3. *Ramboli A.L., Falowo O.E., Chan A.H.* Bandwidth aggregation in heterogeneous wireless networks: A survey of current approaches and issues // Journal of Network and Computer Applications. – May, 2012, № 35. – P. 1674-1690.
4. *Chebrolu K. and Rao R.R.* Bandwidth Aggregation for Real-Time Applications in Heterogeneous Wireless Networks // IEEE Mobile Transactions on Mobile Computing. – April, 2006. – Vol. 5, № 4. – P. 388-403.
5. *Jurca D. and Frossard P.* Video Packet Selection and Scheduling for Multipath Streaming // IEEE Transactions on Multimedia. – April, 2007. – Vol. 9, № 3. – P. 629-641.
6. *Singh V., Ahsan A. and Ott J.* MPRTP: Multipath Considerations for Real-time Media // MMSys '13, Proceedings of the 4th ACM Multimedia Systems Conference. – February 26-March 1, 2013. – P. 190-201.
7. *Singh V., Karkkainen T., Ott J. and Ahsan S.* Multipath RTP (MPRTP), 2012. IETF Draft, draft-singh-avtcore-mprtp.
8. *Schulzrinne H., Casner S., Frederick R. and Jacobson V.* RTP: A Transport Protocol for Real-Time Applications., RFC 3550, 2003.
9. Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF), RFC 4585.

Статью рекомендовал к опубликованию к.т.н. С.А. Третьяков.

Пакулова Екатерина Анатольевна – Южный федеральный университет; e-mail: epakulova@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: +78634371905; кафедра безопасности информационных технологий; инженер.

Pakulova Ekaterina Anatol'evna – Southern Federal University; e-mail: epakulova@sfedu.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; engineer.

УДК 004.056.5 004.89

А.А. Бешта, А.М. Цыбулин

АЛГОРИТМ ОБНАРУЖЕНИЯ ВНУТРЕННЕГО НАРУШИТЕЛЯ НА ОСНОВЕ МЕХАНИЗМА ОЦЕНКИ ДОВЕРИЯ*

Целью исследования является разработка алгоритма использования модели оценки доверия для решения задачи обнаружения внутреннего нарушителя в информационной системе. Описана разработанная авторами модель оценки доверия, ее управляющие параметры и коэффициенты. Показан алгоритм работы модели и описана последовательность действий при обнаружении нарушителя. Проведено исследование влияния коэффициентов модели на значение уровня доверия, определены их допустимые значения. На первом этапе допустимые значения коэффициентов определяются аналитически. В результате получены зависимости, позволившие установить границы значений коэффициентов. На втором этапе значения определяются экспериментально при различных наборах параметров. Экспериментальное исследование влияния коэффициентов проводилось путем обнаружения воздействий нарушителя по заранее определенной последовательности входных данных, в которой запрещенные действия совершены три раза. Проводилась оценка 27 вариантов различных наборов параметров модели. Предложенная модель реализована в виде многоагентной системы, показан пользовательский интерфейс агента при обнаружении нарушителя.

Внутренний нарушитель; оценка доверия; агент; событие информационной системы.

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

A.A. Beshta, A.M. Tsybulin

ALGORITHM OF INSADERS DETECTION BASED ON CONFIDENCE EVALUATION

The purpose of the research is development of algorithm of developed confidence evaluation model using for insiders detection. In this work the model of confidence evaluation, its parameters and coefficient are described. The algorithm of model is shown and sequence of action for insider detection is described. Also in this research influence of model coefficients on confidence value evaluation is investigated. Allowable coefficients values are defined. At first, these values are defined analytically. Obtained dependence let to set bounds. Secondary, values are defined with experiment on different sets of model parameters. Experiment consists in insider detection with predetermined sequence of the input data with three maliciously action. 27 sets of parameters are estimated. The range of optimal parameters for model is proposed. Described model implemented as multiagent system and agent user interface in the moment of insider detection is shown.

Insider; confidence evaluation; agent; information system event.

