УДК 004.942

ПОСТРОЕНИЕ МОДЕЛИ ДОВЕРИЯ К ОБЪЕКТАМ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПРЕДОТВРАЩЕНИЯ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ НА СИСТЕМУ

А.А. Бешта, М.А. Кирпо

Волгоградский государственный университет
E-mail: abewta@rambler.ru

Описана формальная модель деструктивного воздействия на систему, и выделены основные возможные деструктивные воздействия. Описана предложенная авторами модель доверия к объекту автоматизированной информационной системы на основе мониторинга действий объекта. Предложена сервис-ориентированная концепция предоставления услуг по обеспечению безопасности информации и реализующая ее многоагентная распределенная архитектура.

Ключевые слова:
Многоагентная система, деструктивное воздействие, оценка доверия к объекту, сервис-ориентированная архитектура.

Key words:
Multiagent system, destructive influence, object trust assessment, service oriented architecture.

Автоматизированные информационные системы (АИС), реализуемые на компьютерах, состоят из множества разнородных, распределенных в пространстве компонентов: аппаратных средств, системных утилит, пользовательских приложений, средств защиты информации, массивов данных и персонала. При этом данные компоненты генерируют множество событий, связанных с действиями пользователей, процессами обработки информации, получением и отправкой сетевых пакетов, доступом к файлам. Дальнейший анализ этих событий позволяет выявить различные нарушения информационной безопасности.

Для повышения эффективности работы АИС, снижения нагрузки на ресурсы и уменьшения объема анализируемой информации предлагается использовать сервис-ориентированную архитектуру системы защиты информации. Кроме того, подобная архитектура позволяет повысить гибкость и масштабируемость АИС и легко интегрировать в нее новые компоненты [1].

Формально АИС можно представить в виде:

$$S = \{E^T, R^E\},$$

где E^T – множество объектов различных типов T информационной системы S, $E^T = \bigcup_{i=1,n} E_i^T$, где n – количество объектов класса T; R^E – множество отношений между объектами, $R^E = E^T \times E^T$.

Каждый класс E^T представляет собой совокупность однотипных объектов, описанных с помощью набора свойств:

$$E_i^T = \bigcup_{k=1,m} P_k^{E_i^T},$$

где $P_k^{E_i^T}$ – k-е свойство i-го объекта E_i^T типа T.

Все объекты АИС могут быть разделены на две группы: активные и пассивные. Активные объекты могут выполнять различные операции над другими объектами (пассивными и активными), в том числе над собой. К пассивным объектам относятся все другие объекты.

Типы объектов T можно определить следующим набором:

$$T = \tilde{T} \cup \bar{T} = \langle C, U \rangle \cup \langle H, A, R \rangle,$$

где $\tilde{T}$=<C,U> – активные объекты типов C (программный компонент, процесс) и U (пользователь), $\bar{T}$=<H,A,R> – пассивные объекты типов H (аппаратный компонент), A (актив), R (разрешение).

Тогда система будет состоять из следующих типов объектов E^T={E^H,E^C,E^U,E^A,E^R}, где E^H – множество узлов; E^C – множество компонентов; E^U – множество пользователей; E^A – множество активов; E^R – множество разрешений.

Множество отношений между объектами R^E описывается непересекающимся объединением:

$$R^E = R_{is}^E \cup R_{part}^E, R_{is}^E \cap R_{part}^E \neq 0,$$

где R_{is}^E – отношение категоризации между объектами; R_{part}^E – отношение принадлежности между объектами.

Такое представление системы позволяет определить распределение отдельных объектов и их свойств по АИС, то есть:

$$p(E_i^T) = \frac{\sum E_i^T}{\sum E^T},$$

где $p\,(E_i^T)$ – доля объектов E_i^T среди объектов определенного типа E^T.

$$p(P_k^{E_i^T}) = \frac{\sum P_k^{E_i^T}}{\sum P^{E^T}},$$

где $p(P_k^{E_i^T})$ – распределение свойства $P_k^{E_i^T}$ среди свойств объектов типа E^T.

Таким образом, несмотря на разнородность компонентов АИС, можно определить конечное множество типовых объектов, характерных для всей системы, и выделить свойства, идентичные для многих объектов.

