7. *Конявский В.А.* Управление защитой информации на базе СЗИ НСД «АККОРД». – М.: Радио и связь, 1999. – 325 с.
8. *Веретенников А.А.* Развертывание СЗИ НСД Secret Net в корпоративной сети с использованием протокола RDP, функции автоматической установки клиента и удаленной установки программного обеспечения аппаратной поддержки» // [Электронный ресурс] http://www.itsecurity.ru/press/pdf/Secret_Net_deployment_with_RDP.pdf.

Статью рекомендовал к опубликованию д.т.н., профессор И.И. Исмагилов.

Ляшко Дмитрий Анатольевич – ОАО «АйСиЭл – КПО ВС»; email: dimal@icl.kazan.ru; 420111, г. Казань, Сибирский тракт, 10; тел.: 89872964027; технический директор; соискатель.

Аникин Игорь Вячеславович – Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ; email: anikinigor777@mail.ru; 420073 г. Казань, ул. Гвардейская, 24-45; тел.: 89520421458; кафедра систем информационной безопасности; зав. кафедрой; к.т.н.; доцент.

Lyashko Dmitriy Anatol'evich – ICL-KME CS; email: dimal@icl.kazan.ru; 10, Siberian road, Kazan', 420111, Russia; phone: +79872964027; technical director; competitor.

Anikin Igor Vyacheslav'ovich – Kazan State Technical University named after A.N. Tupolev-KAI; email: anikinigor777@mail.ru; 24-45, Gvardeyskayu street, Kazan', 420073, Russia; phone: 89520421458; the department of information security; head the department; cand. of eng. sc.; associate professor.

УДК 004.056.5 004.89

А.А. Бешта

АРХИТЕКТУРА АГЕНТА КОНТРОЛЯ НАД ВНУТРЕННИМ ЗЛОУМЫШЛЕННИКОМ НА ОСНОВЕ МЕХАНИЗМА ОЦЕНКИ ДОВЕРИЯ

Целью данного исследования является разработка архитектуры агента контроля над внутренним злоумышленником на основе механизма оценки доверия. В рамках данного исследования была предложена методика оценки доверия к наблюдаемому объекту на основе поданных за объект голосов с учетом важности этих голосов, для этого разработана (ε; θ) – доверительная модель объекта. Показано влияние коэффициентов модели на уровень доверия и предложены управляющие параметры модели. На основе этой модели построен алгоритм контроля над внутренним злоумышленником. Предложена архитектура программного агента, реализующая данный алгоритм. Показаны основные модули агента и составляющие их блоки, описаны информационные потоки между ними, описаны основные функции всех блоков и логика работы агента.

Внутренний злоумышленник; деструктивное воздействие; доверие к объекту; событие информационной системы.

A.A. Beshta

ARHITECRURE OF INSADERS CONTROL AGENT BASED ON CONFIDENCE EVALUATION APPROACH

The purpose of the research is development of architecture of control over insiders agent based on object confidence evaluation approach. In this research the method of confidence evaluation to observed object was proposed. This method account voices for observed object and their importance. For this purpose (ε; θ) – object confidence model was developed. Influence of model's factors on confidence level was shown and control parameters of model were developed. Algo-

rithm of control over insiders and architecture of software agent implements this algorithm were developed. Modules of agent architecture and their components were shown; data flows between these components, block's functions and the logic of the agent were described.

Insider; destructive impact; confidence in the object; information system event.

В настоящее время при обеспечении безопасности конечных рабочих мест пользователей стремятся к распределению функций безопасности среди множества систем. К таким подходам можно отнести появление механизмов оценки репутации объектов, заявленные многими производителями средств защиты конечных рабочих мест. Этот подход заключается в том, что некоторый объект,получивший оценку безопасности на одной рабочей станции, можно не оценивать на другой станции, а использовать результат оценки. Это позволяет повысить скорость работы систем безопасности и понизить загрузку ресурсов. Можно выделить несколько зарубежных работ [1, 2, 5], посвященных данной тематике, тем не менее, ощущается недостаточность отечественных научных исследований, проведенных в данной области. В данной статье предлагается подход к построению системы контроля над внутренним злоумышленником на основе механизма оценки доверия к объектам информационной системы.

Каждому объекту системы можно поставить в соответствие некоторый уровень доверия. Тогда высоким уровнем доверия может обладать объект, который не является источником деструктивных воздействий.

В данном случае под уровнем доверия понимается ожидаемая реакция объекта – что можно ожидать от объекта в различных ситуациях и взаимодействиях [3].