До сегодняшнего времени системы защита информации были ориентированы в большей степени на защиту периметра, каналов связи и инфраструктуры. В [1] показано, что в последнее время происходит все больше инцидентов информационной безопасности, связанными с внутренними угрозами, источниками которых являются внутренние нарушители, а также выделяется необходимость усиления защиты от них.

Подход с применением механизма оценки доверия позволяет анализировать действия самого пользователя, ставить ему в соответствие значение доверия и делать вывод о том, является ли пользователь нарушитель. Некоторые возможности такого подхода рассматривались [2, 3]. В статье предлагается алгоритм использования механизма оценки доверия для решения задачи обнаружения внутреннего нарушителя.

В [2, 3] показана модель оценки доверия, в которой 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:

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

где $\gamma = \gamma^+ + \gamma^-$; γ^+ – сигнал положительной направленности; γ^- – сигнал отрицательной направленности; ε – коэффициент достаточности и θ – коэффициент критичности. Одним из возможных источников сигналов могут быть события информационной системы, связанные с деятельностью пользователя (этот вопрос подробно рассматривался в работе [4]). 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 *T*.

Предложенная модель имеет следующие управляющие параметры:

- $\Omega = \left(\gamma^-\right)^\theta + \gamma^-$ – 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 $B_{E_i^{\tilde{T}}} = 1/2$.

Коэффициент достаточности ε указывает на то, какое количество сигналов необходимо, чтобы достигнуть уровня доверия 0,5, и позволяет контролировать скорость роста доверия к субъекту.

Коэффициент критичности θ позволяет контролировать величину падения уровня доверия к субъекту при появлении отрицательного сигнала.

Алгоритм обнаружения нарушителя включает в себя 10 шагов и показан на рис. 1.

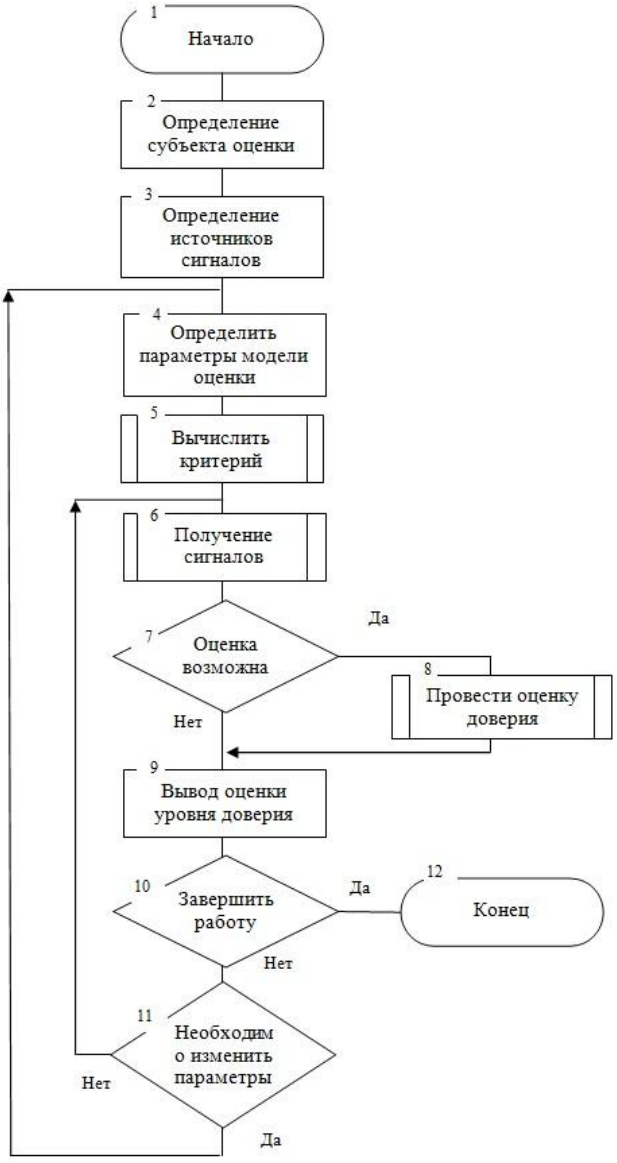

Рис. 1. Алгоритм оценки доверия

Шаг 1. Выбор субъекта для оценки (блок 2).

