

# **Система обнаружения и предотвращения мошеннических транзакций «Smart Ftaud Detection»**

Руководство по эксплуатации

## Оглавление

1. Введение.....	3
1.2. Назначение документа.....	3
1.3. Термины и сокращения .....	3
2. Администрирование системы .....	5
2.1 Управления приложениями .....	5
2.2 Конфигурационные файлы .....	6
2.3 Логирование .....	6
2.3.1. Лог файлы стандартных потоков операционной системы .....	7
2.3.2. Лог файлы приложения Extended Rule Engine .....	7
4.1.1. Лог файлы приложения Advanced Adaptive Authentication .....	7
4.1.2. Лог файлы приложения Policy .....	7
4.1.3. Лог файлы приложения Database Save .....	8
4.1.4. Лог файлы приложения Scheduler.....	8
2.4 Обновление базы GeoIP .....	8
2.5 Работа с планировщиком .....	9
4.1.5. Процедуры планировщика.....	9
3. Эксплуатация системы .....	10
3.1. Проверка правильности функционирования системы .....	10
3.2. Перечень профилактических мероприятий.....	11
3.3. Восстановление работоспособности системы .....	12
4. Требования к персоналу .....	13
4.2. Состав и квалификация персонала, допускаемого к эксплуатации систему. ....	13
4.3. Порядок проверки знаний персонала и допуска его к работе .....	15



## 1. Введение

### 1.2. Назначение документа

Документ содержит описание системы для противодействия мошенничеству (Smart Fraud Detection). В документе представлено

- Описание процессов администрирования системы
- Описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения, в том числе устранение неисправностей.
- Требования к персоналу, обеспечивающему эксплуатацию системы

### 1.3. Термины и сокращения

ТАБЛИЦА 1. ТЕРМИНЫ.

Термин	Описание
<b>Событие (транзакция)</b>	Инициированное клиентом действие, по выполнению платежной или не платежной операции в любых каналах обслуживания.
<b>Сессионная транзакция</b>	Инициированное клиентом событие, не приводящее к финансовым операциям (вход в систему, изменение настроек профиля, получение выписок, смена пароля и пр.).
<b>Платежная транзакция</b>	Инициированное клиентом событие, приводящее к финансовой операции (переводы, платежи, погашение кредита и пр.).
<b>Инцидент</b>	Событие, отмеченное в системе как как подозрительное или мошенническое.
<b>Клиент</b>	Потребитель услуг, предоставляемых финансовым институтом с помощью различных каналов обслуживания.
<b>Подразделение</b>	Структурное подразделение финансового института, предоставляющее услуги
<b>Оценка риска, скоринг</b>	Оценка действий Клиента в числовом выражении, определяющем насколько данная операция отличается от типовых операций Клиента. Значение рассчитывается Системой и является показателем вероятности мошеннических действий в отношении Клиента. Методика расчета является конфиденциальной информацией.

<b>Smart Fraud Detection, Система</b>	Комплексная система обнаружения мошенничества в реальном времени методом анализа поступающих транзакций в различных каналах обслуживания клиентов
<b>Сессия</b>	Цикл операций обмена данными, непрерывно выполняющийся от источников запросов к конечным объектам и имеющий некий обобщающий признак (идентификатор) и конечный результат.
<b>Сессионные данные</b>	Данные передаваемые в рамках одной сессии.
<b>Белый список</b>	Список заведомо добросовестных получателей платежа
<b>Чёрный список</b>	Список, содержащий реквизиты мошенников. Разные типы списков отличаются по назначению и структуре реквизитов
<b>ДБО</b>	Дистанционное банковское обслуживание – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленно (то есть без визита в банк), чаще всего с использованием компьютерных и телефонных сетей

**Таблица 2. Сокращения**

<b>Сокращение</b>	<b>Расшифровка</b>
AAA	Advanced Adaptive Authentication
БД	База данных
AAA_Policy	Policy
AAA_Scheduler	Scheduler
DBSave	Database Save
SFD	Smart Fraud Detection
ДБО	Дистанционное банковское обслуживание

## 2. Администрирование системы

Место установки дистрибутива по умолчанию /opt/sfd.

В дистрибутиве присутствуют следующие папки необходимые для администрирования системы:

- apps – в подпапках расположены jar файлы модулей
- admin – скрипты управления модулями
- profile – содержит в себе следующие подпапки в которых располагаются:
  - config – конфигурационные файлы
  - log – логи работы модулей
  - geoip – база GeoIP

### 2.1 Управления приложениями

Для управления приложениями используются скрипты, расположенные в папке admin.

