

# Мониторинг подозрительных операций

# Содержание

ВВЕДЕНИЕ	2
ГЛАВА 1. ОБЩИЕ ПРИНЦИПЫ МОНИТОРИНГА	3
ГЛАВА 2. НАСТРОЙКА КРИТЕРИЕВ ОЦЕНКИ ПОДОЗРИТЕЛЬНОСТИ	5
Настройка критериев	5
Использование Схем Контроля Рисков при настройке критериев	8
ГЛАВА 3. АНАЛИЗ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ	9
Список подозрительных операций	9
Список операций, сгруппированных по критериям	12
Список подозрительных операций, сгруппированный по картам	13
Формирование списка подозрительных операций	14

## Введение



В системе WAY4™ реализована возможность мониторинга операций в режиме on-line по специально заданным параметрам. Модуль мониторинга (CSA – Card Suspect Activity Monitoring) ведет расчет уровня риска подозрительных операций и, на основании этого, транзакции, распознанные как подозрительные, могут быть отклонены автоматически.

Настоящий документ предназначен для сотрудников службы безопасности, занимающихся мониторингом рисков по карточным операциям.

При работе с данным документом рекомендуется пользоваться следующими источниками из комплекта документации OpenWay:

- "Контроль рисков";
- "Документы и их обработка";
- "Общие перечни системы WAY4™";
- "Пакеты Сервисов системы WAY4™".

В документе используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- названия кнопок экранных форм приводятся в квадратных скобках, например [Approve];
- последовательность выбора пункта в меню пользователя отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- комбинации клавиш, используемые при работе с DB Manager, приводятся в угловых скобках, например <Ctrl>+<F3>;
- предостережения в связи с возможностью совершения неправильных действий отмечены знаком ;
- сообщения, помеченные знаком , содержат информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

## Глава 1. Общие принципы мониторинга

Каждая операция проверяется по критериям оценки подозрительности, заданным для всех банковских карт, и по критериям, являющимся параметрами Схемы Контроля Рисков, относящейся к соответствующему карточному контракту или Пакету Сервисов данного контракта.

В системе имеется специальная форма для настройки критериев, по которым операция может быть признана подозрительной (см. "Настройка критериев оценки подозрительности").

Параметры, заданные для всех банковских карт, могут быть переопределены параметрами Схемы Контроля Рисков, для этого наименования параметров, заданных для всех банковских карт и заданных в отдельной Схеме Контроля Рисков должны совпадать.

Критерии могут иметь пороговые значения по сумме или количеству операций, при превышении этого порогового значения операция оценивается как подозрительная.

Все критерии модуля мониторинга настраиваются при помощи комбинирования запрограммированных условий проведения операций и варьируемых параметров.

К запрограммированным условиям проведения операций относится распознавание системой определенных типов нарушения, а именно:

- смена страны при выполнении операций по одной банковской карте в течение заданного периода времени;
- повторение операций по одной банковской карте на устройстве одного и того же торговца в течение заданного периода времени;
- операции, в результате которых сумма доступных средств на карте уменьшается на указанное количество процентов от текущего состояния;
- многократные последовательные попытки выполнить операцию по одной и той же банковской карте с последовательным уменьшением суммы операции в течение заданного периода времени;
- многократные неуспешные попытки ввода PIN-кода.

К варьируемым параметрам относятся:

- сумма операции или процент от остатка на счете;
- наблюдаемый период;
- количество разрешенных операций;
- характеристики места проведения операции (страна, категория торговца, торговец);
- реакция на нарушение данного ограничения (например, блокирование карты или уведомление держателя карты о совершенной операции).

В результате выполнения проверки (см. "Анализ подозрительных операций"), подозрительные операции регистрируются в специальной форме и могут быть отклонены с указанным отрицательным кодом ответа.

Зарегистрированная запись о подозрительной операции имеет статус "Active". В результате выяснения обстоятельств операции пользователь может присвоить записи статус "Inactive" или "Closed".

