УДК 004.056.5 004.89

А.А. Бешта

АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА КОНТРОЛЯ НАД ВНУТРЕННИМ ЗЛОУМЫШЛЕННИКОМ*

Целью данного исследования является разработка архитектуры программного комплекса контроля над внутренним злоумышленником на основе механизма оценки доверия. В рамках данного исследования была показана методика оценки доверия к субъекту на основе разработанной (ε; θ)-доверительная модель субъекта. Показано сравнение разработанной модели оценки доверия с существующими моделями и выделены ее преимущества. Показана архитектура программного комплекса и предложен набор агентов для реализации разработанной модели оценки доверия. Показаны архитектуры агентов, входящих в программный комплекс. Показана схема взаимодействия между агентами и типы передаваемой информации.

Внутренний злоумышленник; программный агент; оценка доверия; событие информационной системы.

A.A. Beshta

ARHITECRURE OF INSADERS CONTROL SOFTWARE DEVELOPMENT

The purpose of the research is development of architecture of control over insiders software based on object confidence evaluation approach. In this research the method of confidence evaluation based on (ε; θ)-object confidence was proposed. Developed model was compared with existing models and its advantages were shown. The set of software agent is proposed. Architecture of different agents type and interaction between agents were shown.

Insider; software agent; confidence evaluation; information system event.

В настоящее время при обеспечении безопасности информационных систем организации основная задача заключается в защите внешнего периметра и обнаружении вторжений из-за пределов организации. При этом внутреннему злоумышленнику уделяется меньшее внимание. Обычно используются средства предотвращения утечек информации во внешние сети и контроль съемных устройств. Возможность анализировать самого пользователя и делать вывод о том, что его действия могут быть злоумышленными. Одним из эффективных подходов является использования механизмов оценки доверия к субъектам. Этот подход предполагает, что субъекту, на основе его действий, ставится некоторый уровень доверия, который означает, что наблюдаемый субъект не является источником злоумышленного воздействия на информационную систему. Этот вопрос активно исследуется в зарубежных работах, но в отечественных исследованиях практически не рассматривается. В данной статье предлагается архитектура программного комплекса системы контроля над внутренним злоумышленником на основе механизма оценки доверия к субъектам.

Прежде чем рассматривать архитектуру программного комплекса необходимо рассмотреть саму модель оценки доверия, которая лежит в его основе.

Оценка уровня доверия $B_{E_i^{\tilde{T}}}$ к субъекту $E_i^{\tilde{T}}$ определяется из количества исходящих сигналов $\gamma = \left(\gamma^+ \cup \gamma^-\right)$ противоположной направленности с разной степенью значимости: γ^+ – сигнал положительной направленности и γ^- – сиг-

* Работа выполнена при поддержке гранта РФФИ и Волгоградской области (№ 13-07-97040).

нал отрицательной направленности. Сигналом отрицательной направленности (отрицательным сигналом) является обнаруженное в системе событие, указывающее на то, что субъект попытался выполнить или выполнил некоторое запрещенное воздействие. Сигналом положительной направленности (положительным сигналом) является отсутствие запрещенных воздействий на некотором интервале наблюдения за субъектом *T*. Одним из возможных источников сигналов могут быть события информационной системы, связанные с деятельностью пользователя (подробнее в [1]).

Кроме того, можно выделить следующие требования к значению доверия:

- для нового объекта всегда начинается с минимального значения и не может быть выше доверия существующего объекта;
- ограничено сверху;
- зависит от полученных сигналов и обновляется после каждой оценки;
- увеличение доверия объекта, уже имеющего высокое значение, намного меньше, чем для объекта с низким доверием.

Для оценки доверия используется (ε; θ)-доверительная модель объекта, которая выглядит следующим образом (более подробно в работах [2, 3]):

$$B_{E_i^{\tilde{T}}} = \begin{cases} \dfrac{\gamma^+ - \left(\gamma^-\right)^\theta}{\gamma + \dfrac{\varepsilon^2}{\gamma}}, \gamma > \Omega; \\ 0, \gamma < \Omega. \end{cases} \quad (1)$$

где $\gamma = \gamma^+ + \gamma^-$; ε – коэффициент достаточности; θ – коэффициент критичности.

Функция (1) имеет следующие управляющие параметры, которые позволяют подобрать коэффициенты модели ε и θ для различных типов субъектов:

$\Omega = \left(\gamma^-\right)^\theta + \gamma^-$ – значение γ, при котором можно говорить о доверии к субъекту $B_{E_i^{\tilde{T}}} = 0$;

$\Psi = \begin{cases} \varepsilon, & \text{при } \gamma^- = 0; \\ \Omega + \sqrt{\Omega^2 + \varepsilon^2}, & \text{при } \gamma^- \neq 0, \end{cases}$ – значение γ, при котором достигается середина уровня доверия $B_{E_i^{\tilde{T}}} = 1/2$.