В названии каждого скрипта присутствует имя приложения, к которому он относится.

Скрипты начинающиеся на node\_ используются для управлением приложений на локальном узле, заканчивающиеся на \_mgmt используются для управлением приложениями на всех узлах кластера.

Все скрипты в качестве аргумента требуют одну из команд:

- start – запустить приложение
- stop – остановить приложение
- restart – перезапустит приложение
- kill – убить процесс приложения
- version – отобразит версию приложения
- status – отобразит состояния процесса приложения

В дистрибутиве доступны следующие скрипты:

- AdvancedAA\_DBSave\_mgmt.sh

- AdvancedAA\_mgmt.sh
- AdvancedAA\_Policy\_mgmt.sh
- AdvancedAA\_Scheduler\_mgmt.sh
- ExtendedRuleEngineAsync\_mgmt.sh
- node\_AdvancedAA\_DBSave.sh
- node\_AdvancedAA\_Policy.sh
- node\_AdvancedAA\_Scheduler.sh
- node\_AdvancedAA.sh
- node\_ExtendedRuleEngineAsync.sh

## 2.2 Конфигурационные файлы

Все конфигурационные файлы находятся в папке profile/config.

Внутри каждого конфигурационного файла находится описание доступных в нём параметров.

Список конфигурационных файлов и их предназначение:

Конфигурационный файл	Предназначение
<b>env.conf</b>	параметры среды исполнения
<b>afd_eea_config.properties</b>	параметры приложения ExtendedRuleEngine
<b>ignite-eea-calc-config.xml</b>	параметры кластера ignite приложения ExtendedRuleEngine
<b>afd_aaap.properties</b>	параметры приложения AdvancedAA Policy
<b>ignite-aaap-config.xml</b>	параметры кластера ignite приложения AdvancedAA_Policy
<b>afd_config.properties</b>	параметры приложения AdvancedAA
<b>ignite-cache-config.xml</b>	параметры кластера ignite приложения AdvancedAA
<b>afd_db_save.properties</b>	параметры приложения AdvancedAA_DBSave
<b>afd_scheduler.properties</b>	параметры приложения AdvancedAA Scheduler
<b>ignite-scheduler-config.xml</b>	параметры кластера ignite приложения AdvancedAA Scheduler

## 2.3 Логирование

Все файлы логов находятся в папке profile/log.

### 2.3.1. Лог файлы стандартных потоков операционной системы

Лог файлы начинающиеся на `stderr_*` и `stdout_*` содержат в себе вывод стандартных потоков операционной системы. Данные файлы создаются на каждый запуск и в своём имени имеют наименования приложения и дату запуска.

### 2.3.2. Лог файлы приложения Extended Rule Engine

`afd-eea.log` – основной файл логов приложения.

`afd-eea-stat.log` – файл статистики работы приложения

`afd-eea.gc.log` – файл статистики работы garbage collector в приложении

Параметры мониторинга:

- Наличие строк типа ERROR в файле `afd-eea.log`
- Файл `afd-eea-stat.log`, строки статистики `EEA_SERVLET` – показывают время обработки транзакций приложением, от приёма запроса до отправки ответа по нему.
- Файл `afd-eea-stat.log`, строки статистики `AFD_SENDING` – показывает суммарное время обработки транзакций последующими модулями системы (AAA, AAA\_Policy), включая отправку запроса и получение ответа.

### 4.1.1. Лог файлы приложения Advanced Adaptive Authentication

`afd-front.log` – основной файл логов приложения.

`afd-front-stat.log` – файл статистики работы приложения

`afd-front.gc.log` – файл статистики работы garbage collector в приложении

Параметры мониторинга:

- Наличие строк типа ERROR в файле `afd-front.log`
- Файл `afd-front-stat.log`, строки статистики `PROC_EVENT` – показывают время обработки транзакций приложением, от приёма запроса до отправки ответа по нему.
- Файл `afd-front-stat.log`, строки статистики `AAAP_REQUEST` – показывает время обработки транзакций модулем системы AAA\_Policy, включая отправку запроса и получение ответа.

### 4.1.2. Лог файлы приложения Policy

`afd-aap.log` – основной файл логов приложения.



afd-aap-stat.log – файл статистики работы приложения

afd-aap.gc.log – файл статистики работы garbage collector в приложении

Параметры мониторинга:

- Наличие строк типа ERROR в файле afd-aap.log
- Файл afd-aap-stat.log, строки статистики REQUESTS\_ALL – показывают время обработки транзакций приложением, от приёма запроса до отправки ответа по нему.

