

# Система обнаружения и предотвращения мошеннических транзакций «Smart Fraud Detection»

ОПИСАНИЕ ПРОЦЕССОВ, ОБЕСПЕЧИВАЮЩИХ ПОДДЕРЖАНИЕ  
ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ

ВЕРСИЯ СИСТЕМЫ 3.5

МОСКВА, 2021

## Оглавление

Оглавление .....	1
Введение .....	2
Назначение документа.....	2
Термины и сокращения .....	2
Описание процессов, обеспечивающих поддержание жизненного цикла Системы .....	4
Администрирование системы.....	4
Настройка уровня логирования в приложениях.....	4
Конфигурационные файлы.....	5
Запуск приложений .....	6
Обновление базы GeoIP .....	7
Проверка правильности функционирования системы .....	7
Перечень профилактических мероприятий.....	8
Восстановление работоспособности системы .....	8
Возможные неисправности и методы их устранения.....	10
Требования к персоналу.....	12
Состав и квалификация персонала, допускаемого к эксплуатации системы .....	12
Порядок проверки знаний персонала и допуска его к работе .....	13
Техническая поддержка продукта .....	13
Регламент устранения неисправностей в системе .....	14
Типы запроса .....	14
Приоритеты и сроки исполнения.....	15
Специалисты, обеспечивающие техническую поддержку .....	16

## Введение

### Назначение документа

Документ содержит описание основных процессов, обеспечивающих Поддержание жизненного цикла Системы (Smart Fraud Detection), в том числе устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения, совершенствование программного обеспечения, а также информацию о персонале, необходимом для обеспечения такой поддержки.

### Термины и сокращения

Таблица 1. Термины.

Термин	Описание
<b>Advanced Adaptive Authentication</b>	Приложение оценки рисков
<b>Advanced Adaptive Authentication Policy</b>	Приложение работы с правилами
<b>Smart Fraud Detection, Система</b>	Комплексная система обнаружения мошенничества в реальном времени методом анализа поступающих транзакций в различных каналах обслуживания клиентов
<b>ExtendeRuleEngine</b>	Приложение обработки транзакций
<b>Инцидент</b>	Событие, отмеченное в системе как как подозрительное или мошенническое.
<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>Сессионные данные</b>	Данные передаваемые в рамках одной сессии.

Таблица 2. Сокращения

Сокращение	Расшифровка
AAA	Advanced Adaptive Authentication
AAA_Policy	Policy
AAA_Scheduler	Scheduler
DBSave	Database Save
SFD	Smart Fraud Detection

ДБО	Дистанционное банковское обслуживание
БД	База данных

## Описание процессов, обеспечивающих поддержание жизненного цикла Системы

### Администрирование системы

#### Настройка уровня логирования в приложениях

Настройка уровня логирования выполняется в файлах конфигурации logback\*.xml

```
<logger name={наименование_логера} level={уровень_логирования} additivity={} />
```

##### Уровни логирования:

ERROR — записывает в журнал только сообщения уровня ERROR.

WARN — записывает в журнал только сообщения уровня WARN и выше.

INFO — записывает в журнал только сообщения уровня INFO и выше.

DEBUG — записывает в журнал только сообщения уровня DEBUG и выше.

TRACE — записывает в журнал все сообщения логера.

##### Уровни сообщений:

ERROR — выполнение задачи не было завершено. Работоспособность приложения была затронута либо приложение не работает. Требуется немедленно вмешательство.

WARN — произошло непредвиденное событие, но работоспособность приложения в целом не затронута. Немедленного вмешательства не требуется.

INFO — произошло нормальное события для данного приложения.

DEBUG — подробная информация о информационных потоках в приложении.

TRACE — полная информация обо всем происходящем в приложении.

В таблице ниже перечислены конфигурационные файлы для настройки уровней логирования:

Файл конфигурации	Назначение
logback.xml	Файл настройки логирования приложения Advanced Adaptive Authentication
logback-aaap.xml	Файл настройки логирования приложения Advanced Adaptive Authentication Policy
logback-db-save.xml	Файл настройки логирования приложения DBSave
logback-eea.xml	Файл настройки логирования ExtendedRuleEngineAsync
logback-scheduler.xml	Файл настройки логирования приложения Advanced Adaptive Authentication Scheduler

## 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
env.conf	параметры среды исполнения
afd_eea_config.properties	параметры приложения ExtendedRuleEngine
ignite-eea-calc-config.xml	параметры кластера ignite приложения ExtendedRuleEngine
afd_aaap.properties	параметры приложения AdvancedAA_Policy
ignite-aaap-config.xml	параметры кластера ignite приложения AdvancedAA_Policy
afd_config.properties	параметры приложения AdvancedAA
ignite-cache-config.xml	параметры кластера ignite приложения AdvancedAA
afd_db_save.properties	параметры приложения AdvancedAA_DBSave
afd_scheduler.properties	параметры приложения AdvancedAA_Scheduler
ignite-scheduler-config.xml	параметры кластера ignite приложения AdvancedAA_Scheduler

## Запуск приложений

Для запуска приложений перейти в папку /opt/atm/admin/ и выполнить один из скриптов.