## Глава 2. Настройка критериев оценки подозрительности

### Настройка критериев

Настройка критериев оценки подозрительности выполняется в форме "Full → Stop List → Merchant Stop List" (см. Рис. 1)

Card Risk Monitoring Rules											<< < > >>			9 of 11	
Group Code	Area	Merchant Bant	SIC	ans Condit	Spc Condition	Resp Code	Active	Date From	Date To	iv (Ho mit Cui	Amnt / %	Limit			
Risky Country					Check Usage	Successfully complete	Yes	26/10/2004	00/00/0000	24		0.00/15			
Amount Fitting					Amount Fitting	Successfully complete	Yes	26/10/2004	00/00/0000	24		0.00/15			
The Same Merchant					The Same Mercha	Successfully complete	Yes	26/10/2004	00/00/0000	24		0.00/15			
Risky SIC Group				POS Key Ent		Refer to card issuer	Yes	26/10/2004	00/00/0000	24		0.00/15			
Risky SIC			7995 Casino			Successfully complete	Yes	26/10/2004	00/00/0000	24		0.00/15			
Single Amount						Do not Honour	Yes	26/10/2004	00/00/0000	0	USD	800.00/15			
Change Country					Change Country	Successfully complete	Yes	26/10/2004	00/00/0000	24		0.00/15			
Amount Fitting		ANY_BIN			Amount Fitting	Successfully complete	Yes	05/04/2005	00/00/0000	0		0.00/0			
Utilization					Utilization	Successfully complete	Yes	26/10/2004	00/00/0000	24		80.00/0			
Total Amount						Successfully complete	Yes	26/10/2004	00/00/0000	2	USD	1,000.00/0			
Utilization 6h					Utilization	Successfully complete	Yes	10/06/2004	00/00/0000	6		90.00/0			
◀															
Ins	Del	Query	Full Info												

Рис. 1. Форма для настройки критериев подозрительности операций

Для удобства ввода параметров предназначена форма "Full Info for <наименование критерия>" (см. Рис. 2), которая открывается при нажатии на кнопку [Full Info] в форме "Merchant Stop List".

Full Info for [Empty]		
<b>Parameter</b> Group Code: <input type="text"/> Comment: <input type="text"/>  <b>Risk Scheme Rules</b> Switch Tag: <input type="text"/> Activated For Scheme (Single): <input type="text"/> Scheme (Group): <input type="text"/>	<b>Criteria</b> Merchant BIN: <input type="text"/> Trans Cond: <input type="text"/> SIC: <input type="text"/> Area: <input type="text"/> Merchant Name: <input type="text"/> Special Params: <input type="text"/>	<b>Limits</b> Limit Interval: <input type="text"/> 0 (Hours) Limit Curr: <input type="text"/> Limit Amount: <input type="text"/> 0.00 Limit Number: <input type="text"/> 0
<b>Actions</b> Resp Code: <input type="text"/> Successfully completed Event Type: <input type="text"/> Suspect Factor: <input type="text"/> 1,000 Activity Period: <input type="text"/> 12/12/2005 <input type="text"/> 00/00/0000 Activity Tag: <input type="text"/>		

Рис. 2. Форма для просмотра и ввода полной информации о критериях подозрительности операций

Форма для настройки критериев содержит следующие поля, разделенные на несколько блоков;

- *Group Code* – код критерия, который будет указываться в протоколе выполнения процессов WAY4™ (Process Log) при регистрации операции в списке подозрительных; рекомендуется соблюдать уникальность кода;
- *Comment* – дополнительная информация о критерии; если в данное поле поместить тег TRCITY= <Наименование города>, то данный критерий будет действовать только для документов, у которых поле TRANS\_CITY соответствует указанному значению. Другими словами,

критерий будет проверяться только для транзакций, выполняемых в указанном городе;

Поля группы "Risk Scheme Rules" используются для настройки критерия для группы карт или отдельной карты. Для того чтобы критерий действовал для всех карт, следует оставить данные поля незаполненными. Использование полей группы "Risk Scheme Rules" описано в параграфе "Использование Схем Контроля Рисков при настройке критериев".

