Digital Security

БЕЗОПАСНОСТЬ КАК ИСКУССТВО

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

по результатам проведения анализа защищённости
исходного кода смартконтракта
компании AA.M GROUP

Даты проведения работ:
26.12.2017-27.12.2017
Технический менеджер проекта:
А.О. Перцев
Директор департамента аудита:
А.Н. Тюрин

1. Введение

1.1. Общие положения

В настоящем экспертном заключении представлены результаты проведения работ по анализу защищенности исходного кода смартконтакта (далее – Система), принадлежащего компании AA.M GROUP (далее – Компания), а также предложены рекомендации по устранению выявленных слабостей (уязвимостей) и повышению уровня защищенности.

1.2. Принятые сокращения

Таблица 1.2–1. Принятые сокращения

Сокращение	Расшифровка
ИБ	Информационная безопасность
ИС	Информационная система
EVM	Виртуальная машина Ethereum
ERC20	Принятый стандарт токена в экосистеме Ethereum
Ether	Критовалюта в сети Ethereum
ICO	Initial coin offering

1.3. Резюме

В соответствии с договором ДСС-КУ-2017/40 от 25 декабря 2017 специалистами компании «Digital Security» в период с 26.12.17 по 27.12.17 были проведены работы по анализу защищенности исходного кода смартконтракта Компании.

Были рассмотрены следующие модели нарушителя:

- внешний нарушитель из сети Ethereum;
- внутренний (владелец или оператор).

Проведенные работы показали, что:

1. Имеющийся уровень безопасности смартконтракта можно определить как «средний».
2. Обнаружена одна критичная уязвимость.

Основными рекомендациями являются:

1. Устранение выявленных уязвимостей и слабостей.

Далее содержится описание выявленных недостатков и связанных с ними рисков информационной безопасности, а также детальные рекомендации по их устранению.

2. Принципы проведения работ

2.1. Угрозы ИБ

На информационные ресурсы Компании могут действовать следующие три угрозы ИБ: угрозы нарушения конфиденциальности, целостности и доступности.

Угроза нарушения конфиденциальности направлена на разглашение информации, имеющей в Компании статус конфиденциальной. При реализации угрозы информация становится известной лицам, которые не должны иметь к ней доступ – ряду сотрудников Компании, клиентам, партнерам, конкурентам, третьим лицам.

Угроза нарушения целостности направлена на модификацию или искажение информации, приводящее к изменению ее структуры или смысла, полному или частичному уничтожению.

Угроза нарушения доступности (угроза отказа в обслуживании) заключается в невозможности получения доступа к информационному ресурсу пользователями информационной системы.

Основным принципом проведения аудита ИБ является проверка возможности реализации указанных угроз, воздействующих на информационные ресурсы Системы, в рамках заданной модели нарушителя.

2.2. Модель нарушителя

В качестве вероятного нарушителя информационной безопасности Системы Компании рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий потенциально могут реализовать угрозы ИБ, осуществить посягательства на информационные ресурсы Системы и нанести ущерб интересам Компании.

В качестве угроз ИБ рассматриваются базовые угрозы нарушения конфиденциальности и целостности информации, а также угроза отказа Системы в обслуживании клиентов Компании.

Умышленно действующий нарушитель может преследовать следующие цели (а также их всевозможные комбинации):

- злонамеренный вызов отказа в обслуживании;
- повышение собственных привилегий;
- несанкционированное изменение критичной с точки зрения бизнеса информации.

В ходе работы были использованы модели внешнего и внутреннего нарушителя.

2.2.1. Внешний нарушитель

При проведении теста на проникновение используются следующие модели внешнего нарушителя:

- внешний нарушитель из сети Интернет, имеющий доступ к сети Ethereum и обладающий знаниями о тестируемой Системе (поскольку исходный код контракта открыт), но не обладающий правами в ней.

2.2.2. Внутренний нарушитель

При проведении теста на проникновение используются следующие модели внутреннего нарушителя:

- внутренний нарушитель из сети Ethereum, обладающий знаниями о тестируемой Системе и обладающий правами в ней.

2.3. Область тестирования

В ходе проведения работ был использован код, доступный по ссылке:

rinkeby.etherscan.io/address/0x5f8d71b04a4e91c45685aca4f5fbd9ac7b2fb279#code

Таблица 2.3 – 1. Область тестирования

Смартконтракт	Описание
SafeMath	Реализация безопасных вычислений
Ownable	Реализация разграничения владения и его передача
Pausable	Реализация возможности блокировки функций владельцем
ERC20	ERC20 – абстрактный класс
StandartToken	Реализация функциональности ERC20 токена
BurnableToken	Реализация функции «сжигания» токена
MintableToken	Реализация функции «выпускаемого» токена
Manageable	Реализация функциональности добавления и удаления менеджеров
Token	Свойства ALL.ME токена
Crowdsale	Реализация контракты распродажи ALL.ME токена

2.4. Сценарий ICO

До старта ICO выпускается 3 000 000 000 ME токенов для внутренних нужд проекта (зачисления пользователям, вознаграждения и т.п.). Далее выставляется цена токена для первой волны продаж, и начинается старт первой волны продаж.

