Аудит смарт-контракта.

Общее описание.
Смарт-контракт LeadRexToken предназначен для выпуска LeadRex токенов. В данном документе описаны выводы, полученные в ходе технического аудита контракта. Выявлены потенциальные проблемы и предложены методы их решения.

1. Анализ правильности введенных данных
Контракт соответствует стандарту ERC20, а именно его актуальной версии в репозитории (https://github.com/OpenZeppelin/openzeppelin-solidity/tree/master/contracts/token/ERC20).

2. Анализ кода смарт-контракта
2.1. Строка: 310
Статус: [Ошибка компиляции]
Описание: В конструктор контракта не передается адрес, на который будут выпущены токены. Из-за этого контракт выдает ошибку при компиляции.
Решение: добавить в конструктор аргумент типа address (строка 309 должна выглядеть так: constructor(address minter) public {…). Использовать эту переменную при вызове функции _mint (строка 310 должна выглядеть так: _mint(minter, INITIAL_SUPPLY);).

3. Использование библиотеки безопасной математики
Библиотека SafeMath соответствует актуальной версии в репозитории OpenZeppelin (https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/math/SafeMath.sol).

Выводы:
После публикации контракта будет выпущено 135,900,000 токенов LDX. Токен LDX будет иметь 18 знаков после запятой. Все токены будут переведены на адрес, переданный при публикации контракта в качестве аргумента. Контракт был опубликован и протестирован в тестовой сети Ropsten (https://ropsten.etherscan.io/token/0x6da131daa91da9fcdd62eb689b6aa5cc228eb9f9).