Группа "Criteria" содержит поля, предназначенные для детальной настройки параметров подозрительности:

- *Merchant BIN* – присвоенный платежной системой BIN торговца, на устройстве которого была выполнена операция; поле может содержать как непосредственно значение BIN, так и одно из следующих значений:
  - *ON\_US* – операция будет проверяться по данному критерию, только если она выполняется на устройстве торговца, который зарегистрирован в системе;
  - *FOREIGN* – операция будет проверяться по данному критерию, только если она выполняется на устройстве торговца, который не зарегистрирован в системе;
  - *ANY\_BIN* – независимо от того, зарегистрирован ли торговец в системе, операция будет проверяться по данному критерию;
- *Trans Condition* – условия выполнения операции (см. раздел "Условия (Transaction Conditions)" документа "Документы и их обработка");
- *SIC* – код, определяющий тип торговой точки (SIC/MCC) в соответствии с характером бизнеса (см. раздел "Перечень "SIC Group"" документа "Общие перечни системы WAY4");
- *Area* – название региона, в котором была совершена сделка (см. раздел "Поддержка регионов" документа "Общие перечни системы WAY4");
- *Merchant Name* – наименование торговца, на устройстве которого была выполнена операция;
- *Special Parms* – поле для указания критериев, которые проверяются по соглашению кодов (программных критериев); в системе могут использоваться следующие программные критерии:
  - *"CHANGE\_COUNTRY"* (Change Country) – смена страны при выполнении операций по одной банковской карте в течение заданного периода;
  - *"THE\_SAME\_MERCHANT"* (The Same Merchant) – повторение операций по одной банковской карте на устройстве одного и того же торговца в течение заданного периода;
  - *"AMOUNT\_FITTING"* (Amount Fitting)– многократные попытки выполнить операцию по одной и той же карте с последовательным уменьшением суммы операции в течение заданного периода времени;

- "UTILIZATION" (Utilization) – операции, в результате проведения которых сумма доступных средств на карте уменьшается на указанное количество процентов от текущего состояния;
- "INVALID\_PIN" (Invalid PIN) – многократные попытки ввода PIN;
- критерий "Check Usage" используется следующим образом: если при проведении авторизации операция удовлетворяет параметрам данного критерия, система проверяет, настроен ли для контракта, по которому выполняется операция, ограничитель (Usage Limiter) с типом "Risk Rule ". Если такой ограничитель настроен, то по его параметрам задействуются счетчики (о принципах работы и настройке ограничителей см. документ "Ограничители активности контракта"). Если счетчики переполняются, ограничитель срабатывает, операция попадает в список подозрительных;

Группа полей "Limits" содержит поля, предназначенные для указания пороговых значений:

- *Limit Interval (Hours)* – интервал времени в часах, в течение которого операции по карте анализируются в соответствии с критерием; система анализирует операции по данной карте за указанное количество часов;
- *Limit Curr* – валюта, в которой задается пороговое значение суммы операций;
- *Limit Amount* – числовое значение, с помощью которого определяется пороговое значение суммы транзакций; данное поле может содержать:
  - сумму транзакций по карте за заданный период (кроме случая, когда полю *Special Parms* присвоено значение "UTILIZATION");
  - процент от суммы доступных средств на карте в случае, если полю *Special Parms* присвоено значение "UTILIZATION";
- *Limit Number* – пороговое количество операций, начиная с которого сделка регистрируется как подозрительная;

Группа полей "Actions" содержит следующие поля:

- *Resp Code* – код ответа системы по результатам анализа операции; используя код отрицательного ответа в этом поле, можно настроить критерии, по которым подозрительные операции будут отклоняться;
- *Event Type* – наименование системного события, которое должно быть открыто для карты в случае, если транзакция по ней будет определена как подозрительная;
- *Suspect Factor* – множитель, позволяющий увеличить удельный вес данного критерия подозрительности;
- *Activity Tag* – поле может принимать одно из следующих значений: "Yes" – по данному критерию выполняется анализ операций; "No" – не выполняется;
- с помощью полей *Activity Period* задается период времени, в течение которого данный критерий активен либо неактивен.