То есть доверие к объекту – это вероятность того, что объект не является источником деструктивного воздействия на объекты информационной системы. Под внутренним злоумышленником понимается объект информационной системы, который может быть источником деструктивного воздействия.

Тогда логичным будет повышенное внимание к возможным внутренним злоумышленникам, то есть объектам с низким уровнем доверия.

Возникает задача контроля доверия к объектам системы и выполнение определенных функций защиты при появлении объектов с уровнем доверия ниже установленной нормы [4].

Поставленная задача достигается тем, что уровень доверия $B_{E_i^{\tilde{T}}}$ объекта $E_i^{\tilde{T}}$ типа $\tilde{T}$ системы E складывается из голосов $\gamma = \left(\gamma^+ \cup \gamma^-\right)$, поданных за этот объект: γ^+ – положительный голос и γ^- – отрицательный голос.

При оценке доверия к объектам необходимо учитывать:

- объект с малым количеством голосов имеет низкий уровень доверия;
- увеличение количества положительных голосов за объект повышает его уровень доверия;
- отрицательный голос за объект понижает его уровень доверия;
- степень влияние положительных и отрицательных голосов за объект на уровень доверия зависит от параметров, определяемых важностью оцениваемого объекта.

Тогда для оценки доверия к объекту необходимо использовать функцию с параметрами ε и θ, определяющими степень влияния положительных и отрицательных голосов соответственно.

Для оценки доверия используется (ε; θ)-доверительная модель объекта, которая выглядит следующим образом:

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

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

Функция (1) имеет следующие управляющие параметры:

$$\Omega = \left(\gamma^-\right)^\theta + \gamma^-;$$

$$\Psi = \begin{cases} \varepsilon, & \text{при } \gamma^- = 0 \\ \Omega + \sqrt{\Omega^2 + \varepsilon^2}, & \text{при } \gamma^- \neq 0 \end{cases},$$

где $\gamma = \Omega$ – значение, при котором $B_{E_i^{\bar{\gamma}}} = 0$; $\gamma = \Psi$ – значение, при котором $B_{E_i^{\bar{\gamma}}} = 1/2$.

Коэффициент достаточности объекта εопределяет значимость положительных голосов и указывает на то, какое количество голосов должен получить объект, что бы достигнуть уровня доверия 0,5, и позволяет контролировать скорость роста доверия к объекту.

Коэффициент критичности θ позволяет контролировать величину падения уровня доверия к объекту при отрицательном голосе.

Управляющие параметры позволяют подобрать коэффициенты модели ε и θ для различных типов объектов.

На рис. 1 показано влияние параметра ε на рост уровня доверия.

Рис. 1. (ε;θ)-доверительная модель объекта, влияние параметра ε (сплошная линия – ε=10, точка – ε= 20, пунктир – ε= 30)

На рис. 2 показана доверительная модель с различным количеством отрицательных голосов.

Тогда алгоритм контроля над внутренним злоумышленником на основе оценки доверия к объектам состоит из следующих шагов:

1. Определение объекта оценки.
2. Определение источника голосов γ^+ и γ^-.
3. Оценка объекта и вычисление управляющих параметров Ω и Ψ.

4. Установить критерий β.
5. Определение коэффициентов ε и θ.
6. Получение голосов γ^+ и γ^-, вычисление $B_{E_i^{\tilde{I}}}$.
7. Если достигнуто значение β, то обнаружен потенциальный внутренний злоумышленник, который может быть источником деструктивного воздействия.
8. Повторять шаг 6 до тех пор, пока не потребуется корректировка.
9. Если необходима корректировка параметров модели, перейти к шагу 3.

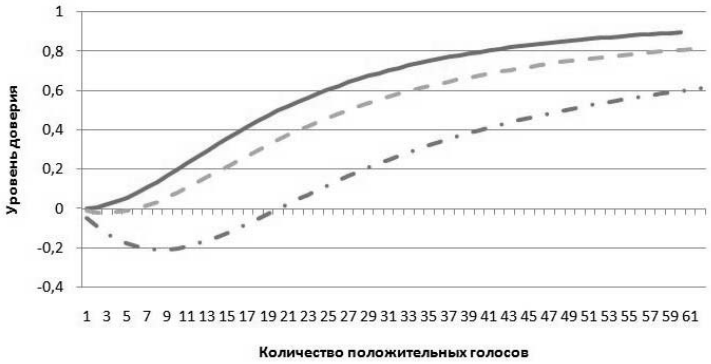

Рис. 2. (ε;θ)-доверительная модель объекта с параметрами ε = 20 и θ = 2 и различным количеством отрицательных голосов (сплошная линия – $\gamma^- = 0$, тире – $\gamma^- = 2$, точка-тире – $\gamma^- = 4$)

Для реализации данного алгоритма в виде программного агента должны быть реализованы возможности установки параметров оценки, выбора источника голосов и их получения; должна быть реализована процедура оценки. Также необходимо обеспечить возможность предоставить результат оценки внешним объектам.

