**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на закупку информационной системы (ИС) логирования обращений к критичным данным клиента в ИС Банка и обезличивания тестовых баз**

**для ПАО «МТС-Банк»**

# 1. Общие требования к работам/услугам, условия и сроки выполнения работ/ оказания услуг.

* 1. Поставка ИС соответствующего всем обязательным требованиям, перечисленным в настоящем Техническом задании

1.2 Внедрение ИС и начало ее использования в МТС-Банк

1.3 Обучение профильных специалистов МТС-Банк процедурам работы с ИС

Желаемый срок выполнения работ, начиная от даты старта, если не указано иное.

|  |  |  |
| --- | --- | --- |
| **№** | **Работа** | **Длительность** |
| 1 | Поставка Инструмента  | 14 календарных дней |
| 2 | Внедрение (разработка) Инструмента  | 60 календарных дней  |
| 3 | Обучение профильных специалистов МТС-банк процедурам работы с Инструментом | 14 календарных дней |
| 4 | Поддержка Инструмента | 2 года |

##

## Требования к производительности ИС:

* В случае применения логирования действий пользователей на системах Банка время обработки запросов пользователей не должно увеличиваться
* Инструмент должен поддерживать маскирование больших объемов данных
* В случае статического маскирования объекта, время маскирования не должно превышать время ее копирования более чем на 30% (не блокирующее)
* В случае применения динамического маскирования данных на системах Банка время обработки запросов пользователей не должно увеличиваться более чем на **N** % (не блокирующее)

## Перечень систем для внедрения ИС логирования обращений к критичным данным клиента в ИС Банка и обезличивания тестовых баз:

1. Дистанционное банковское обслуживание (ДБО)
2. ЦФТ РБО (АБС)
3. Siebel CRM
4. Tieto Card Suite (ПЦ)
5. Единое хранилище данных (ЕХД)
6. **Техническое задание на модуль логирования обращений к критичным данным** **клиента в ИС Банка**



1. **Техническое задание на модуль маскирования критичных данных и обезличивания тестовых баз ИС Банка**



1. **Предварительные сценарии использования ИС логирования обращений к критичным данным клиента в ИС Банка и обезличивания тестовых баз**

|  |
| --- |
| **Сценарий № 1 «Создание тестовой базы данных посредством статического маскирования»** |
| Описание сценария: | 1. Ключ по обезличиванию данных тестовых сред хранится в отдельной базе данных
2. В ходе процесса копирования чувствительные данные замещаются по заданному ключу (маскируются)
3. Тестирование проводится в тестовой среде на маскированных данных
4. Данные тестовых стендов консистентные между собой

ДОПОЛНЕНИЕ: изменяемые при обезличивании данные должны соответствовать по формату требованиям, аналогичным оригинальным данным. Например, ФИО должно быть текстовым, номер паспорта или банковской карты обезличены в соответствии с требованиями к формату оригинальных номеров. Требования к форматам каждого обезличиваемого поля необходимо будет детально прописать в рамках проекта |
| **Сценарий № 2 «Динамическое маскирование чувствительных данных»**  |
| Описание сценария: | 1. При обращении пользователей, которым не разрешено иметь доступ к оригинальным данным, чувствительные данные маскируются «на лету»
2. В результате пользователь, обращающийся к чувствительным данным, получает маскированные данные, которые сохраняют формат и структуру оригинальных данных. Замещение чувствительных значений нечувствительными происходит незаметно для пользователя.
 |
| **Сценарий № 3 «Маскирование части чувствительного значения при доступе к данным»** |
| Описание сценария: | Аналогично сценарию № 2, но больше внимания уделяется бизнес-правилам формирования данных. В зависимости от имеющихся у пользователя прав доступа, осуществляется маскирование не всего чувствительного значения целиком, а только его части. |
| **Сценарий № 4 «Автоматическое обнаружение чувствительных данных»** |
| Описание сценария: | Инструмент сканирует таблицы на предмет наличия в них чувствительных данных. Результат сканирования содержит категорию данных и место их расположения. |
| **Сценарий № 5 «Маскирование чувствительных данных при запросе пользователем детализации данных из сводных отчётов и форм»** |
| Описание сценария: | 1. Пользователь заходит в сводную форму или отчет, в котором есть «ФИО», «Остаток на счете»
2. Средствами администратора ИС настраивается маскирование (например, «Остаток на счете» = 0 или пусто) для поля «Остаток на счете»
3. Чтобы посмотреть «Остаток на счете» пользователю нужно войти («провалится») в форму конкретного клиента или договора
4. Факт просмотра (входа) в форму конкретного клиента или договора попадает под процесс Логирования и виден в отчете
 |
| **Сценарий № 6 «Маскирование чувствительных данных для пользователей, не имеющих согласованных прав доступа к персональным данным»** |
| Описание сценария: | 1. Ведется отдельный реестр пользователей, имеющих согласованные права доступа к чувствительным данным
2. Если пользователь, который не входит в данный реестр, выполнит отчет или запустит форму, в которой есть чувствительные данные, то они должны будут выводиться в маскированном виде
 |
| **Сценарий № 6 «Чувствительные данные маскируются в отчетности, выписках и выгрузках ЦФТ, если у пользователя нет прав»** |
|  | Пользователь, у которого нет доступа к чувствительным данным, при формировании выписок / отчетов в word, xls из ЦФТ видит замаскированные данные |

По факту выполнения работ/оказания услуг Поставщик передает комплект документов на данную продукцию:

1. Подробная документация по Инструменту, включающей руководство по настройке и эксплуатации функциональности.
2. Обязательно наличие документации для следующих групп пользователей:
3. Системные администраторы (установка, настройка, старт, остановка, работа с неполадками, мониторинг системы)
4. Специалисты по безопасности (создание, настройка и применение правил)
5. Разработчики (описание API)