На расчет общей суммы авторизаций за период, заданный в параметрах мониторинга подозрительных операций, влияют значения тега CH\_ST\_LST. Этот тег указывается в поле *Additional Criteria* формы "Full Info For...", открываемой после нажатия на кнопку [Full Info] в форме "Merchant Stop List" (Full → Stop List → Merchant Stop List). В качестве значений тега через запятую задается список кодов, соответствующих статусам записей таблицы CREDIT\_HISTORY.credit\_status, которые будут анализироваться в рамках данного правила.

## Использование Схем Контроля Рисков при настройке критериев

С помощью Схем Контроля Рисков в системе существует возможность присвоения отдельного критерия группе контрактов или отдельной карте.

Для этого необходимо выполнить следующие настройки:

- Зарегистрировать Схему Контроля Рисков. О настройке Схем Контроля Рисков см. документ "Контроль рисков (настройка отчетности)".
- В зависимости от того, группе контрактов или отдельному контракту необходимы дополнительные критерии, выполняются следующие действия:
  - Пакету Сервисов назначается созданная Схема Контроля Рисков (см. документ "Пакеты Сервисов системы WAY4™"). В этом случае операции по всем контрактам, использующим данный Пакет Сервисов, будут анализироваться по выбранному критерию.
  - Контракту назначается созданная Схема Контроля Рисков (см. документ "Модуль эмиссии"). В этом случае операции по данному контракту будут анализироваться по выбранному критерию.
- В форме "Full Info for <наименование критерия>" (см. Рис. 2) необходимо заполнить поля группы "Risk Scheme Rules":
  - *Switch Tag* – поле может принимать следующие значения:
    - ♦ "Activate For" – критерий активен для контрактов со Схемой Контроля Риска, указанной в поле *Scheme (Single)*, либо для контрактов со Схемами Контроля Риска, указанными в поле *Scheme (Group)*;
    - ♦ "Inactivate For" – критерий не действует на контракты со Схемой Контроля Риска, указанной в поле *Scheme (Single)*, либо на контракты со Схемами Контроля Риска, указанными в поле *Scheme (Group)*;
  - *Scheme (Single)* – поле со списком для указания отдельной Схемы Контроля Рисков,
  - *Scheme (Group)* – текстовое поле для перечисления через ";" списка кодов Схем Контроля Рисков.

Таким образом, поля группы "Risk Scheme Rules" предназначены для настройки связи между критерием и группой контрактов.

## Глава 3. Анализ подозрительных операций

Для анализа подозрительных операций предназначена группа меню пользователя "Monitoring" (см. Рис. 3).

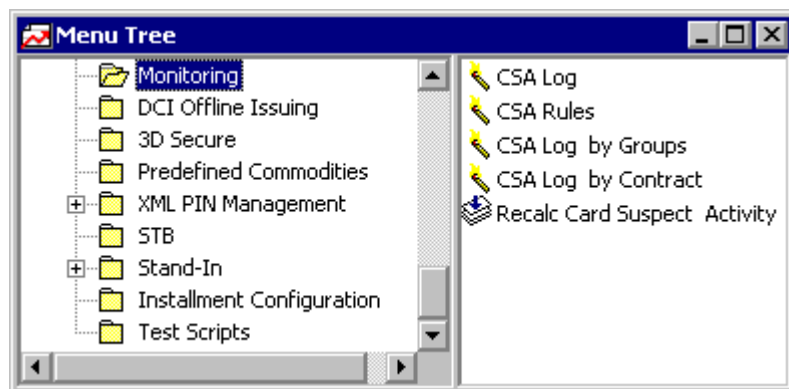


Рис. 3. Пользовательское меню для мониторинга операций

Проверка операций в соответствии с зарегистрированными в системе, выполняется в следующих случаях:

- при проведении авторизации;
- при обработке финансового документа;
- проверка всех операций за указанный период по команде пользователя.