По достижению определённого числа продаж владелец останавливает их вызовом функции pause(). Для начала следующей волны владелец вызовет фунцию unpause(), и так будет продолжаться до последней волны.

В процессе ICO цена ETH может меняться, поэтому владелец может в любой момент поставить контракт на паузу и скорректировать ее.

Другие характеристики:

- Эмиссия токенов ограничена (всего 10 000 000 000 токенов, токены выпускаются во время Crowdsale)
- Цена токена во время старта: 1 ETH = 200 токенов
- Минимальная сумма покупки: 0.001 ETH
- Токенов на продажу 7 000 000 000
- Средства от покупки токенов передаются бенефициару
- Закрытие Crowdsale происходит с помощью функции withdraw(): управление токеном передаётся бенефициару
- Изменение цены токена происходит функцией setTokenPrice(_value), где _value - количество токенов, приобретаемое за 1 Ethe0r. Смена стоимости токена доступна только во время паузы администратору, после завершения Crowdsale функция становится недоступной.

3. Анализ исходного кода смартконтракта

3.1. Перечень обнаруженных уязвимостей

3.1.1. Ошибка округления при покупке токенов

Критичность: высокая
Вероятность эксплуатации: высокая
Итоговый риск: высокий

Описание:

При расчете количества купленных токенов не учитывается, что EVM отбрасывает дробную часть при делении целых типов.

Риск:

Из-за отбрасываемой дробной части приобретаемых токенов пользователь будет терять некоторую часть токенов. Потерянная сумма может быть весомой для пользователя. Это также может привести к репутационному ущербу Компании.

Уязвимый ресурс:

- Crowdsale

Технические детали:

Для расчета количества токенов (amount), которые будут зачислены пользователю, используется следующий код:

```
uint public priceTokenWei = 1 ether / 200;           // 5000000000000000
uint sum = msg.value;                                // 333333333333333333
uint amount = sum.div(priceTokenWei).mul(1 ether);   // 660000000000000000
```

Отбрасывание дробной части происходит на этапе sum.div(priceTokenWei). Если вызвать функцию purchase() с 0.333333333333333333 ETH, то amount составит 66 токенов вместо 66.666666666666666600. То есть 333333333333333333 / 5000000000000000 = 66.

Рекомендации:

- Использовать паттерн RATE для вычисления amount.
- Или поменять очередность умножения и деления при вычислении amount.

3.2. Перечень обнаруженных слабостей

3.2.1. Избыточная функциональность

Описание:

Функция burn в контракте BurnableToken реализует функциональность «сжигания» токенов для вызывающего.

Уязвимый ресурс:

- BurnableToken

Рекомендации:

- Поскольку сценарий crowdsale и использование токенов не предусматривает их сжигание, рекомендуется убрать эту возможность.

3.2.2. Функция перевода токенов доступна во время паузы продаж

Описание:

В соответствии со сценарием ICO распродажа токенов будет приостанавливаться, чтобы разделить разные стадии продаж. Однако смартконтракт ограничивает не все возможности передачи токенов между участниками.

Риск:

Пользуясь отсутствием официальных продаж, некоторые участники могут перепродавать токены по их собственной цене.

Уязвимый ресурс:

- StandardToken

Технические детали:

Средствами смартконтракта приостановка продаж реализована с помощью модификаторов whenNotPaused и whenPaused контракта Pausable. Однако они применены только для функций контракта Crowdsale.

Рекомендации:

- Ограничить возможность использования функций transfer и transferFrom во время пауз продаж.

3.2.3. Версия компилятора не зафиксирована

Описание:

При финальном деплое контракт должен быть скомпилирован той версией компилятора, на которой он разрабатывался и тестировался.

Риск:

Фиксирование версии компилятора в исходном коде поможет избежать деплоя смартконтракта с использованием более новой версии компилятора, у которой выше риск наличия нераскрытых ошибок.

Уязвимый ресурс:

- Итоговый смарт-контракт

Технические детали:

Выбор версии компилятора реализуется с помощью директивы pragma solidity.

Рекомендации:

- Задать версию компилятора, например, pragma solidity 0.4.18; (следует обратить внимание на отсутствие знака **^**).

3.2.4. Менеджер не сможет закрыть ICO

Описание:

Смартконтракт предусматривает покупку токенов в других валютах через менеджера.

Риск:

Из-за строгого условия проверки превышения максимального количества токенов менеджер не сможет закрыть ICO.

Уязвимый ресурс:

- Crowdsale

Технические детали:

В функции externalPurchase происходит строгая проверка превышения выпускаемых токенов, из-за чего менеджер не сможет закрыть продажу (последней покупкой).

```
require(tokensSold.add(_value) < tokensForSale);
```

Рекомендации:

- Изменить знак < на <=.