В общем случае снижение уровня доверия при любом $\gamma >> \varepsilon$ стремится к величине Ω/γ, а величина уровня доверия $B_{E_i^{\tilde{T}}}$ не превосходит $B_{\max} = 1 - \dfrac{\Omega}{T + \dfrac{\varepsilon^2}{T}}$.

Тогда критерий β для оценки доверия можно выбрать из условия:

$$\beta \geq B_{\max} - \frac{\Omega}{\gamma}. \quad (2)$$

Из этого выражения получены критерии, позволяющие обнаружить различное количество отрицательных сигналов за наблюдаемый период (табл. 1).

Среди существующих моделей оценки доверия (подробно описаны в [4]), которые могут быть использованы для решения поставленной задачи, можно выделить модели, основанные на Байесовом подходе, модель Josang и модель средних.

Таблица 1

Критерии оценки β для различных параметров модели

γ^-	T				
	40	80	120	160	400
2	0,65	0,86	0,92	0,95	0,98
3	0,5	0,79	0,87	0,91	0,96
4	0,3	0,69	0,80	0,86	0,94
5	0,05	0,57	0,72	0,79	0,92
6	0	0,42	0,62	0,72	0,89

Разработанная модель соответствует требованиям, предъявляемым к моделям данного типа, а в сравнении с существующими моделями обладает следующими преимуществами:

- требует существенно меньшее количество отрицательных сигналов (рис. 1);

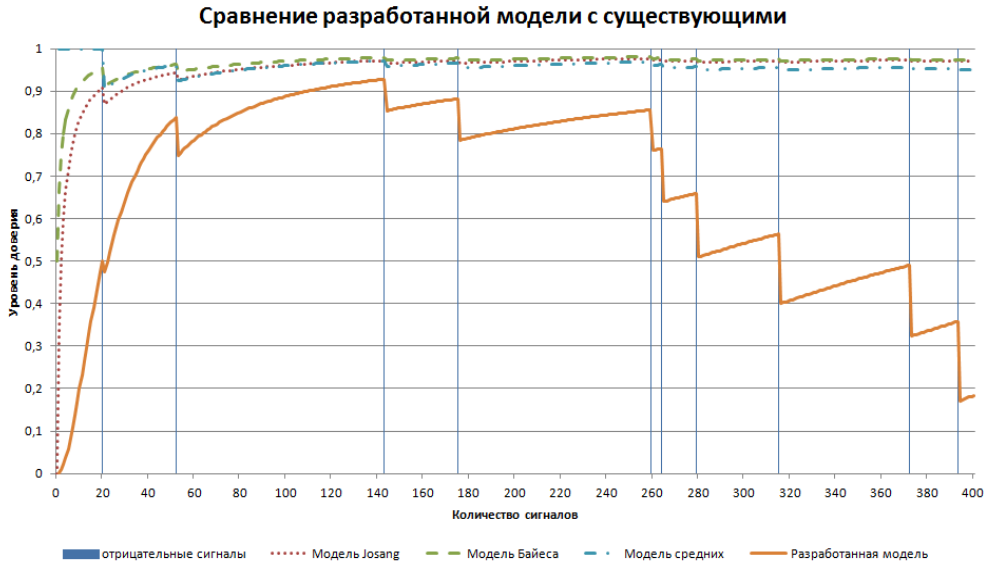

Рис. 1. Сравнение моделей оценки доверия

- имеет временное окно для расчета доверия и учитывает возможность изменения поведения объекта.

На рис. 1 у разработанной модели наблюдается снижение уровня доверия при получении отрицательных сигналов, что позволяет установить критерий для оценки доверия.

Алгоритм оценки доверия к субъектам состоит из следующих шагов:

1. Определение субъекта оценки.
2. Определение источника сигналов γ^+ и γ^-.
3. Определение интервала наблюдения T, коэффициентов ε и θ, вычисление управляющих параметров Ω и Ψ.
4. Выбор критерия β, позволяющего обнаружить заданное количество отрицательных сигналов.

5. Получение сигналов γ^+ и γ^-, вычисление $B_{E_i^{\tilde{t}}}$.
6. Если значение доверия меньше β, то субъект является злоумышленником.
7. Повторение шага 6 до тех пор, пока не потребуется корректировка параметров модели.
8. Если необходима корректировка параметров модели, перейти к шагу 3.