Шаг 2. Определение источников сигналов γ^+ и γ^- (блок 3).

Шаг 3. Определение параметров модели коэффициентов критичности и достаточности, интервала наблюдения *T*, вычисление управляющих параметров Ω и Ψ (блок 4).

Шаг 4. Определение критерия β, позволяющего обнаружить заданное количество отрицательных сигналов (блок 5). Подробнее о вычислении критерия β изложено в работе [5].

Шаг 5. Получение сигналов γ^+ и γ^- за один такт наблюдения *T* за субъектом (блок 6).

Шаг 6. Проверка условия $\gamma > \Omega$ из выражения 1, определяющего возможность оценки доверия (блок 7). Если оценка возможна – переход к шагу 7, иначе – шаг 8.

Шаг 7. Выполнение оценки доверия, вычисление $B_{E_i^{\tilde{T}}}$ по выражению (1) (блок 8).

Шаг 8. Сравнение оценки доверия с критерием и вывод результата (блок 9).

Шаг 9. Проверка необходимости завершения работы (блок 10). Если работа продолжается – переход к шагу 10, иначе – завершение работы.

Шаг 10. Проверка необходимости изменения параметров (блок 11). Если корректировка требуется – переход к шагу 3 (блок 4), иначе – продолжение работы на текущих параметрах модели, переход к шагу 5 (блок 6).

Данный алгоритм предполагает выбор коэффициентов модели, поэтому для решения этой задачи было проведено исследование влияния коэффициентов на значение уровня доверия и определены допустимые значения этих коэффициентов.

При выборе коэффициента достаточности ε следует руководствоваться тем, что он должен иметь целое положительное значение, и тем, что при $\gamma^- = 0$ и $\gamma = \varepsilon$ уровень доверия будет $B_{E_i^{\tilde{T}}} = 1/2$. При повышении коэффициента достаточности рост значения доверия замедляется. Влияние этого коэффициента особо значимо на начальном этапе наблюдения, а также при малом интервале наблюдений.

Выбор коэффициента критичности θ не так однозначен, однако можно учитывать следующие особенности, полученные при исследовании выражения (1):

- при $\gamma = \varepsilon$, $\gamma^- = 1$ величина θ не имеет значения, а уровень доверия снизится на величину $1/\varepsilon$;
- при $\gamma = \varepsilon$, $\theta = 1$ уровень доверия снизится на величину γ^-/ε, тогда $B_{E_i^{\tilde{T}}} = 0$ при $\gamma^- = \varepsilon/2$;
- при $\gamma = \varepsilon$, $\theta \neq 1$ уровень доверия снизится на величину $\Omega/2\varepsilon$, но при $\Omega > \varepsilon$ уровень доверия $B_{E_i^{\tilde{T}}} = 0$;
- при $\gamma = \varepsilon$, $\theta = \log_2(\varepsilon - 2)$ и двух отрицательных голосах $\gamma^- = 2$ уровень доверия $B_{E_i^{\tilde{T}}} = 0$.

Таким образом, с учетом указанных особенностей коэффициент критичности θ находится в интервале $1 \le \theta \le \log_2(\varepsilon - 2)$.

Экспериментальное исследование влияния коэффициентов проводилось путем обнаружения воздействий нарушителя по заранее определенной последовательности входных данных, в которой запрещенные действия были совершены три раза.

Для эксперимента были выбраны следующие значения коэффициента θ:

- условие 1 – $\theta = 1$;
- условие 2 – $\theta = 2$;
- условие 3 – $\theta = 3$.

Для коэффициента ε использовались значения 10, 20, 30. Значения интервала наблюдения и критерии были выбраны следующие: для T = 40 β = 0,5, для T = 80 β = 0,79, для T = 400 β = 0,96. Итого в эксперименте использовалось $3^3 = 27$ наборов параметров для модели.

Критерии β, позволяющие обнаружить различное количество отрицательных сигналов за наблюдаемый период, для различных периодов наблюдений показаны в табл. 1. Получение этих критериев подробнее описано в [5].

На рис. 2–4 показано влияние различных наборов параметров модели на значение оценки уровня доверия.