В процессе проверки система анализирует информацию:

- в соответствии с критериями, настроенными для всех операций;
- в соответствии с критериями, настроенными для Схемы Контроля Рисков, относящейся к соответствующему карточному контракту и/или Пакету Сервисов.

В результате анализа операций в специальной таблице базы данных регистрируются записи о подозрительных операциях.

### Список подозрительных операций

Для просмотра списка зарегистрированных в системе подозрительных операций следует выбрать пункт меню "Monitoring → CSA Log", после чего на экране отобразится форма "CSA Log" совместно с подчиненной ей формой (см. Рис. 4).

Registration Date	Contract	Risk Level	Channel	Amount	Curr	Trans Type	Trans Country	Return Code
16/04/03 20:10:16	5413330107540297		EPI	30 000,00USD	Retail		Afghanistan	Expired card / target
23/04/03 14:16:46	5413330132334682		EPI	200,00USD	Retail		Algeria	Not sufficient funds
23/04/03 14:17:38	5413330132334682		EPI	100,00USD	Retail			Not sufficient funds
23/04/03 14:18:58	5413330132334682		EPI	70,00USD	Retail		Algeria	Successfully compl
24/04/03 11:34:56	5413330107540297			111 111,00USD	Credit		Russia	Chain not found
24/06/03 12:22:55	5413330153196572			800,00RUR	Retail		Russia	Successfully compl
19/06/03 16:43:52	5413330153196572		Internal	800,00RUR	Retail		Russia	Successfully compl
20/06/03 16:36:06	5413330102992758		EPI	120,00USD	Retail		Iraq	Successfully compl
20/06/03 18:07:18	5413330102992758		EPI	321,00USD	Retail		Iraq	Successfully compl
24/06/03 11:38:06	5413330102992758		EPI	13,00USD	Unique		American Samoa	Successfully compl
24/06/03 11:44:24	5413330153196572		Internal	6 000,00RUR	Retail		Russia	Not sufficient funds
24/06/03 11:46:02	5413330153196572		Internal	5 000,00RUR	Retail		Russia	Not sufficient funds
24/06/03 11:56:18	5413330153196572		Internal	4 500,00RUR	Retail		Russia	Not sufficient funds

Group Code	Risk Level	Risk Factor
Risky Country		0,000
Total Amount		0,96666
Single Amount		0,97333

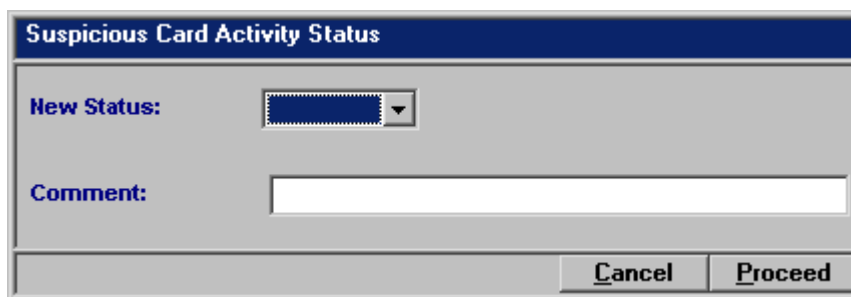
Рис. 4. Формы для просмотра информации о зарегистрированных подозрительных операциях

Форма "CSA Log" содержит следующие данные об операции:

- *Registration Date* – дата и время регистрации операции в списке подозрительных;
- *Contract* – номер карточного контракта;
- в поле *Risk Level* в графическом виде отображен общий уровень подозрительности операции; размер и цвет индикатора зависит от значения в поле *Risk Factor*: черный – очень низкий коэффициент подозрительности, синий – низкий коэффициент, зеленый – средний, оранжевый – высокий и красный – очень высокий коэффициент;
- *Channel* – наименование канала передачи транзакционной информации, например, "VISA", "EPI", "Our ATM", "Our VISA Cards" и т. д.;
- *Amount* – сумма транзакции;
- *Curr* – валюта транзакции;
- *Trans Type* – тип операции;
- *Return Code* – код ответа системы;
- *SIC Code* – код, определяющий тип торговой точки (SIC/MCC) в соответствии с характером бизнеса; список зарегистрированных в системе кодов представлен в форме "SIC Codes" ("Full → Configuration Setup → Main Tables → SIC Codes");
- *Trans Condition* – условия выполнения карточной операции; описание справочника условий выполнения операций описан в документе "Документы и их обработка";
- *Risk Factor* – общий коэффициент подозрительности операции (в пределах от "0" до "1"), который рассчитывается исходя из коэффициентов подозрительности по отдельным критериям (см. ниже описание формы, подчиненной форме "CSA Log");
- *Status* – статус записи о подозрительной операции; поле может принимать значения "Active", "Inactive" или "Closed".

Для того чтобы изменить статус записи, следует выбрать эту запись в форме "CSA Log" и нажать на кнопку [Status]. В появившейся форме "Suspicious Card Activity Status" (см. Рис. 5) следует указать новый статус

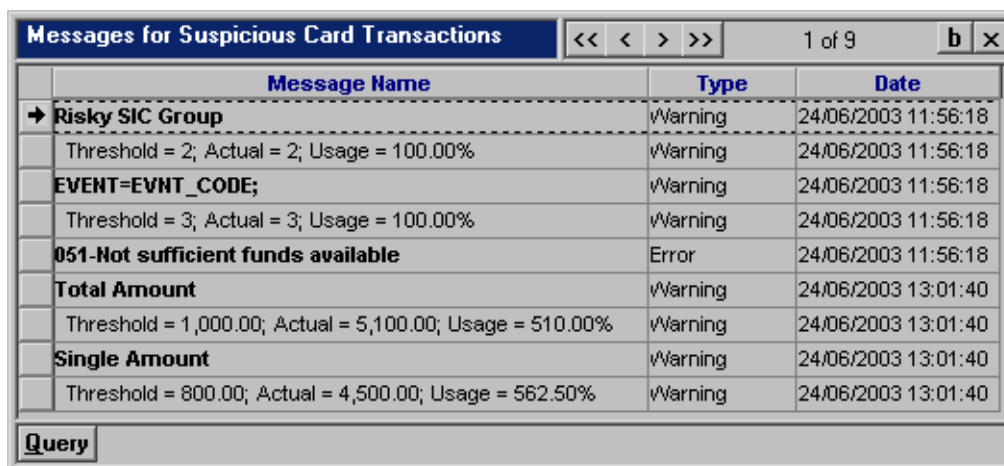
в поле *New Status*, при необходимости добавить комментарии в поле *Comment* и нажать на кнопку [Proceed].



The form has a title bar 'Suspicious Card Activity Status'. It contains two main input areas: 'New Status' with a dropdown menu and 'Comment' with a text area. At the bottom right are 'Cancel' and 'Proceed' buttons.

Рис. 5. Форма для смены статуса записи о подозрительной операции

Для анализа обработки операции следует воспользоваться кнопкой [Messages] в форме "Suspicious Card Transactions". По этой команде на экране будет представлена форма "Messages for Suspicious Card Transaction" (см. Рис. 6), содержащая сообщения, сформированные системой при обработке документа.



Message Name	Type	Date
→ Risky SIC Group	vWarning	24/06/2003 11:56:18
Threshold = 2; Actual = 2; Usage = 100.00%	vWarning	24/06/2003 11:56:18
EVENT=EVNT_CODE;	vWarning	24/06/2003 11:56:18
Threshold = 3; Actual = 3; Usage = 100.00%	vWarning	24/06/2003 11:56:18
051-Not sufficient funds available	Error	24/06/2003 11:56:18
Total Amount	vWarning	24/06/2003 13:01:40
Threshold = 1,000.00; Actual = 5,100.00; Usage = 510.00%	vWarning	24/06/2003 13:01:40
Single Amount	vWarning	24/06/2003 13:01:40
Threshold = 800.00; Actual = 4,500.00; Usage = 562.50%	vWarning	24/06/2003 13:01:40

Query

Рис. 6. Форма для отображения сообщений системы

В поле *Message Name* формы "Messages for Suspicious Card Transaction" полужирным шрифтом отображаются коды критериев, по которым операций была признана как подозрительная, и следующая информация: пороговое значение критерия (Threshold), фактическое значение для данной операции (Actual) и процент превышения порогового значения (Usage).