#### 4.1.3. Лог файлы приложения Database Save

afd-db-save.log – основной файл логов приложения.

afd-db-save -stat.log – файл статистики работы приложения

afd-db-save.gc.log – файл статистики работы garbage collector в приложении

Параметры мониторинга:

- Наличие строк типа ERROR в файле afd-db-save.log

#### 4.1.4. Лог файлы приложения Scheduler

afd-scheduler.log – основной файл логов приложения.

afd- scheduler.gc.log – файл статистики работы garbage collector в приложении

Параметры мониторинга:

- Наличие строк типа ERROR в файле afd-db-save.log
- Раз в сутки наличие строки: «Offline tasks finished successfully»

## 2.4 Обновление базы GeoIP

Используемая в приложении Advanced Adaptive Authentication база привязки ip-адресов и реального месторасположения, требует периодического обновления.

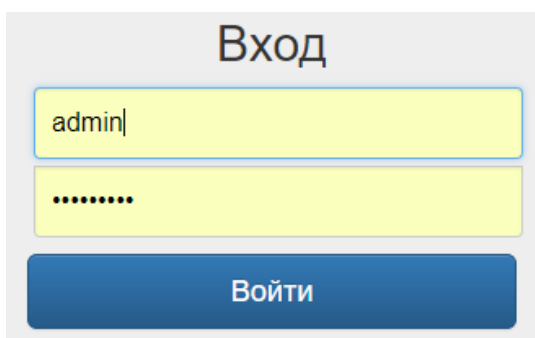
Для этого необходимо файл с новой версией базы положить в profile/geoip и в конфигурационном файле afd\_config.properties в параметре geoip.profile.active.fileName прописать имя нового файла.

В течении 5 минут должен произойти импорт новой базы в приложение, и в этот момент старый файл переместится в папку profile/geoip/archive.

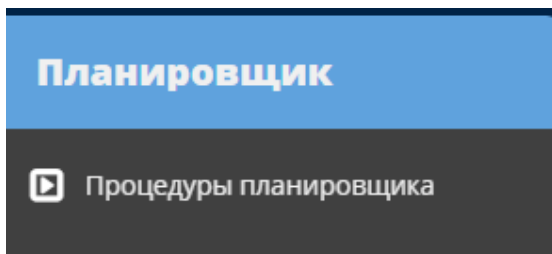
## 2.5 Работа с планировщиком

Для запуска приложения:

- Перейти по ссылке [http://server\\_name:port\\_number/AAAScheduler](http://server_name:port_number/AAAScheduler), где *server\_name:port\_number*- имя хоста и номер порта вашего сервера где установлено приложение AAA\_Scheduler.
- Выполнить вход в Систему.

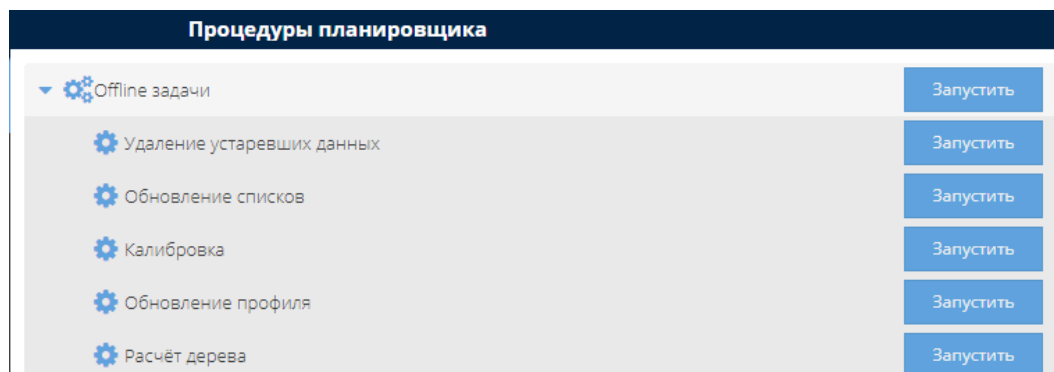


В левой части формы расположена закладка - Процедуры планировщика



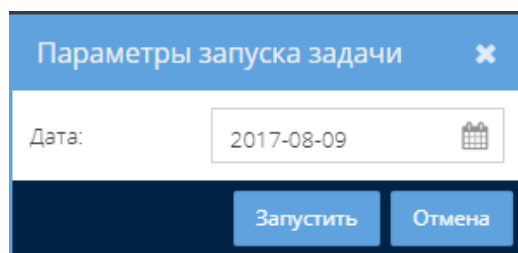
### 4.1.5. Процедуры планировщика

При выборе меню «Процедуры планировщика» в правой части формы отображаются доступные процедуры планировщика.



