We Can Develop IT

Независимый аудит смарт-контрактов Kassa 400/100 Kassa 200/50 Kassa 100/30

от компании We Can Develop IT

Версия 2.0
Обновлено 11.12.2018

Оглавление

Контракт Kassa 400/100 (депозит средств с реферальной бонусной системой)

Описание программы KASSA 400/100

Адрес смарт контракта: 0x069b5065fadfedbfe9094029234a9bc3838f2f2e
Дата окончания аудита и публикация контракта: 11.12.2018

Общий функционал для всех контрактов:
Каждый день суточный лимит для всех контрактов будет увеличиваться на 2%
Изначальный лимит для всех программ ставим 50 ETH в сутки
Максимальная сумма депозита с 1-го кошелька:
Программа Kassa 400/100: 50 ETH +1% в день
Программа 200/50: 50 ETH +1% в день
Программа 100/30: 50 ETH+1% в день

Сумма начисления в сутки: 1%
Сумма удержания в фонд проекта: 5%
Реферальные пригласителю:
Линк (1 линия): 5%
2-я линия: 2%
3-я линия: 1%
4-я линия: 1%
5-я линия: 2%
Минимальная сумма взноса: 1 ETH
Максимальная сумма взноса: 50 ETH
Лимит на взнос средств в сутки:
лимит растет каждый день на 2% до 100 ETH и потом останавливается на достигнутом уровне. Общий лимит на взносы в систему устанавливается с 50 ETH и растет 1% в день до достижения уровня в 100 ETH. Установлен общий порог лимитов, который снимается при достижении общей суммы депозитов более 3000 ETH.

При превышении лимита в сутки, действует система автовозврата с удержанием штрафа в 10% от суммы депозиты.

Если в качестве реферера указать самого себя, функционирование реферальной программы не произойдет, но, тем не менее, пользователю удастся обойти выплату лишних 10% на кошелек системы.

Контракт обеспечивает пользователю возможность инвестировать любую сумму в ETH (от 1 до 50) в контракт и получить 200% возврат в течение 400 дней. Отправить эфир

можно напрямую на адрес контракта, либо вызвав функцию invest. Каждый последующий вклад ведется раздельно в контракте, с целью сохранения срока выплаты по каждой инвестиции.

Сумма к выплате начинает насчитываться сразу после вклада, вывод доступен в любое время.

Вывод пользователем осуществляется отправкой 0 эфиров на адрес контракта, либо вызовом функции withdraw.

Все начисления суммируются и доступны к выводу в любое время, т.е. не имеет значения в какой момент пользователь решит снять дивиденды.

Если пользователь запрашивает вывод средств сразу после инвестирования, то пользователю не выплачиваются дивиденды, а списывается 10%.

Выполненные тестовые кейсы

Тестирование выполнялось как вручную, так и с использованием автоматических скриптов. Контракт тестировался в режиме ускоренного времени.

KASSA Base				
1	**Кейс**	**Шаги**	**Ожидаемый Результат**	**Статус**
2	Перевод средств на депозит с одного кошелька с минимально допустимой суммой	Перевести с кошелька сумму 1 eth на депозит с указанием реферала	Средства зачислены на счет контракта	pass
3	Перевод средств на депозит с одного кошелька ниже минимально допустимой суммы (0.99)	Перевести с кошелька сумму 0.99 eth на депозит с указанием реферала	Средства остаются на счету системы	pass
4	Перевод средств в размере 1 eth на депозит в первый раз с указанием овнера как реферала	После активации кошелька при первом переводе средств на депозит указать овнера как реферала	Средства зачислены на счет контракта. Комиссия и реферальный бонус начислен на счет овнера	pass
5	Перевод средств на депозит с одного кошелька с максимально допустимой суммой с указанием реферала	Перевести с кошелька сумму в 50 eth на депозит с указанием реферала	Средства зачислены на счет системы в размере 50 eth комиссия в размере 5% зачислена на счет овнера, реферальные 5% зачислены рефералу	pass