Синтаксис использования скрипта: *./имя\_скрипта параметр*

Рекомендованный порядок запуска приложений: AdvancedAA, AdvancedAA\_Policy, AdvancedAA\_DBSave, AdvancedAA\_Scheduler, ExtendedRuleEngineAsync.

Скрипты node\_\*.sh используются для управления отдельным приложением на ноде на которой запускается скрипт.

Скрипты \*\_mgmt.sh используются для управления отдельным приложением на всех нодах, где оно установлено (на основании файла настройки env.conf).

Скрипт send\_all.sh используется для запуска всех приложений на всех нодах (на основании файла настройки env.conf).

### Параметры скриптов:

- start — запуск приложения
- stop — штатная остановка приложения
- kill — экстренная остановка приложения
- status — отображает статус приложения
- restart — рестартует приложение
- version — отображает версию установленного приложения.

### Список скриптов управления приложениями

- AdvancedAA\_DBSave\_mgmt.sh
- AdvancedAA\_mgmt.sh
- AdvancedAA\_Policy\_mgmt.sh
- AdvancedAA\_Scheduler\_mgmt.sh
- AFD\_UI\_mgmt.sh
- ExtendedRuleEngineAsync\_mgmt.sh
- node\_AdvancedAA\_DBSave.sh
- node\_AdvancedAA\_Policy.sh
- node\_AdvancedAA\_Scheduler.sh
- node\_AdvancedAA.sh
- node\_ExtendedRuleEngineAsync.sh
- send\_all.sh

- sync\_nodes.sh

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

## 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.



## 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.

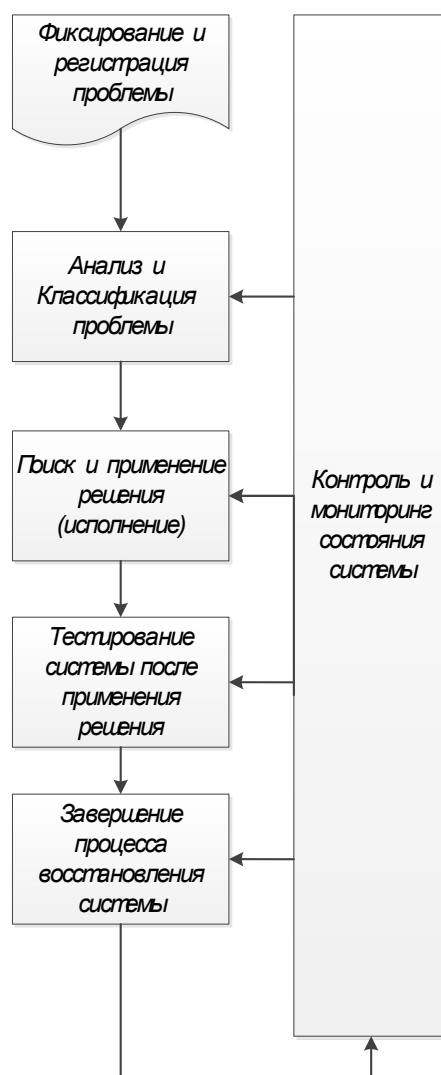
Последовательность выполнения работ при ежедневной профилактике не важна. Данные работы позволяют своевременно выявлять предаварийные ситуации и минимизировать простой системы и соответствуют нормальному режиму функционирования, последовательность выполнения описана в разделе «Нормальный режим».