Для определения деструктивного воздействие на объекты АИС сначала необходимо определить

нормальное воздействие, осуществляемое активными объектами в процессе работы.

Нормальное допустимое воздействие определяется в виде правила R, установленного в системе, которое устанавливает допустимое действия *Act* для активного объекта по отношению к другому объекту:

$$R = (E_i^{\tilde{T}} \to Act) \mid E_j^T .$$

Каждое правило означает, что активный объект $E_i^{\tilde{T}}$ может выполнить некоторое действие по отношению к объекту E_j^T.

В качестве множества простых действий *Act* можно определить:

$$Act = \langle Read, Write, Execute \rangle,$$

где *Read* – операция чтения; *Write* – операция записи; *Execute* – операция выполнения.

Тогда нормальное воздействие $Sa_{E_i^{\tilde{T}}}$, осуществляемое активным объектом $E_i^{\tilde{T}}$, описывается следующим образом:

$$Sa_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v \mid \exists R = (E_i^{\tilde{T}} \to Act) \mid E_j^T$$

и означает, что некоторый объект E_i^T системы имеет свойство $P_k^{E_i^T}$ со значением v, которое позволяет активному объекту $E_i^{\tilde{T}}$ выполнить действие *Act* по отношению к некоторому объекту E_j^T (возможно, тому же самому).

Но может существовать такое значение $v^* \neq v$ свойства $P_k^{E_i^T}$, что оно позволяет создать в системе новое правило $R^* \notin R$, в котором нарушается установленное соотношение между $E_i^{\tilde{T}}$, *Act*, E_j^T, что означает выполнение в системе действия *Na*, которое не установлено в системе в виде правила. Такое действие является деструктивным по отношению к объекту E_j^T и может нанести вред как отдельным объектам, так и всей автоматизированной системе в целом:

$$Na_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v^* \mid \exists R^* = (E_i^{\tilde{T}} \to Act) \mid E_j^T, R^* \notin R,$$

то есть у некоторого объекта E_i^T существует такое значение v^* некоторого его свойства $P_k^{E_i^T}$, что имеется возможность в обход установленных в системе правил R установить новое правило R^*, позволяющее для некоторого активного объекта $E_i^{\tilde{T}}$ выполнить какое-то действие *Act* по отношению к некоторому объекту E_j^T.

Теперь можно описать различные типы деструктивных воздействий на объекты АИС в терминах этой модели.

Ознакомление:

$$Know_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v^* \mid \exists R^* =$$

$$= (E_i^{\tilde{T}} \to \mathrm{Re}\, ad) \mid E_j^T, R^* \notin R.$$

Копирование:

$$Copy_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v^* \mid \exists R^* =$$

$$= (E_i^{\tilde{T}} \to Write) \mid E_j^T, R^* \notin R, i \neq j.$$

Модификация:

$$Modify_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v^* \mid \exists R^* =$$

$$= (E_i^{\tilde{T}} \to Write) \mid E_i^T, R^* \notin R.$$

Удаление:

$$Rem_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v^* \mid \exists R^* =$$

$$= (E_i^{\tilde{T}} \to Write) \mid Null, R^* \notin R.$$

Запуск:

$$Exec_{E_i^{\tilde{T}}} \to P_k^{E_i^T} = v^* \mid \exists R^* =$$

$$= (E_i^{\tilde{T}} \to Execute) \mid E_j^T, R^* \notin R.$$

С другой стороны, для всех активных объектов АИС можно поставить в соответствие уровень доверия к объекту $B_{E_i^{\tilde{T}}} \in (0,1)$.

В данном случае под уровнем доверия к объекту понимается ожидаемая реакция объекта – что можно ожидать от объекта в различных ситуациях и взаимодействиях [2].

Тогда высоким уровнем доверия $B_{E_i^S} \to 1$ может обладать объект, который не является источником деструктивных воздействий.

Низким уровнем доверия $B_{E_i^{\tilde{T}}} \to 0$ обладают объекты, только что появившиеся в системе, ранее неизвестные объекты, то есть объекты, которые являются или могут являться источником деструктивных воздействий.