Для реализации данного алгоритма был разработан программный комплекс, архитектура которого представленная в виде многоагентной системы и состоит из шести типов агентов:

$$A^S = \{A_K, A_M, A_{SM}, A_B, A_{SA}, A_A\}, \quad (3)$$

где A_K – агент координатор; A_M – агент мониторинга; A_{SM} – агент специализированного мониторинга; A_B – агент оценки доверия; A_{SA} – агент анализа защищенности; A_A – агент адаптации.

Для организации взаимодействия между отдельными агентами для достижения цели была предложена схема обмена информацией между агентами (рис. 2), которая учитывает возможность установки параметров оценки для различных субъектов и получение сигналов из различных источников.

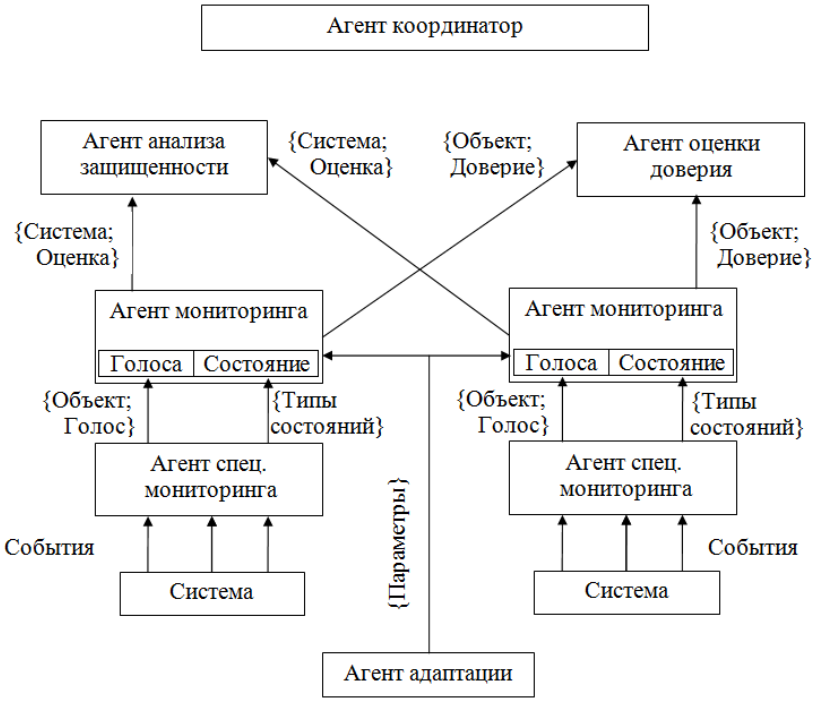

Рис. 2. Схема взаимодействие агентов

Были разработаны архитектуры всех типов агентов и определены основные этапы работы. На рис. 3 представлена архитектура агента основного агента – мониторинга, показаны отдельные модули, блоки, из которых они состоят, и связи между ними.