## 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.

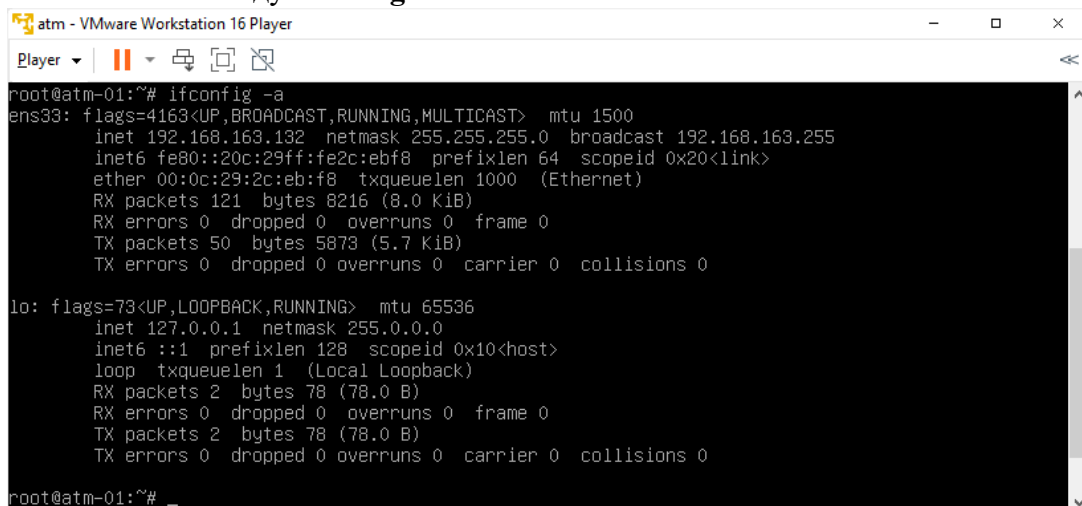


## Возможные неисправности и методы их устранения

В случае проблем со входом в Web-интерфейс следует проверить следующее:

1. Виртуальная машина получила IP адрес:
  - а. После полной загрузки системы необходимо ввести данные пользователя и пароль на Операционную систему: root/2zJxSxI0nJJ6

b. Выполнить команду: **ifconfig -a**:



```
root@atm-01:~# ifconfig -a
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.163.132 netmask 255.255.255.0 broadcast 192.168.163.255
    inet6 fe80::20c:29ff:fe2c:ebf8 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:2c:eb:f8 txqueuelen 1000 (Ethernet)
    RX packets 121 bytes 8216 (8.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50 bytes 5873 (5.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 2 bytes 78 (78.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2 bytes 78 (78.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@atm-01:~# _
```

- c. Проверить правильность выданного адреса, в случае если адрес не выдан или сетевой интерфейс в состоянии “DOWN” устранить проблему самостоятельно или обратиться в поддержку компании «Фаззи Лоджик Лабс» для получения консультации.

2. Запуск базы данных Cassandra:

- a. После старта приложения, выполнить команду «**ps -ef | grep cassandra**», в результате выполнения должен содержаться текст:

<i>atm</i>	<i>&lt;PID&gt;</i>	<i>&lt;Дата запуска&gt;</i>	<i>&lt;Время работы&gt;</i>	<i>java .....</i>
------------	--------------------	-----------------------------	-----------------------------	-------------------

- b. В случае если процесс не обнаружен проанализировать лог:

*/opt/apache-cassandra-3.11.0/logs/system.log*

На наличие ошибок

3. В случае, если при старте одно из приложений сообщит об ошибке, необходимо проанализировать логи:

*/opt/atm/profile/log/afd-front.log*

*/opt/atm/profile/log/afd-eea.log*

*/opt/atm/profile/log/afd-aaap.log*

*/opt/atm/profile/log/afd-scheduler.log*

*/opt/atm/profile/log/afd-db-save.log*

Либо прислать их на анализ в поддержку компании «Фаззи Лоджик Лабс».

## Требования к персоналу

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

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.	1

		Взаимодействие со службой поддержки поставщика и производителя оборудования и ПО. Модернизация оборудования, установка обновлений ПО.	
--	--	--	--

## 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.

## Техническая поддержка продукта

В данном разделе приведено описание порядка регистрации и устранения инцидентов, возникших у Заказчика.

## Регламент устранения неисправностей в системе

Запрос может быть направлен в службу технической поддержки одним из следующих способов:

- посредством регистрации Запроса в Редмайне
- по электронной почте с [support@fzlabs.ru](mailto:support@fzlabs.ru)

Запрос должен содержать следующие сведения:

- дата и время Запроса;
- описание Запроса;
- тип Запроса: Инцидент, Дефект, Консультационный запрос (см. стр. 14).
- приоритет Запроса в соответствии с классификацией настоящего приложения;
- по мере обработки Запроса, при необходимости, Заказчик предоставляет дополнительную информацию.

После регистрации Запроса ответственный сотрудник отдела внедрения и сопровождения организует работу по устранению заявленной проблемы в сроки, соответствующие категории критичности. О выполнении Запроса сотрудник уведомляет Заказчика путем направления информационного сообщения на адрес электронной почты Ответственного со стороны Заказчика, содержащего уникальный номер Запросу, и описание принятых мер.

