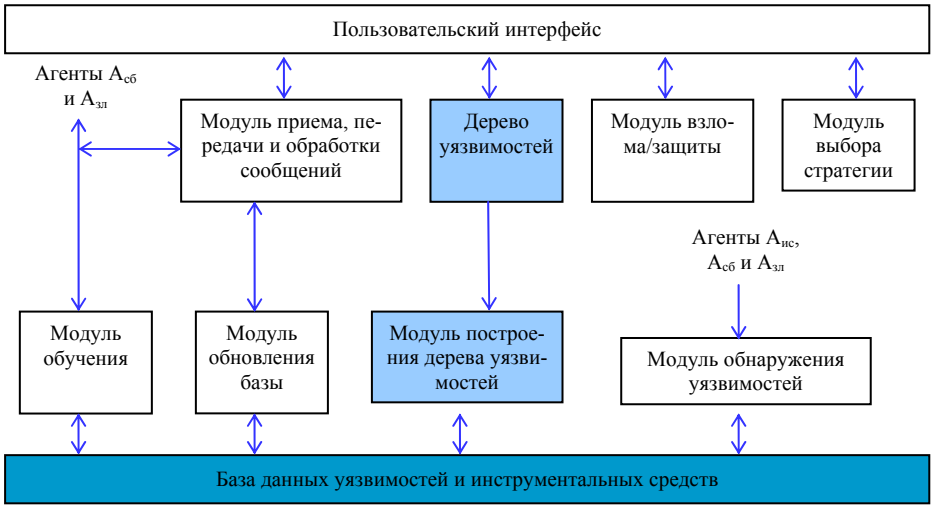

Рис. 1. Архитектура интеллектуальной многоагентной модели

Модель использовалась для исследования ИС, имеющей 50 уязвимостей. Количество типов уязвимостей составило 4, согласно исследованию [4]. Было сгенерировано 2 дерева, содержащих 21 и 35 уязвимостей. Было выделено 4 вида варьируемых параметров (количество агентов-злоумышленников; количество агентов СЗИ; количество шагов; количество инструментов), для каждого из случаев было проведено по 3 эксперимента.

Результаты 3-х противоборств агентов службы безопасности и агентов злоумышленников представлены на рис. 2.

В случае б) агент службы безопасности отключил сервис, тем самым прервав возможную атаку. В случае в) агент службы безопасности установил заплатку на данную уязвимость. В случае г) агенты злоумышленники осуществили обход защиты и достигли своей цели, однако информация об их деятельности зафиксирована.

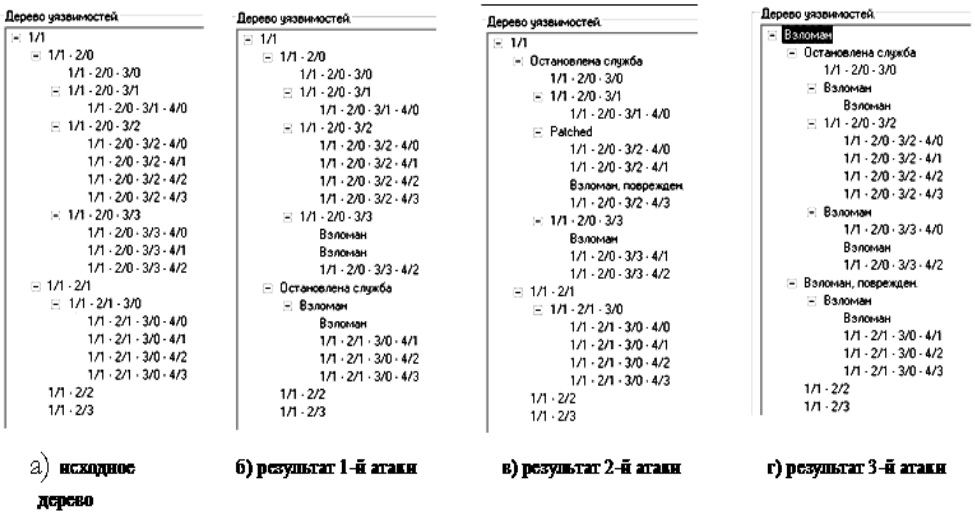

Рис. 2. Результаты противоборств агентов службы безопасности и агентов злоумышленников

Использование этой модели позволяет исследовать различные стратегии усиления системы защиты и выбрать оптимальную стратегию при атаках одного злоумышленника и ассоциации злоумышленников, проводящих распределенные атаки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Цыбулин А.М., Шипилева А.В.* Математическая модель злоумышленника в корпоративной сети. Управление большими системами. Выпуск 19. – М.: ИПУ РАН, 2007. – 127-133 с.

2. *Брюхомицкий Ю.А.* Нейросетевые модели для систем информационной безопасности: Учебное пособие. – Таганрог, 2006.

3. *Никишова А.В.* Программный комплекс диагностики атак на информационную систему. Тезисы докладов XII региональной конференции молодых исследователей Волгоградской области, РПК «Политехник». – Волгоград, 2008. – 201-203 с.

4. *Милославская Н. Г., Толстой А. И.* Интрасети обнаружение вторжений. – М.: ЮНИТИ-ДАНА, 2001. – 587 с.