Запустить процедуру можно с помощью кнопки напротив каждой процедуры - «Запустить».

При нажатии кнопки «Запустить», если у процедуры есть доступные параметры должно появляться окно, куда данные параметры можно ввести и запустить процедуру, иначе происходит запуск процедуры.



### 3. Эксплуатация системы

#### 3.1. Проверка правильности функционирования системы

Проверка правильности функционирования системы проводится по следующим основным параметрам, перечисленным в Таблице.

Таблица 3. Проверки системы

Проверка	Результат
<b>Просмотр журнала системных сообщений</b>	Должны отсутствовать сообщения об ошибках. При наличии ошибок в системном журнале по коду ошибки выяснить причину и выполнить работы по ее устранению.
<b>Осмотр состояния дискового массива</b>	При наличии сигнализации о некорректной работе дисков дискового массива, заменить проблемный диск. На

	рекомендуемом оборудовании остановки всего дискового массива при этом не требуется..
<b>Проверка температурного режима</b>	Кондиционер должен исправно работать, температура не выше 20°C. В противном случае остановить работу и произвести ремонт кондиционера или его замену.
<b>Проверка вентиляторов</b>	Вентиляторы вращаются без посторонних шумов. В противном случае произвести замену вентиляторов. На рекомендуемом оборудовании его остановки для замены не требуется.
<b>Проверка доступа к хранилищу</b>	Каналы доступа к хранилищу данных функционируют без ошибок. При выходе из строя или некорректной работе произвести необходимые работы по устранению неполадок.

### 3.2. Перечень профилактических мероприятий

Поддержание функционирования системы требует проведения ежедневной профилактики, перечень работ которой приведен в Таблице 2.

**ТАБЛИЦА 4. ПЕРЕЧЕНЬ РАБОТ ПРИ ВЫПОЛНЕНИИ ЕЖЕДНЕВНОЙ ПРОФИЛАКТИКИ**

Описание работ	Действия при наличии нарушений
<b>Мониторинг температурного режима в серверных помещениях</b>	При нарушении температурного режима проверить и при необходимости заменить кондиционер.
<b>Проверка нормальной работы вентиляторов охлаждения серверов</b>	При нарушении работы вентиляторов заменить вентилятор.
<b>Мониторинг журналов системных событий</b>	При наличии ошибок в системном журнале по коду ошибки выяснить причину и выполнить работы по ее устранению.
<b>Проверка наличия свободного дискового пространства</b>	При недостатке места на диске рекомендуется удалить ненужные для дальнейшей работы файлы. Если это не решит проблему с местом на диске, необходимо провести работы по наращиванию дискового пространства хранилища данных.

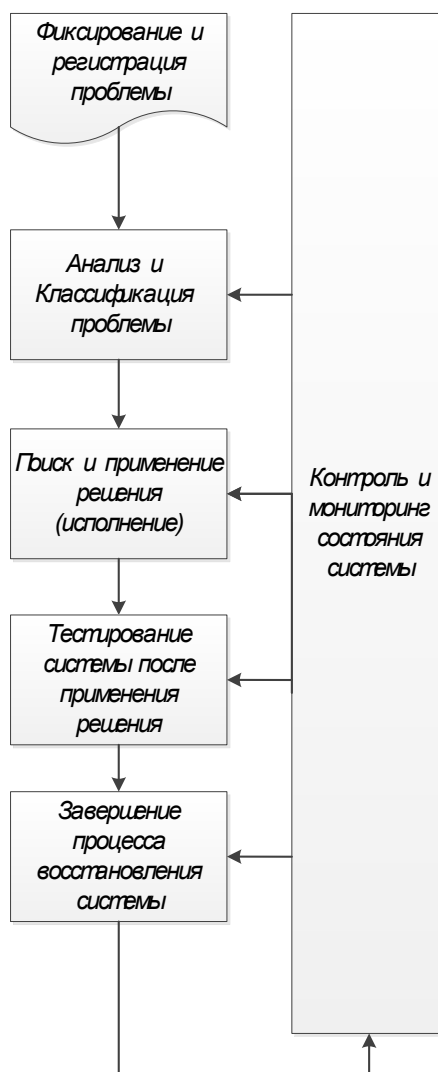
Последовательность выполнения работ при ежедневной профилактике не важна. Данные работы позволяют своевременно выявлять предаварийные ситуации и минимизировать простой системы и соответствуют нормальному режиму функционирования, последовательность выполнения описана в разделе «Нормальный режим».