### Типы запроса

Тип	Описание
Расследование/ Консультация	Расследование – обращение по поводу некорректной работы программного обеспечения. По результатам расследования может быть оформлен Дефект.  Обращение сотрудника Заказчика по вопросам внедренного ПО: <ul style="list-style-type: none"><li>• Использование внедренного ПО</li><li>• Реализация технических решений</li><li>• Проведение технологических работ</li><li>• Настройка внедренного ПО и средства мониторинга</li></ul>
Инцидент	Любое обращение сотрудника Заказчика по поводу незапланированного прерывания или снижения качества ИТ-

Тип	Описание
	услуги, а также сбой элемента ИТ-инфраструктуры, в том числе, который еще не оказал влияние на ИТ-услугу. По согласованию сторон Инцидент может быть переведен в Дефект.
Дефект	Обращение по поводу выявленного несоответствия программного обеспечения установленным требованиям, ошибка в функционировании ПО.

### Приоритеты и сроки исполнения

Приоритеты событий, в связи с которыми направляются Запросы, определяются в соответствии с важностью (срочностью), а также исходя из масштабности её влияния. Существует три уровня важности:

- «Критичная» – недоступность функционала приводит к прерыванию работы Системы;
- «Высокая» – недоступность либо существенное снижение доступности функционала приводит к ухудшению Системы;
- «Средняя» – недоступность либо снижение доступности функционала оказывает опосредованное влияние на Системы.

Уровни влияния Инцидента:

- «А» (авария) - Инцидент ведёт к недоступности функционала Решения и носит массовый характер, затрагивающий более 5% пользователей данного функционала;
- «В» - Инцидент ведёт к недоступности функционала для отдельных пользователей либо объектов, что приводит к нарушению бизнес-процесса;
- «С» - Инцидент ведёт к снижению доступности функционала для отдельных пользователей либо сущностей. При этом существует временное (обходное) решение, позволяющее обеспечить приемлемый уровень функционирования затронутых Инцидентом бизнес-процессов и не требующее высоких трудозатрат.

Важность/влияние	А	В	С
«Критичная»	«Блокирующий»	«Высокий»	«Средний»



«Высокая»	«Высокий»	«Средний»	«Средний»
«Средняя»	«Средний»	«Низкий»	«Низкий»

Применяются следующие нормативы обработки Запросов:

- **«Блокирующий».** Время реакции – 2 рабочих часа, интенсивность обмена информацией – раз в день (только в рабочие дни);
- **«Высокий».** Время реакции – 4 рабочих часа, интенсивность обмена информацией – раз в 3 дня (только в рабочие дни);
- **«Средний».** Время реакции – 2 рабочих дня, интенсивность обмена информацией – раз в неделю;
- **«Низкий».** Время реакции – 5 рабочих дней, интенсивность обмена информацией – раз в месяц;

Где:

- Время реакции – это время, необходимое для старта обслуживания Запроса.
- Интенсивность обмена информацией – это частота коммуникаций для локализации проблемы (инцидента), выработки плана мероприятий по её устранению и/или, при необходимости, поиск обходного решения (workaround)

При разрешении Инцидента устанавливается его причина. Одной из причин Инцидента может быть Дефект.

## Специалисты, обеспечивающие техническую поддержку

Техническая поддержка продукта осуществляется специалистами отдела внедрения и сопровождения. В обязанности сотрудников отдела входят:

- Консультирование сотрудников Заказчика по вопросам оперативного использования Решения.
- Услуги по восстановлению работоспособности ПО в среде промышленной эксплуатации после сбоя.
- Разрешение Инцидентов и Дефектов, связанных с работоспособностью Решения в среде промышленной эксплуатации.

- Заккрытие разрешенных Инцидентов, связанных с работоспособностью Решения в среде промышленной эксплуатации, и информирование сотрудников Заказчика.
- Сопровождение работ, связанных с обновлением системы заказчиком в среде промышленной эксплуатации.

Для каждого Заказчика назначается ответственный специалист из отдела сопровождения и внедрения, который курирует все обращения и несет ответственность за их своевременное исполнение.

Если обращение Заказчика не удастся решить силами сотрудников отдела сопровождения и внедрения, к их решению привлекаются специалисты других отделов:

- Аналитический отдел – разработка Технических заданий на новые доработки.
- Отдел разработки – ведение новых разработок и исправление дефектов.
- Отдел обеспечения контроля качества – тестирование новых доработок и исправленных Дефектов.