То есть уровень доверия к объекту – это вероятность того, что объект не является источником деструктивного воздействия $Na_{E_i^{\tilde{T}}}$:

$$B_{E_i^{\tilde{T}}} = 1 - p(Na_{E_i^{\tilde{T}}}).$$

На конечном рабочем месте пользователя в некоторый момент времени могут функционировать только объекты определенных типов.

Возникает задача контроля уровня доверия к объектам системы и выполнения функций защиты при функционировании активных объектов с уровнем доверия ниже установленной нормы $B_{E_i^{\tilde{T}}} < \beta$. При этом необходимо выполнять защитные функции, связанные с конкретным объектом $E_i^{\tilde{T}}$, а не всей системой.

При оценке уровня доверия к объектам необходимо учитывать, что распространенность объекта повышает его уровень доверия. В то время как малораспространенные объекты имеют низкий уровень доверия. Если объект является или может являться источником (участником) деструктивных воздействий, то его уровень доверия понижается.

Пусть уровень доверия к объекту $E_i^{\tilde{T}}$ складывается из голосов $\gamma = (\gamma^+ \cup \gamma^-)$, поданных за этот объект: γ^+ – положительный голос и γ^- – отрицательный голос. Если в системе обнаружено событие, указывающее на то, что объект попытался выполнить или выполнил некоторое деструктивное воздействие в обход установленных в системе правил, за него подается отрицательный голос γ^-. Если за некоторое время наблюдения объект не был источником деструктивного воздействия, за него подается положительный голос γ^+.

С учетом особенностей для получения оценки уровня доверия к объекту можно использовать функцию следующего вида:

$$F(\varepsilon,\theta,\gamma)=\frac{\gamma^{+}-(\gamma^{-})^{\theta}}{\gamma+\frac{\varepsilon^{2}}{\gamma}}, \quad (1)$$

где γ^{+} – количество положительных голосов, поданных за объект; γ^{-} – количество отрицательных голосов, поданных за объект; γ – общее количество голосов, поданных за объект; ε – коэффициент, определяющий степень значимости положительного голоса (коэффициент достаточности); θ – коэффициент, определяющий степень значимости отрицательного голоса (коэффициент критичности).

Эта функция имеет некоторые ограничения:

- так как значение доверия к объекту находится в интервале $B_{E_i^{\tilde{T}}}\in(0,1)$, а область значений функции (1) находится в интервале $F(\varepsilon,\theta,\gamma)\in(-\infty,1)$, то при $F(\varepsilon,\theta,\gamma)<0$ нельзя говорить о доверии к объекту. Поэтому можно определить $\gamma=\Psi$, при котором $F(\varepsilon,\theta,\Psi)=0$;
- величина Ω зависит от количества отрицательных голосов γ^{-} и коэффициента θ, определяющего степень значимости отрицательного голоса. Из равенства $F(\varepsilon,\theta,\Psi)=0$ можно показать, что $\Omega=(\gamma^{-})^{\theta}+\gamma^{-}$;
- можно определить значение $\gamma=\Psi$, при котором функция достигает середины уровня доверия $F(\varepsilon,\theta,\Psi)=1/2$. Если $\gamma^{-}=0$, то равенство $F(\varepsilon,\theta,\Psi)=1/2$ достигается при $\Psi=\varepsilon$. Если $\gamma^{-}\neq 0$, то равенство $F(\varepsilon,\theta,\Psi)=1/2$ достигается при $\Psi=\Omega+\sqrt{\Omega^{2}+\varepsilon^{2}}$.

С учетом установленных ограничений значение оценки уровня доверия к объекту АИС вычисляется следующим образом:

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

Выражение (2) можно назвать (ε,θ) доверительной моделью объекта.

Коэффициент достаточности ε указывает на то, какое количество голосов должен получить объект, чтобы достигнуть уровня доверия 0,5, и позволяет контролировать скорость роста доверия к объекту.

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 $B_{E_i^{\tilde{T}}}=1/2$.

На рис. 1 показано влияние коэффициента достаточности ε на значение оценки уровня доверия. Все голоса, поданные за объект, являются положительными.

Коэффициент критичности θ позволяет контролировать величину падения уровня доверия к объекту при появлении деструктивного воздействия.