6	Перевод средств на депозит овнера свыше максимальной суммы	Перевести с кошелька сумму в 10 eth на депозит с указанием реферала	Средства возвращаются на счет пользователя с удержанием штрафа 10%	pass
7	Перевод средств на депозит овнера ниже минимальной суммы	Перевести с кошелька сумму в 0.99 eth на депозит с указанием реферала	Средства остаются на балансе системы	pass
8	Запросить вывод процентов сразу после пополнения	Перевести с кошелька сумму в 1 eth на депозит с указанием реферала Запросить вывод выплат.	Взымается только комиссия за вызов метода	pass
9	Пополнить депозит с одного кошелька на 0.99	Перевести с кошелька сумму в 0.99 eth на депозит с указанием реферала	Сумма переведена на счет системы процент за транзакцию снят	pass
10	Пополнить депозит с одного кошелька на 50.001	Перевести с кошелька сумму в 50.01 eth на депозит с указанием реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
11	Пополнить депозит с нескольких кошельков для достижения дневного лимита	Перевести с 5 разных кошельков сумму в 10.eth на депозит с указанием реферала	Для 6-го перевода средства возвращаются на счет пользователя с удержанием штрафа 10%	pass
12	Перевод средств в размере 1 eth на депозит без указания реферала	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
13	Пользователь должен получить возврат вносимых средств на депозит при вводе неверной реферальной ссылки с удержанием 10% штрафа	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
14	Убедиться что штраф не превышает 10%	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
15	Убедиться , что пользователь может получать несколько реферальных начислений	Указать у нескольких пользователей одного и того же реферала	Реферальные приходят с каждого депозита	pass
16	Убедиться , что пользователь может	Указать у нескольких пользователей одного и того	Реферальные 5% приходят с каждого	pass

	получать несколько реферальных начислений одного типа (5%)	же реферала	нового депозита	
17	Убедиться что комиссия системы не превышает 5%	отправить 10 eth	Комиссия системы 0.5 eth	pass
18	Убедиться, что реферальная комиссия не превышает 5%	Отправить несколько депозитов с разных кошельков с указанием одного и того же реферала	Реферальные вознаграждения 5% с каждого депозита	pass
19	Проверить суточный лимит не должен превышать 50 eth	Отправить несколько депозитов с разных кошельков с указанием реферала на общую сумму 51 eth	При последней переводе депозита осуществляется автовозврат средств с удержанием штрафа 10%	pass
20	Поверить, что суточный лимит не изменится, если участник отправит больше максимально допустимой суммы		Выполняется полный возврат средств с удержанием штрафа	pass
21	Автовыплата реферальных по достижению порога в 0.015 ETH		Средства начислены на счет пользователя	pass
22	Запрос на выплаты: перевод на адрес смарт-контракта 0 eth с необходимым количеством газа		На счет пользователя приходит сумма процентов с учетом прошедшего времени с момента депозита	pass
23	Запрос выплаты: перевод на адрес смарт-контракта 0 eth в день пополнения депозита		Взымается только комиссия за вызов метода	pass
24	Запрос выплаты при недостаточном балансе смарт-контракта		Возвращается ошибка: revert Not enough balance. Please retry later.	pass
25	Проверка реферальной системы - 1 уровень			pass
26	Проверка динамического максимального лимита на 1 перевод	Перевести на 10 день сумму в 50.01eth	Сумма успешно переведена на баланс системы	pass

27	Проверка динамического максимального лимита на суточный перевод	Перевести на 10 день сумму в 50.5eth	Сумма успешно переведена на баланс системы	pass
28	Депозит закончился, но кто-то делает депозит и указывает этот кошелёк в качестве реферера		Депозит зачислен на счёт нового пользователя, реферальные зачислены	pass
29	Пользователь должен получить возврат вносимых средств на депозит, при вводе в качестве реферального своего кошелька, с удержанием 10% штрафа		Деньги возвращены пользователю, штраф начислен на баланс системы	pass
30	Пользователь должен получить возврат вносимых средств на депозит, при вводе в качестве реферала свой кошелек, с удержанием 10% штрафа, в том числе когда срок депозита закончился		Деньги возвращены пользователю, штраф начислен на баланс системы	pass
31	Проверить начисление реферального вознаграждения в размере (5%/1%/1%/1%/2%) для базового контракта	1 - При отправке первого депозита указать кошелек овнера как реферала 2 - При отправки 2-го депозита с кошелька 2, указать реферала кошелек 1 предыдущего отправителя 3 - При отправки 3 депозита с кошелька 3, указать реферала адресный кошелек 2-го отправителя 4 - При отправки 4 депозита с кошелька 4, указать реферала адресный кошелек 3-го отправителя 5 - При отправки 5 депозита с кошелька 5, указать реферала адресный кошелек 4-го отправителя 6 - При отправки 6 депозита с кошелька 6, указать реферала адресный кошелек 5-го отправителя	1) Овнер должен получить премию в размере 5% от суммы вносимого депозита +5% комиссии 2) Премию в размере 5% от суммы вносимого депозита должен получить владелец 1 кошелька, а собственнику должно быть начислено 1% от суммы вносимых средств +5% комиссии 3) Премию в размере 5% от суммы вносимого депозита должен получить владелец 2 кошелька, а овнеру должно начислиться 1% от суммы вносимых средств +5% комиссии 4) Премию в размере 5% от суммы вносимого	pass