Для доступа к данным о карточном контракте, по которому выполнялась операция, следует выбрать запись в форме "CSA Log" и нажать на кнопку [Card Info].

Для доступа к информации о документе по подозрительной операции, следует выбрать запись в форме "CSA Log" и нажать на кнопку [Doc-Full].

Форма, подчиненная форме "CSA Log", предназначена для отображения информации о том, по каким именно критериям операция попала в список подозрительных. Подчиненная форма может быть вызвана из формы "CSA Log" нажатием на кнопку [Rules] и содержит следующие поля:

- *Group Code* – код критерия;
- в поле *Risk Level* в графическом виде отображен уровень подозрительности операции по данному критерию; размер и цвет индикатора зависит от значения в поле *Risk Factor*: черный – очень низкий коэффициент подозрительности, синий – низкий коэффициент, зеленый – средний, оранжевый – высокий и красный – очень высокий коэффициент;
- *Risk Factor* – коэффициент подозрительности операции (в пределах от "0" до "1") по данному критерию; коэффициент рассчитывается как отношение фактических параметров документа к пороговым параметрам критериев с учетом веса критерия.

Для просмотра полной информации о критерии, по которому операция признана подозрительной, следует выбрать критерий в форме, которая подчинена форме "CSA Log", и нажать на кнопку [Rule].

Для доступа к списку документов, на основании которых данная операция была признана подозрительной по отдельному критерию, следует выбрать критерий в форме, подчиненной форме "CSA Log", и нажать на кнопку [Docs].

## Список операций, сгруппированных по критериям

Для того чтобы проанализировать количество зарегистрированных подозрительных операций, сгруппированных по критериям, следует выбрать пункт меню "Monitoring → CSA Log by Groups", в диалоговой форме "Time From - To" (см. Рис. 7) указать дату начала и окончания периода анализа данных, и нажать на кнопку [Proceed].

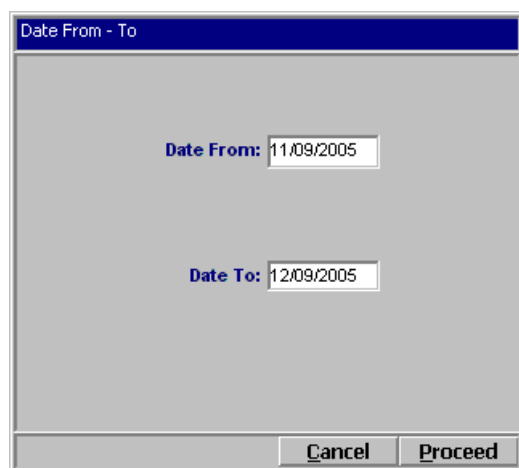
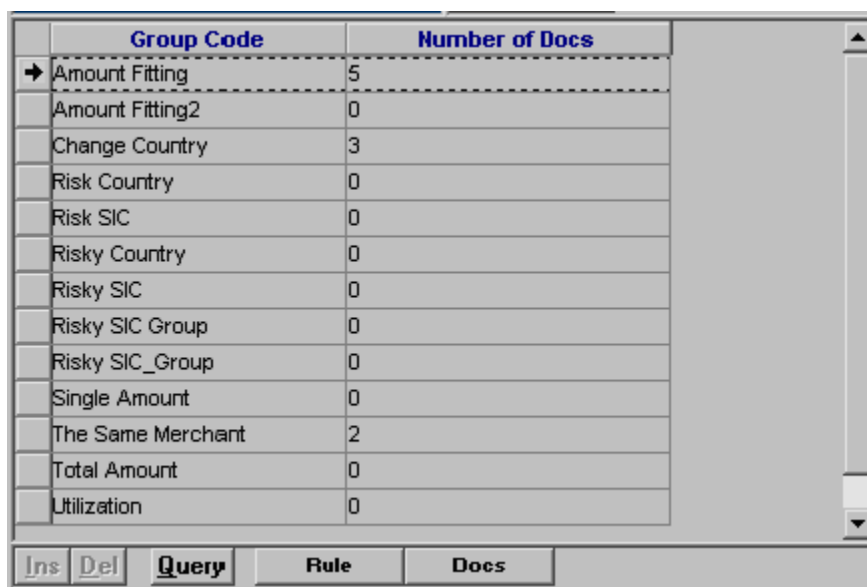