Выбор коэффициента критичности θ не так однозначен, однако можно учитывать следующие рекомендации:

- 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 $\gamma^{-}=\varepsilon$, тогда $B_{E_i^{\tilde{T}}}=0$ при $\gamma^{-}=\varepsilon/2$;
- при $\gamma=\varepsilon$, $\theta\neq 1$ уровень доверия снизится на величину Ω/ε, но при $\Omega>\varepsilon$ уровень доверия $B_{E_i^{\tilde{T}}}=0$;
- при $\gamma=\varepsilon$, $\theta=\log(\varepsilon-2)$ и двух отрицательных голосах $\gamma^{-}=2$ уровень доверия $B_{E_i^{\tilde{T}}}=0$.

На рис. 2 показано влияние отрицательных голосов на значение оценки уровня доверия при параметрах $\varepsilon=20$ и $\theta=2$.

При оценке уровня доверия к объекту $E_i^{\tilde{T}}$ возникает задача сбора голосов $\gamma=(\gamma^{+}\cup\gamma^{-})$, поданных за данный объект.

Пусть на компонентах АИС распределены агенты мониторинга.

Тогда голоса за объект могут подаваться агентами мониторинга следующим образом:

$$\gamma=\begin{cases}\gamma^{+}, \text{ если } Sa_{E_i^{\tilde{T}}},\\ \gamma^{-}, \text{ если } Na_{E_i^{\tilde{T}}}.\end{cases}$$