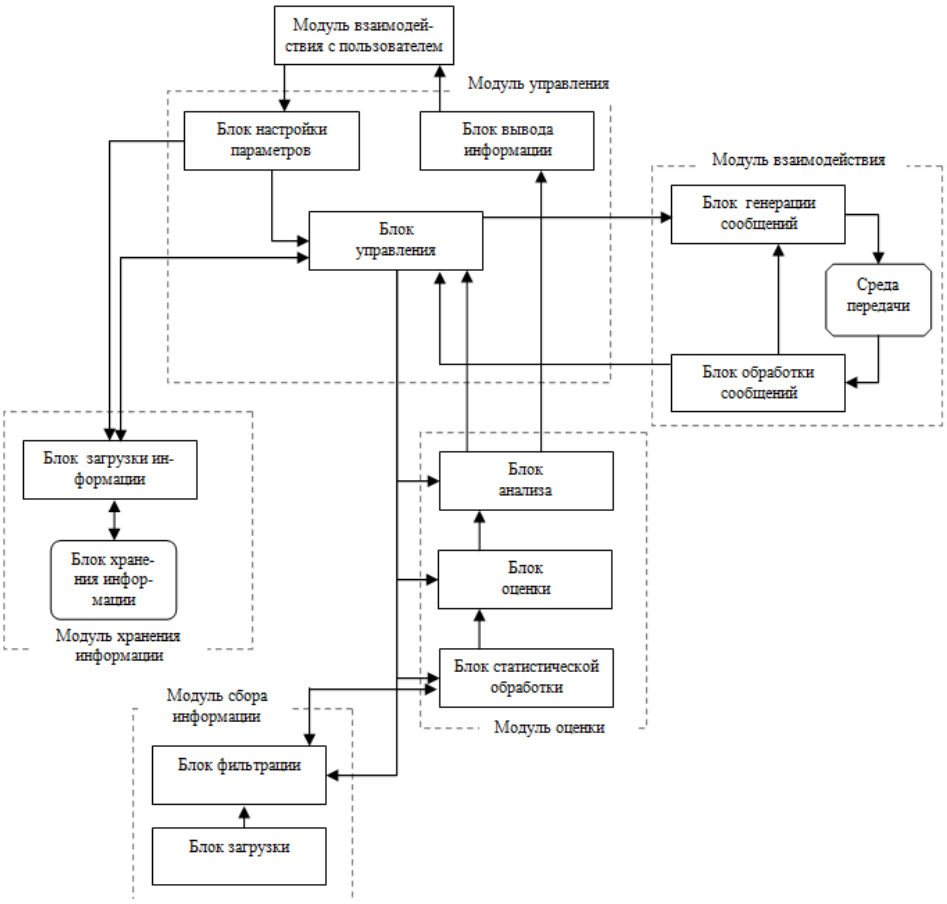

Рис. 3. Архитектура агента мониторинга

Архитектура включает следующие модули:

- модуль взаимодействия с пользователем – позволяет пользователю задавать параметры работы агента;
- модуль управления – обеспечивает взаимодействие всех модулей агента;
- модуль хранения информации – позволяет сохранять и получать информацию об объектах системы, хранит параметры работы агента;
- модуль сбора информации – реализует получение из определенных источников сигналов от объектов; модуль позволяет подключаться к некоторому количеству источников, обнаруживать появление сигналов и передавать их модулю оценки;
- модуль оценки – производит оценку уровня доверия к субъектам;
- модуль взаимодействия – позволяет агенту взаимодействовать с другими агентами по заданному протоколу для обмена информацией или управляющими воздействиями (позволяет сообщать результаты оценки уровня доверия к субъекту другим агентам).

Архитектура агента специализированного мониторинга показана на рис. 4. Отличие от агента мониторинга заключается в отсутствии блока оценки.

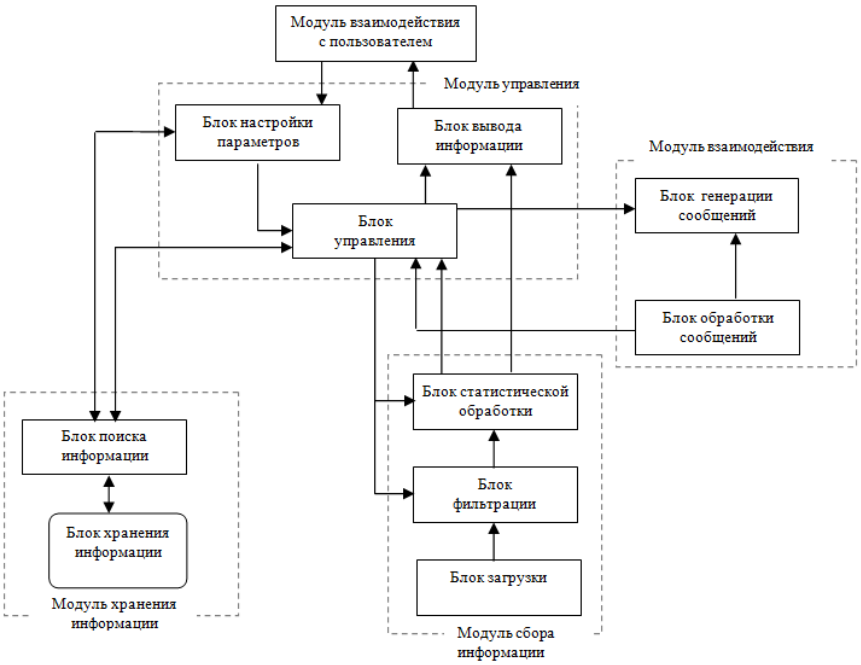

Рис. 4. Архитектура агента специализированного мониторинга

Архитектура агентов оценки доверия, анализа защищенности и адаптации показана на рис. 5. В архитектуре такого типа отсутствует модуль сбора информации, а модуль оценки имеет прямую связь с модулем хранения информации.