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

На рис. 2 видно, что критерий β = 0,5 можно использовать только для третьего условия. Пользователь считается нарушителем на протяжении 70 интервалов или 17,5 % времени наблюдения. При первом и втором условии обнаруживается только первое нарушение.

Рис. 2 Влияние различных наборов параметров (вариант 1)

На рис. 3 видно, что критерий β = 0,79 можно использовать для второго и третьего условия. Пользователь считается нарушителем на протяжении 75 % времени наблюдения. Для третьего условия можно понизить критерий до значения β = 0,6.

При наблюдении на протяжении 400 интервалов было изменено условие 3 (θ = 2,5). На рис. 4 видно, что критерий β = 0,96 не может быть использован. Для второго условия более приемлемо значение β = 0,6, при котором обнаруживаются три злоумышленных воздействия пользователя, и пользователь считается нарушителем на протяжении 46 % времени наблюдения.

Рис. 3 Влияние различных наборов параметров (вариант 2)

Общие результаты по всем 27 наборам параметров показаны в табл. 2. В таблице указан процент времени, при котором значение уровня доверия к субъекту ниже установленного критерия. В скобках указано одно необнаруженное воздействие, при этом результаты с двумя пропущенными воздействиями не рассматриваются.

Из рис. 2–4 и табл. 2 можно сделать вывод, что наиболее оптимальными значениями параметров являются следующие: $T \geq 80$; $\varepsilon \geq 20$; θ = 2–2,5; β = 0,6–0,8.

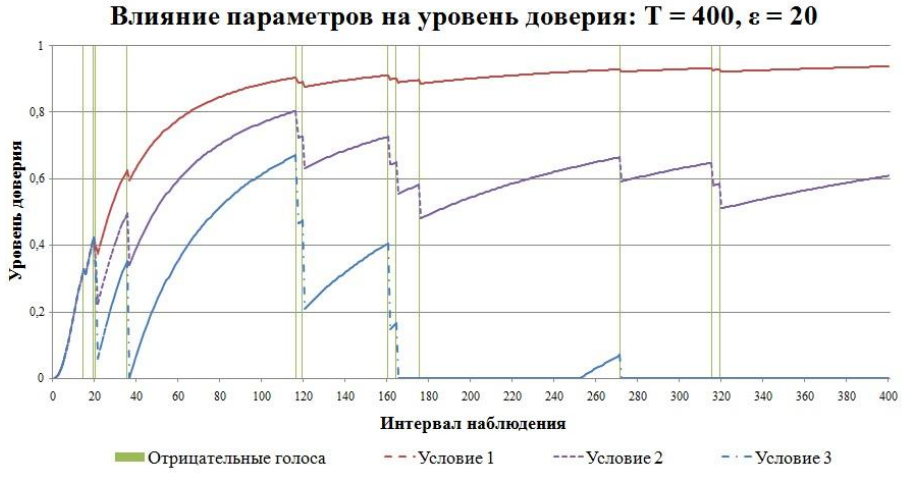

Рис. 4. Влияние различных наборов параметров (вариант 3)

Таблица 2

Значение уровня доверия ниже установленного критерия, %

		T		
ε	Условие	40	80	400
10	1	-	-	-
	2	-	33(1)	46
	3	16(1)	55	-
20	1	-		-
	2	-	33(1)	50
	3	20(1)	55	-
30	1	-	-	-
	2	20(1)	55	57
	3	30	70	-

Предложенный алгоритм обнаружения внутреннего нарушителя реализован в виде многоагентной системы. Подробнее о наборе агентов, входящих в систему, и их архитектурах показано в [5]. Полученные параметры использовались при обнаружении нарушителя в тестовой информационной системе. Пользовательский интерфейс агента мониторинга в момент обнаружения нарушителя показан на рис. 5.