### 3.3. Восстановление работоспособности системы

Основными операциями процесса восстановления являются:

- Фиксирование и регистрация проблемы – администратор фиксирует некорректную работу модуля или всей системы в целом, падение системы;
- Анализ и классификация проблемы – администратор проводит подробный анализ проблемы для выявления причины возникшего сбоя, используя инструменты для диагностики и логи системы. Определяет область (программная или аппаратная часть), которая отвечает за возникший сбой для дальнейшего его устранения;
- Поиск решения – администратором осуществляется поиск решения проблемы;
- Применение решения – администратором осуществляется применение найденного решения для восстановления работы системы;
- Тестирование системы после применения решения – администратором осуществляется тестирование системы после применения решения для проверки устранения проблемы и корректного функционирования системы;
- Мониторинг и контроль состояния системы в течение и после решения проблемы – администратором осуществляется мониторинг и контроль состояния системы в процессе решения проблемы (к примеру, если сбой произошел в одном из приложений системы, при этом другие приложения функционируют корректно, но необходимо контролировать работу данных приложений, т.к. применение решения для устранения возникшего сбоя может повлиять на их корректную работу), а так же после завершения работ по восстановлению системы для исключения повторного возникновения аналогичных сбоев.

На рисунке 1 приведена схема процесса восстановления работоспособности системы. На нем изображена последовательность действий при восстановлении работоспособности системы. Так же можно отметить, что процесс контроля и мониторинга состояния системы происходит постоянно параллельно с работами по устранению сбоя, а так же продолжается после завершения работ по восстановлению работы системы. Предполагается, что если в процессе мониторинга и контроля работы системы после восстановления будет зафиксирована подобная или иная проблема, процесс устранения сбоя будет повторен с момента классификации проблемы.



## 4. Требования к персоналу

### 4.2. Состав и квалификация персонала, допускаемого к эксплуатации системы.

Численность и квалификация персонала должна быть достаточной для выполнения всех функций и задач, возложенных на систему. Предлагается обслуживающий персонал систему формировать на основе существующего персонала.

Основные роли и функции по эксплуатации системы представлены в Таблице 1.

**Таблица 5. Основные роли и функции по эксплуатации системы**

№ п/п	Название роли	Основные функции	Количество единиц
1	Администратор вычислительных систем	Мониторинг и управление оборудованием и программным обеспечением серверной подсистемы. Анализ показателей производительности, диагностика оборудования. Взаимодействие со службой поддержки поставщика и производителя оборудования. Модернизация оборудования, установка обновлений ПО.	1
2	Администратор систем хранения данных и резервного копирования	Мониторинг и управление оборудованием и программным обеспечением сетей хранения, систем хранения. Организация резервного копирования данных. Анализ показателей производительности, диагностика оборудования. Взаимодействие со службой поддержки поставщика и производителя оборудования и ПО. Модернизация оборудования, установка обновлений ПО.	1
3	Администратор сети передачи данных	Мониторинг и управление оборудованием и программным обеспечением сети передачи данных. Анализ показателей производительности, диагностика оборудования. Взаимодействие со службой поддержки поставщика и производителя оборудования и ПО. Модернизация оборудования, установка обновлений ПО.	1

### 4.3. Порядок проверки знаний персонала и допуска его к работе

Проверка знаний администраторов для выполнения указанных работ должна производиться в рамках проведения аттестаций сотрудников предприятия на соответствие занимаемой должности и при приеме на работу. В аттестационные комиссии организации должны быть включены сотрудники, обладающие достаточной квалификацией для осуществления такой проверки.

Допуск к работе осуществляется по результатам аттестации.

Техническое обслуживание должен проводить квалифицированный персонал, прошедший специализированное обучение, допущенный соответствующим порядком к проведению работ на электроустановках до 1000В и имеющий квалификационную группу по электробезопасности не ниже третьей.

Эксплуатационный и обслуживающий персонал должен иметь высшее или среднее техническое образование и пройти специальную подготовку в соответствующем объеме на этапе опытной эксплуатации комплекса. Подготовка должна включать в себя получение навыков пользовательской работы с общим и специальным программным обеспечением АРМ в объеме выработки навыков поддержания их работоспособности.

Персонал, обслуживающий технические средства комплекса, по квалификации должен соответствовать требованиям, предъявляемым изготовителями средств вычислительной техники.