Таким образом, агент может обнаружить появление потенциального источника деструктивного воздействия в системе, и сообщить об этом.

Архитектура такого агента состоит из следующих модулей (рис. 3):

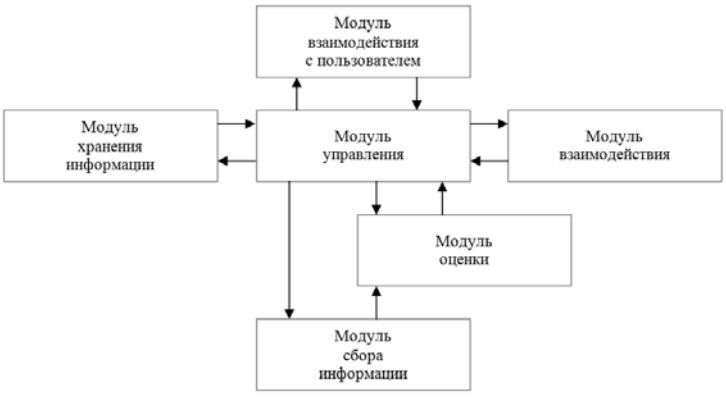

Рис. 3. Архитектура агента

- модуль взаимодействия с пользователем – позволяет пользователю задавать параметры работы агента, обеспечивает представление необходимой информации;
- 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 – выполняет сбор из определенных источников по заданным правилам информации о событиях, связанных с объектами информационной системы; модуль позволяет подключаться к некоторому количеству источников информации, обнаруживать появление событий, отбирать значимые события и передавать отобранные события модулю оценки для последующего анализа;
- модуль оценки – проводит оценку событий и определяет уровень доверия к объектам, с которыми связано это событие, а также вырабатывает управляющее решения при достижении некоторого уровня доверия;
- модуль взаимодействия – позволяет агенту взаимодействовать с другими агентами по заданному протоколу для обмена информацией или управляющими воздействиями (позволяет сообщать результаты оценки уровня доверия к объектам другим агентам, передавать выработанное управляющее решение, запрашивать у другого агента необходимую информацию).

На рис. 4 показаны отдельные блоки, из которых состоят модули агент, и связи между этими блоками.

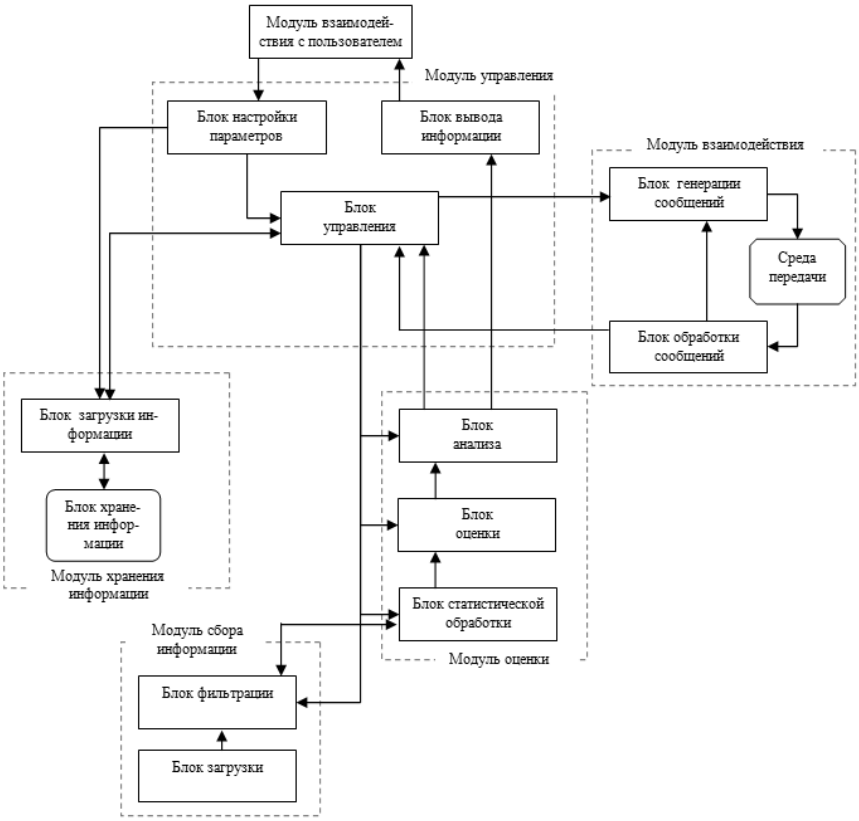

Рис. 4. Структура блоков агента

Модуль управления включает в себя три блока: блок настройки параметров, блок управления, блок вывода информации.