			депозита должен получить владелец 3 кошелька, а собственнику должно быть начислено 1% от суммы вносимых средств +5% комиссии 5) Премию в размере 5% от суммы вносимого депозита должен получить владелец 4 кошелька, а собственнику должно быть начислено 2% от суммы вносимых средств +5% комиссии 6) Премию в размере 5% от суммы вносимого депозита должен получить владелец 5 кошелька, а собственнику должно быть начислено 2% от суммы вносимых средств +5% комиссии	
32	Овнер не должен получать реферальные начисления после 5 уровня	1 - При отправке первого депозита указать кошелек овнера как реферала 2 - При отправки 2-го депозита с кошелька 2, указать реферала кошелек 1 предыдущего отправителя 3 - При отправки 3 депозита с кошелька 3, указать реферала адресный кошелек 2-го отправителя 4 - При отправки 4 депозита с кошелька 4, указать реферала адресный кошелек 3-го отправителя 5 - При отправки 5 депозита с кошелька 5, указать реферала адресный кошелек 4-го отправителя 6 - При отправки 6 депозита с кошелька 6, указать реферала адресный кошелек 5-го отправителя	Овнер должен получить только 5% комиссии	pass
33	Дневной лимит должен увеличиваться			pass

	ежедневно			
34	Проверить начисление вознаграждения на 400 день		Пользователь должен получить вознаграждение в 2 раза больше от вносимых средств	pass

https://docs.google.com/spreadsheets/d/1Usj94doyz3g4QUNrOgF7P1EgPpvr-jUGBVcRw6WBLuM/edit#gid=1511536476

Результаты Аудита

Дата окончания аудита контракта: 11.12.2018
Критические уязвимости: 0
Ошибки и проблемы: 0
Возможности оптимизации: 1
Возможности снизить стоимость транзакций и уменьшить количество строк кода.
Результаты оптимизации: была реализован алгоритм вычисления лимитов контракта на основе квадратичной оптимизации, что позволило уйти от рекурсивных вычислений и сократить стоимость транзакций.

Примечания и рекомендации

В данном контракте используется библиотека безопасных вычислений SafeMath, предотвращающая ошибки в вычислениях в смарт контрактах.

В контракте данная библиотека используется не повсеместно, а только в формулах для расчета выплат инвесторам. Во всех остальных случаях угроз переполнения нет, так как вычисления не позволяют выйти за рамки 0 и 2256-1, следовательно, все вычисления в контракте безопасны.

Код контракта мог содержать потенциальную возможность закрывать вклад средств в проект. Однако, после проведения проверки адресов:

(assembly { size := extcodesize(addr) })

было доказано, что адреса для перечисления комиссии не являются смарт контрактами, которые могли бы воспрепятствовать отправлению на их баланс комиссии с проекта. Следовательно, возможности дополнительно остановить прием средств у владельцев в контракте нет.

Вызов возврата выплаты может быть инициирован нулевой транзакцией с кошелька, но некоторые кошельки не предоставляют возможности проводить транзакции данного

типа. Следовательно, пользователи зашедшие в проект с такого кошелька, смогут вывести свои средства, только подключив интерфейс контракта в кошельке и вызвав функцию withdraw, либо экспортировав приватный ключ в другой кошелек.

Контракт KASSA 200/50

Результат Аудита от 11.12.2018 по контракту 0x72fa6623cc0800bc180639d60c33c95426d76576

Описание программы KASSA 200/50

Каждый день суточный лимит для всех контрактов будет увеличиваться на 2%
Изначальный лимит для всех программ ставим 50 ETH в сутки
Максимальная сумма депозита с 1-го кошелька:
Программа 200/50: 50 ETH +1% в день

Срок работы депозита: 200 дней (доход +50% от суммы взноса)
Сумма начисления в сутки: 0.75%
Сумма удержания в фонд проекта: 7%
Реферальные пригласителю: 5%
2-я линия: 2%
2-я линия: 1%
Минимальная сумма взноса: 0.5 ETH
Максимальная сумма взноса: 30 ETH

Выполненные тестовые кейсы

Тестирование выполнялось как вручную, так и с использованием автоматических скриптов. Контракт тестировался в режиме ускоренного времени.