3.3. Стилистические замечания

3.3.1. Комментарии

Описание:

Контракту Token предшествует комментарий, отражающий спецификацию на русском языке. Однако далее (для контракта Crowdsale) используются комментарии на английском.

Рекомендации:

- Привести комментарии к единому виду.

3.3.2. Название функции не отражает её функциональность

Описание:

Функция withdraw контракта Crowdsale реализует завершение ICO и смены владельца контракта Token, однако обычно такое название используется для функций, реализующих списание средств.

Рекомендации:

- Использовать название, соответствующее функциональности.

Приложение 1. Анализ уровня защищенности. Справочная информация

Анализ уровня защищенности

Для анализа уровня защищенности необходимо оценить критичность и вероятность реализации выявленных в ходе аудита уязвимостей. Вероятность реализации определяется доступностью и простотой реализации уязвимости.

Критичность реализации уязвимости

Свойство «критичность реализации» некоторой уязвимости характеризует возможные последствия реализации данной уязвимости с точки зрения угроз нарушения конфиденциальности, целостности и доступности информации, обрабатываемой на уязвимом ресурсе. Описание уровней критичности реализации уязвимостей приведено в Таблице А–1.

Таблица А–1. Уровни критичности уязвимостей

Значение	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Отсутствует	Не происходит	Не происходит	Не происходит
Низкий	Получение нарушителем доступа к некритичной информации в результате эскалации привилегий	Нарушение целостности некритичной информации с правами обычного пользователя	Кратковременный отказ в обслуживании критичного приложения
Средний	Нарушение конфиденциальности критичной информации с правами обычного пользователя	Нарушение целостности критичной информации с правами обычного пользователя	Отказ в обслуживании критичного приложения или кратковременный отказ в обслуживании
Высокий	Нарушение конфиденциальности критичной информации с правами	Нарушение целостности критичной информации с правами	Отказ в обслуживании

	администратора	администратора	

Простота эксплуатации уязвимости

Свойство «простота эксплуатации» некоторой уязвимости определяет, какие аппаратные и программные средства, профессиональные навыки, а также какое количество временных и вычислительных ресурсов, необходимо потенциальному нарушителю для реализации некоторой уязвимости (Таблица А–2).

Таблица А–2. Уровни простоты эксплуатации уязвимости

Значение	Описание
Низкий	Для эксплуатации уязвимости требуется разработка новых программных средств, проведение анализа конфигурации атакуемой системы, выявление и проверка различных возможных путей и условий успешной эксплуатации данной уязвимости, вычислительные мощности или временной резерв. Атакующий должен обладать значительными профессиональными навыками и познаниями в специфичных областях.
Средний	Для эксплуатации уязвимости требуется наличие специальных программных или аппаратных средств, проведение анализа конфигурации атакуемой системы, вычислительные мощности или временной резерв. Атакующему достаточно обладать незначительным объемом профессиональных навыков и познаний для реализации атаки.
Высокий	Для эксплуатации уязвимости не требуется использование специальных аппаратных или программных средств, значительные вычислительные мощности или временной резерв, детальное знание конфигурации атакуемой системы. Атакующему для реализации атаки не требуются специфичные профессиональные навыки и познания.

Доступность уязвимости

Свойство «доступность» некоторой уязвимости определяет, каким классам пользователей доступен уязвимый ресурс (Таблица А–3).

Таблица А–3. Уровни доступности

Значение	Описание
Низкий	Привилегированные пользователи
Средний	Зарегистрированные пользователи
Высокий	Все пользователи

Вероятность эксплуатации уязвимости

Вероятность эксплуатации уязвимости рассчитывается на основе простоты эксплуатации и области доступности уязвимости по таблице А–4.

Таблица А–4. Уровень вероятности эксплуатации

Вероятность эксплуатации		Простота эксплуатации		
		Низкий	Средний	Высокий
Доступность	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Риск уязвимости

Риск уязвимости (по одной из угроз) рассчитывается на основе критичности уязвимости (по одной из угроз) и вероятности эксплуатации уязвимости по таблице А–5.

Таблица А–5. Уровень риска

Риск уязвимости		Вероятность эксплуатации		
		Низкий	Средний	Высокий
Критичность уязвимости	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Приложение 2. Анализ уровня защищенности. Перечень обнаруженных слабостей и уязвимостей

Обнаруженные в ходе работ уязвимости и слабости Системы представлены в таблице Б-1.

Таблица Б-1. Перечень обнаруженных уязвимостей и слабостей Системы

Перечень обнаруженных уязвимостей		
Уязвимость	**Итоговый риск**	**Подробности в пункте**
Ошибка округления при покупке токенов	Высокий	3.1.1.
Перечень обнаруженных слабостей		
Слабость	**Подробности в пункте**	
Избыточная функциональность	3.2.1.	
Функция перевода токенов доступна во время паузы продаж	3.2.2.	
Не зафиксирована версия компилятора	3.2.3.	
Менеджер не сможет закрыть ICO	3.2.4.	