Блок настройки параметров загружает параметры работы агента из блока хранения информации или устанавливает и сохраняет параметры, заданные пользователем.

Блок вывода информации создает отчет о работе агента, визуализирует результат анализа информации и предоставляет результаты в модуль взаимодействия с пользователем.

Блок управления определяет последовательность и параметры работы всех блоков, обрабатывает команды пользователя, организует взаимодействие с другими агентами.

Модуль хранения информации включает в себя блок хранения информации и блок загрузки информации.

Блок хранения информации содержит информация о параметрах работы отдельных блоков, правила отбора, фильтрации и обработки событий, правила оценки и анализа, информация об объектах.

Блок загрузки информации обеспечивает взаимодействие с блоком хранения информации: загрузку и сохранение информации, поиск определенных объектов и параметров.

Модуль сбора информации состоит из двух блоков: блока загрузки и блока фильтрации.

Блок загрузки обеспечивает подключение к заданным источникам информации о событиях информационной системы и чтение этой информации.

Блок фильтрации отделяет значимую информацию из общего объема полученной из источника информации. Правила фильтрации определяются предустановленными параметрами из блока хранения информации.

Модуль оценки состоит из трех блоков: блок статистической обработки, блок оценки и блок анализа.

Блок статистической обработки определяет значимость отдельных событий и их совокупностей и передает их в модуль оценки.

Блок оценки проводит оценку доверия к объектам, обозначенных как участники значимого события. Оценка производится на основе предустановленных параметров модели оценивания. На выходе блока оценки будет уровень доверия к объекту. Этот уровень передается в блок анализа.

В блоке анализа проводится соответствие между уровнем доверия к объекту и некоторым критическим значением, а при необходимости и с другими параметрами системы, делается вывод о состоянии системы. При достижении критического уровня доверия формируется управляющее воздействие по отношению к объекту. Если для проведения анализа необходимо получить дополнительную информацию об объектах у других агентов, соответствующий запрос и передается блоку управления. Результат анализа передается блоку вывода информации и блоку управления.

Модуль взаимодействия включает блок генерации сообщений и блок обработки сообщений.

Блок генерации создает запросы к другим агентам на получение необходимой информации или на выполнение определенных управляющих воздействий и передает сформированные запросы по определенному протоколу через среду передачи другому агенту.

Блок обработки сообщений выполняет разбор полученных от других агентов-сообщений и в зависимости от содержания либо продолжает взаимодействие, либо передает содержание сообщения в блок управления.

Таким образом, предложенная архитектура программного агента позволяет учесть все указанные возможности для реализации алгоритма контроля над внутренним злоумышленником и использовать в качестве критерия обнаружения предложенную методику оценки доверия к объектам информационной системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Rosari D., Sarne G., Garruzzo S.* Integrating trust measures in multiagent systems. International journal of intelligent systems. // Wiley Periodical. – 2012. – Vol. 27, № 1. – P. 1-15.
2. *Salehi-Abari A., White T.* DART: a distributed analysis of reputation and trust framework. Computational intelligence // Wiley Periodical. – 2012. – Vol. 28, № 4. – P. 642-682.
3. *Новиков Д.А.* Математические модели формирования и функционирования команд. – М.: Изд-во «Физматлит», 2008. – 184 с.
4. *Бешта А.А.* Подход к выявлению внутреннего злоумышленного воздействия на основе репутации объектов. Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: Материалы Всерос. науч.-практ. конф., г. Волгоград, 27 апреля 2012 г. / ФГБОУ ВПО «Волгогр. гос. ун-т». – Волгоград: Изд-во ВолГУ, 2012. – 185 с.
5. *Arenas A., Aziz B., Silaghi G.* Reputation management in collaborative computing systems. Security and Communication Networks // Wiley Periodical. – 2010. – Vol. 3, № 6. – P. 546-564.

Статью рекомендовал к опубликованию д.т.н. профессор О.Б. Макаревич.

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 University100; e-mail: abewta@rambler.ru; 100, Ave University, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; assistant.