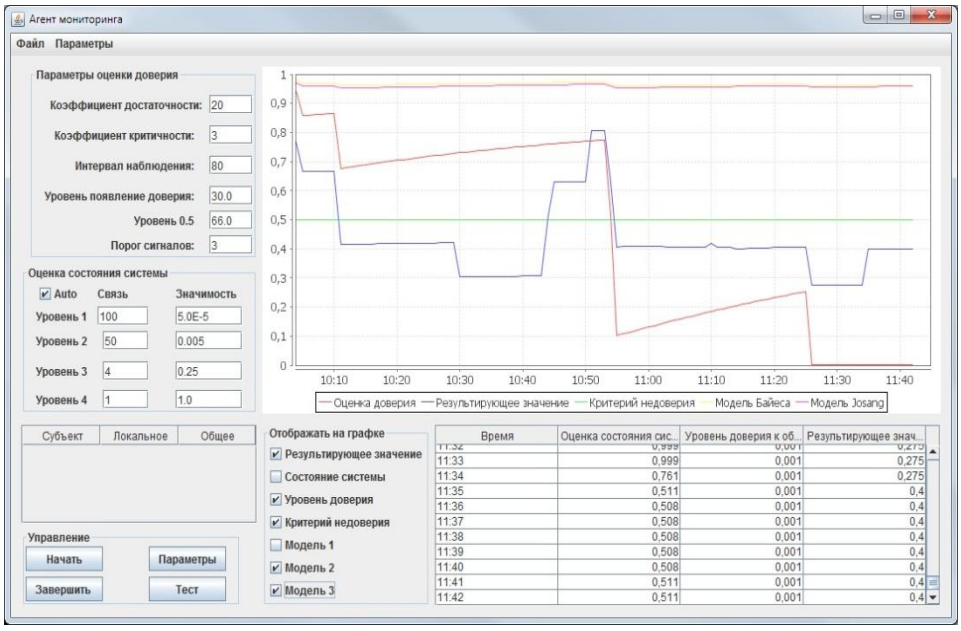

Рис. 5. Пользовательский интерфейс (экранная копия)

Выводы. Алгоритм для обнаружения внутреннего нарушителя состоит из 10 шагов и включает в себя установку параметров модели, выбор критерия, вычисления значения доверия. Аналитическое исследование модели оценки доверия позволило установить ограничения на значения ее коэффициентов, а экспериментальное исследование позволило определить оптимальные значения параметров модели. Вариация параметров модели позволяет использовать ее в различных условиях функционирования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Цыбулин А.М., Свищева М.Н.* Системный подход к повышению эффективности борьбы с инсайдерской деятельностью пользователей информационной системы организации // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 25-33.
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. *Бешта А.А., Новикова Ю.В.* Способ численной оценки состояния автоматизированной информационной системы // Научно-технический вестник Поволжья. – 2013. – № 2. – С. 89-92.
5. *Бешта А.А.* Архитектура программного комплекса контроля над внутренним злоумышленником // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 157-163.

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; старший преподаватель.

Цыбулин Анатолий Михайлович – e-mail: anatsybulin@yandex.ru; кафедра информационной безопасности; зав. кафедрой.

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

Tsybulin Anatoly Mihaylovich – e-mail: anatsybulin@yandex.ru; the department of information security; head of department.

УДК 681.5:004(07)

В.И. Васильев, И.В. Шарабыров

ОБНАРУЖЕНИЕ АТАК В ЛОКАЛЬНЫХ БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Беспроводные сети передачи данных, в том числе и локального типа, продолжают стремительно развиваться. При этом зачастую безопасность в данных сетях не соответствует необходимому уровню. Одним из наиболее актуальных средств защиты от беспроводных атак являются системы обнаружения вторжений. В связи с широкими возможностями методов интеллектуального анализа данных задачу анализа параметров сетевого трафика на предмет наличия признаков атаки можно решать путем применения данных методов. Приведен обзор сетевых атак, актуальных для локальных беспроводных сетей, а также методов интеллектуального анализа данных, которые можно использовать для обнаружения рассмотренных типов атак. В качестве методов интеллектуального анализа данных рассмотрены метод опорных векторов, метод k-ближайших соседей, нейронные сети и деревья принятия решений. Результаты экспериментов позволяют сделать вывод о практической значимости предложенного подхода к обнаружению атак в локальных беспроводных сетях.

Беспроводная сеть; сетевая атака; модель обнаружения; сигнатура; Wi-Fi.