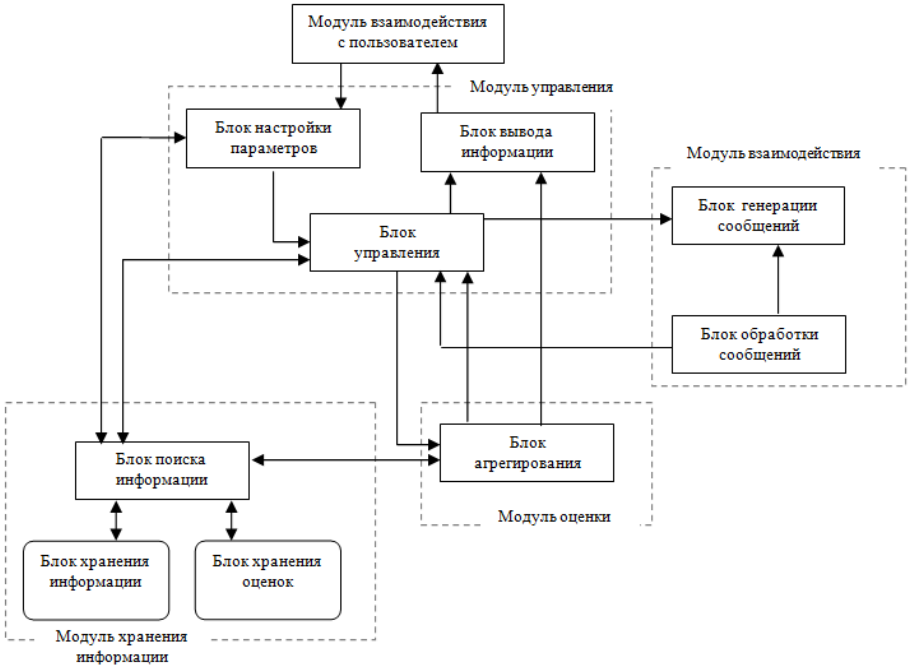

Рис. 5. Архитектура агентов других типов

Отличие заключается в модуле оценки и в модуле работы с базами данных. У агентов оценки доверия и анализа защищенности модуль оценки содержит только блок агрегирования, который ведет перечень объектов, анализирует полученные от различных агентов мониторинга оценки и сохраняет их в базу, вычисляет обобщенную оценку объектов для АИС и распространяет эти оценки среди агентов мониторинга. Модуль хранения информации содержит дополнительно блок хранения оценок. У агента адаптации (подробнее в [5]) модуль оценки содержит только блок адаптации, а вместо блока оценок к модуле хранения информации находится блок параметров.

Таким образом, архитектура программного комплекса состоит из совокупности программных агентов. Предложенная модель оценки доверия к субъектам разделена на подзадачи, которые выполняются различными типами агентов. Предложенные архитектуры программных агентов позволяют учесть указанные возможности для реализации алгоритма контроля над внутренним злоумышленником и использовать в качестве критерия обнаружения предложенную модель оценки доверия к субъектам информационной системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бешта А.А., Новикова Ю.В.* Способ численной оценки состояния автоматизированной информационной системы // Научно- технический вестник Поволжья. – 2013. – № 2. – С. 89-92.
2. *Бешта А.А.* Архитектура агента контроля над внутренним злоумышленником на основе механизма оценки доверия // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 104-110.
3. *Бешта А.А., Кирпо М.А.* Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. Управление, вычислительная техника и информатика. – 2013. – Т. 322, № 5. – С. 104-108.
4. *Губанов Д.А.* Обзор онлайновых систем репутации / доверия. – М.: ИПУ РАН, 2009. Интернет-конференция по проблемам управления. – 25 с. – Режим доступа: http://ubs.mtas.ru/bitrix/components/ bitrix/forum.interface/ show_file.php?fid=1671.
5. *Бешта А.А.* Многоагентная эволюционирующая система как средство контроля над внутренним злоумышленником // Вестник волгоградского государственного университета. Серия 10. Инновационная деятельность. – 2012. – Вып. 6. – С. 93-97.

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

Бешта Александр Александрович – Волгоградский государственный университет; e-mail: abewta@rambler.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; ассистент.

Beshta Alexander Alexandrovich – Volgograd State University; e-mail: abewta@rambler.ru; 100, Ave University, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; assistant.

УДК 004.492

Л.К. Бабенко, А.С. Кириллов

МОДЕЛИ ОБРАЗЦОВ ВПО НА ОСНОВЕ ИСПОЛЬЗУЕМЫХ СИСТЕМНЫХ ФУНКЦИЙ И СПОСОБОВ ПОЛУЧЕНИЯ ИХ АДРЕСОВ

Рассматриваются вопросы построения модели вредоносного программного обеспечения (ВПО), ориентированной на включение в структуру образцов не только информации о конкретных системных функциях, но и способах получения их адресов. Такая модель может быть использована для эффективного обнаружения и классификации неизвестных ра-