Рис. 7. Форма для указания периода, за который следует анализировать данные

В результате на экране отобразится форма "CSA Log by Groups" (см. Рис. 8), которая содержит информацию о количестве зарегистрированных подозрительных операций по каждому из настроенных в системе критериев.



	Group Code	Number of Docs
→	Amount Fitting	5
	Amount Fitting2	0
	Change Country	3
	Risk Country	0
	Risk SIC	0
	Risky Country	0
	Risky SIC	0
	Risky SIC Group	0
	Risky SIC_Group	0
	Single Amount	0
	The Same Merchant	2
	Total Amount	0
	Utilization	0

Buttons: Ins, Del, Query, Rule, Docs

Рис. 8. Форма для просмотра подозрительных операций по критериям

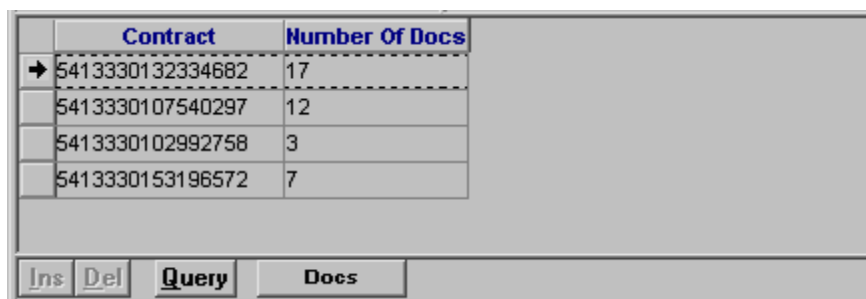
Полную информацию о критерии можно получить, нажав в форме "CSA Log by Groups" на кнопку [Rule].

Для доступа к документам, которые были признаны по данному критерию подозрительными, предназначена кнопка [Docs].

## Список подозрительных операций, сгруппированный по картам

Для того чтобы проанализировать количество зарегистрированных подозрительных операций, сгруппированных по картам, следует выбрать пункт меню "Monitoring → CSA Log by Contract", в диалоговой форме "Time From - To" указать дату начала и окончания периода анализа данных, и нажать на кнопку [Proceed].

В результате на экране отобразится форма "CSA Log by Contract" (см. Рис. 8), которая содержит информацию о количестве подозрительных операций по каждой из зарегистрированных в системе карт.



	Contract	Number Of Docs
→	5413330132334682	17
	5413330107540297	12
	5413330102992758	3
	5413330153196572	7

Buttons: Ins, Del, Query, Docs

Рис. 9. Форма для просмотра подозрительных операций по критериям

Для доступа к документам, которые были признаны по данной карте подозрительными, в форме "CSA Log by Contract" предназначена кнопка [Docs].

## Формирование списка подозрительных операций

Для того чтобы сформировать список подозрительных операций, необходимо выполнить процедуру "Monitoring → Recalc Card Suspect Activity", в диалоговой форме "Time From - To" (см. Рис. 7) указать дату начала и окончания периода анализа данных, и нажать на кнопку [Proceed].

В процессе выполнения процедура удаляет все зарегистрированные записи о подозрительных транзакциях за этот период и на основании анализа операций по текущим критериям, формирует новый список.