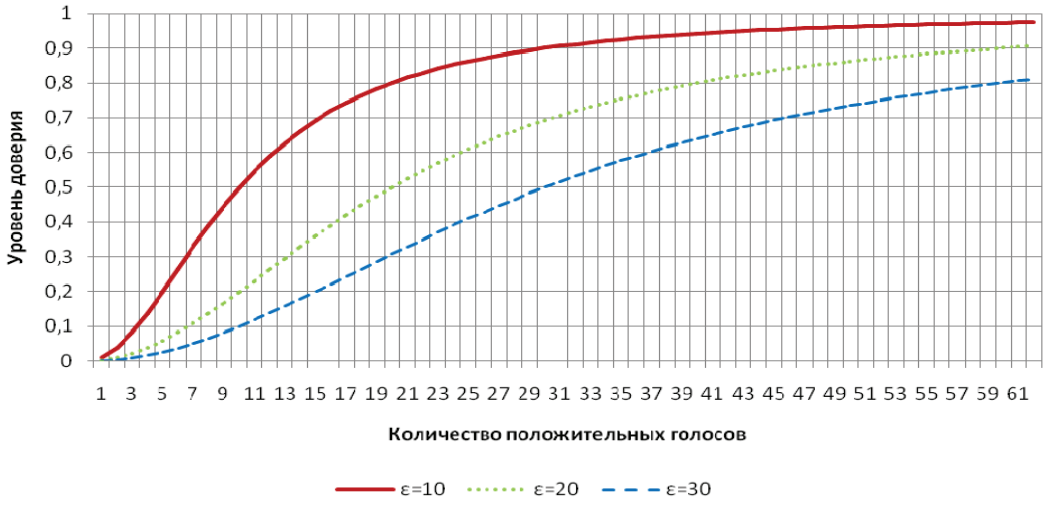

Рис. 1. *Влияние параметра ε на уровень доверия к объекту*

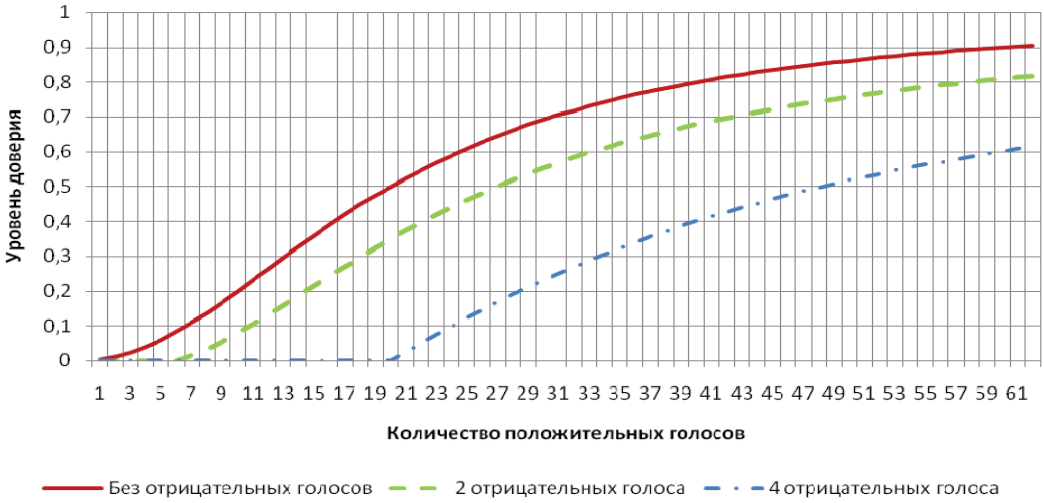

Рис. 2. *Влияние отрицательных голосов на уровень доверия к объекту (γ^-=0, γ^-=2 и γ^-=4)*

Если агент обнаруживает попытку объекта $E_i^{\tilde{T}}$ совершить деструктивное воздействие $Na_{E_i^{\tilde{T}}}$, он подает отрицательный голос γ^-. Если объект $E_i^{\tilde{T}}$ совершает нормальное воздействие $Sa_{E_i^{\tilde{T}}}$, агент мониторинга подает положительный голос γ^+.

Если уровень доверия опускается ниже установленного критерия $B_{E_i^S}<\beta$, агент мониторинга выполняет блокировку подозрительного объекта или другое управляющее воздействие.

Тогда с учетом объектов, определенных выше, многоагентная система защиты может выглядеть следующим образом:

$$A^S = \{A_M, \langle A_{sc}, A_{ssw}, A_{usw}, A_{ac}\ A_{net}, A_{db}, A_{dev}\rangle\},$$

где A_M – агент координатор мониторинга; A_{sc} – агент мониторинга системных компонент; A_{ssw} – агент мониторинга системного программного обеспечения; A_{usw} – агент мониторинга пользовательского программного обеспечения; A_{ac} – агент мониторинга доступа; A_{net} – агент мониторинга сетевых соединений; A_{db} – агент мониторинга баз данных; A_{dev} – агент мониторинга внешних устройств.

Таким образом, агенты координаторы, расположенные на конечных рабочих местах пользователей, выполняют мониторинг объектов на данном рабочем месте.

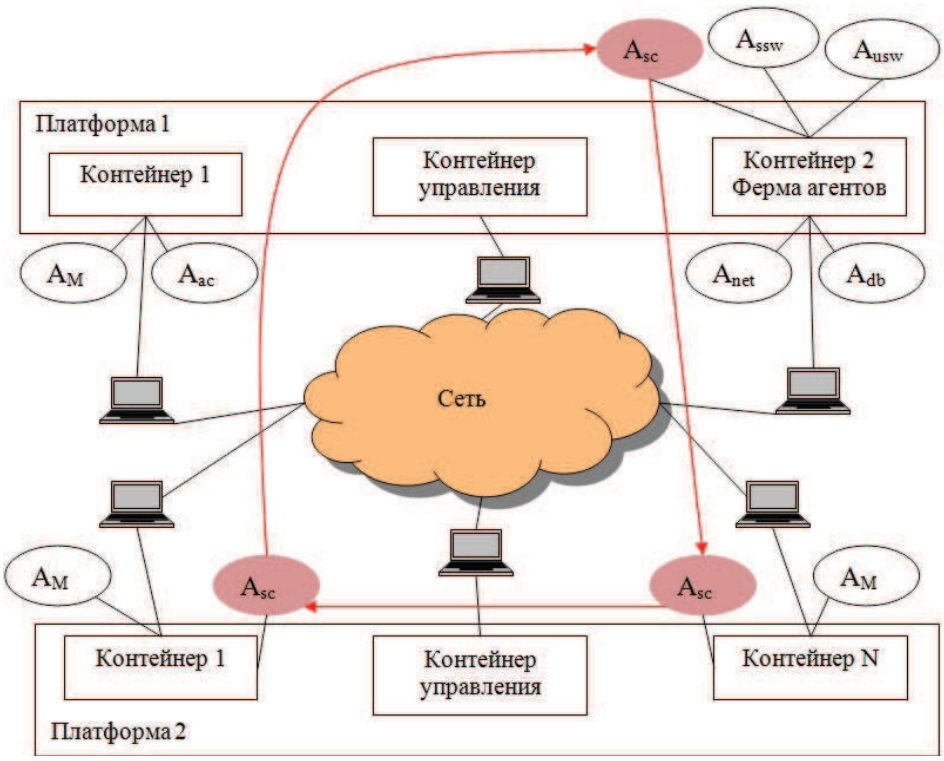

Рис. 3. *Расположение агентов в системе и их миграция*

При появлении объектов определенного типа агент координатор запрашивает специализированного агента мониторинга. Если этот агент обнаруживает объект с низким уровнем доверия, или возникает подозрение на выполнение деструктивных воздействий, агент мониторинга выполняет определенные функции безопасности.

При завершении использования объектов определенного типа работа специализированного агента мониторинга завершается.

Специализированные агенты мониторинга находятся в центральном хранилище – ферме агентов. Каждый агент публикует сведения о предоставляемых сервисах безопасности, и агенты координаторы запрашивают выполнение функций безопасности этими специализированными агентами. При запросе агент мониторинга мигрирует с фермы на конечное рабочее место, выполняет работу и возвращается обратно на ферму (рис. 3).

Таким образом, агент мониторинга выступает сервисом, который заказывает агент координатор.

На схеме также представлены блоки [3]:

- контейнер – агентная среда на конечном рабочем месте в автоматизированной информационной системе;
- платформа – группа контейнеров, объединенная одним блоком управления, реализующим агентную парадигму.

Описанный подход позволяет контролировать изменения среды функционирования АИС и появление новых компонентов, повышает эффективность функционирования конечных рабочих мест пользователей за счет использования средств защиты как сервисов, которые вызываются по необходимости. При этом все компоненты имеют некоторый уровень доверия, что позволяет гибко управлять защитой АИС и контролировать ее защищенность.

СПИСОК ЛИТЕРАТУРЫ

1. Ткаченко Н.И., Спирин Н.А. Применение сервис-ориентированной архитектуры при интеграции систем управления технологическими процессами // Известия Томского политехнического университета. – 2010. – Т. 317. – № 5. – С. 61–67.
2. Новиков Д.А. Математические модели формирования и функционирования команд. – М.: Изд-во физико-математической литературы, 2008. – 184 с.
3. Bellifemine F., Caire G. Developing Multi-Agent Systems with JADE. – Chichester: John Wiley & Sons Ltd., 2007. – 286 p.

Поступила 21.09.2012 г.

УДК 550.8.053

АНАЛИЗ ИНФОРМАЦИОННЫХ СВОЙСТВ ВЗАИМНЫХ ФАЗОВЫХ СПЕКТРОВ ОТРАЖЕННЫХ СЕЙСМИЧЕСКИХ ВОЛН

В.П. Иванченков, А.И. Кочегуров, М.А. Черкасова*

Томский политехнический университет
*ЗАО «Гринатом», г. Северск
E-mail: kai@cc.tpu.edu.ru

На основе принятой модели слоистых поглощающих сред рассмотрены свойства взаимных фазовых спектров сейсмических волн, отраженных от кровли и подошвы исследуемой толщи, определены основные предпосылки их применения для прогноза геологического разреза.

Ключевые слова:
Линейная система, модель слоистой поглощающей толщи, взаимный фазовый спектр сигналов, коэффициенты отражения и преломления волн.

Key words:
Linear system, model of layered absorbing column, mutual phase spectrum of signals, reflection and wave refraction factors.

При решении задач прогноза геологического разреза (ПГР), в том числе прогноза нефтегазоносности осадочных толщ, по данным сейсмических наблюдений наиболее широко используются в качестве диагностических признаков динамические характеристики отраженных волн, непосредственно связанные с их амплитудой и энергией [1, 2]. Информация о свойствах фазочастотных характеристик (ФЧХ) сейсмических волн до последнего времени практически не использовалась. Между тем в фазу сейсмических сигналов, а точнее в сложный закон изменения их фазовых спектров, заложена информация, позволяющая в условиях априорной неопределенности надежно обнаруживать и разрешать сигналы на фоне интенсивных помех, производить оценку их кинематических параметров [3, 4]. Как показано в [5, 6], текущие фазовые спектры отраженных сейсмических волн могут