KASSA Stable				
1	**Кейс**	**Шаги**	**Ожидаемый Результат**	**Статус**
2	Перевод средств на депозит с одного	Перевести с кошелька сумму 1 eth на депозит с	Средства зачислены на счет контракта	pass

	кошелька с минимально допустимой суммой	указанием реферала		
3	Перевод средств на депозит с одного кошелька ниже минимально допустимой суммы (0.99)	Перевести с кошелька сумму 0.99 eth на депозит с указанием реферала	Средства остаются на счету системы	pass
4	Перевод средств в размере 1 eth на депозит в первый раз с указанием овнера как реферала	После активации кошелька при первом переводе средств на депозит указать овнера как реферала	Средства зачислены на счет контракта. Комиссия и реферальный бонус начислен на счет овнера	pass
5	Перевод средств на депозит с одного кошелька с максимально допустимой суммой с указанием реферала	Перевести с кошелька сумму в 50 eth на депозит с указанием реферала	Средства зачислены на счет системы в размере 50 eth комиссия в размере 5% зачислена на счет овнера, реферальные 5% зачислены рефералу	pass
6	Перевод средств на депозит овнера свыше максимальной суммы	Перевести с кошелька сумму в 10 eth на депозит с указанием реферала	Средства возвращаются на счет пользователя с удержанием штрафа 10%	pass
7	Перевод средств на депозит овнера ниже минимальной суммы	Перевести с кошелька сумму в 0.99 eth на депозит с указанием реферала	Средства остаются на балансе системы	pass
8	Запросить вывод процентов сразу после пополнения	Перевести с кошелька сумму в 1 eth на депозит с указанием реферала Запросить вывод выплат.	Взымается только комиссия за вызов метода	pass
9	Пополнить депозит с одного кошелька на 0.99	Перевести с кошелька сумму в 0.99 eth на депозит с указанием реферала	Сумма переведена на счет системы процент за транзакцию снят	pass
10	Пополнить депозит с одного кошелька на 50.001	Перевести с кошелька сумму в 50.01 eth на депозит с указанием реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
11	Пополнить депозит с нескольких кошельков для достижения дневного лимита	Перевести с 5 разных кошельков сумму в 10.eth на депозит с указанием реферала	Для 6-го перевода средства возвращаются на счет пользователя с удержанием штрафа 10%	pass
12	Перевод средств в размере 1 eth на депозит	Перевести с кошелька сумму в 1 eth на депозит без	Сумма возвращается на счет пользователя с	pass

	без указания реферала	указания реферала	удержанием штрафа в 10%	
13	Пользователь должен получить возврат вносимых средств на депозит при вводе неверной реферальной ссылки с удержанием 10% штрафа	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
14	Убедиться что штраф не превышает 10%	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
15	Убедиться , что пользователь может получать несколько реферальных начислений	Указать у нескольких пользователей одного и того же реферала	Реферальные приходят с каждого депозита	pass
16	Убедиться , что пользователь может получать несколько реферальных начислений одного типа (5%)	Указать у нескольких пользователей одного и того же реферала	Реферальные 5% приходят с каждого нового депозита	pass
17	Убедиться что комиссия системы не превышает 5%	отправить 10 eth	Комиссия системы 0.5 eth	pass
18	Убедиться, что реферальная комиссия не превышает 5%	Отправить несколько депозитов с разных кошельков с указанием одного и того же реферала	Реферальные вознаграждения 5% с каждого депозита	pass
19	Проверить суточный лимит не должен превышать 50 eth	Отправить несколько депозитов с разных кошельков с указанием реферала на общую сумму 51 eth	При последней переводе депозита осуществляется автовозврат средств с удержанием штрафа 10%	pass
20	Поверить, что суточный лимит не изменится, если участник отправит больше максимально допустимой суммы		Выполняется полный возврат средств с удержанием штрафа	pass
21	Автовыплата реферальных по достижению порога в 0.015 ETH		Средства начислены на счет пользователя	pass

22	Запрос на выплаты: перевод на адрес смарт-контракта 0 eth с необходимым количеством газа		На счет пользователя приходит сумма процентов с учетом прошедшего времени с момента депозита	pass
23	Запрос выплаты: перевод на адрес смарт-контракта 0 eth в день пополнения депозита		Взымается только комиссия за вызов метода	pass
24	Запрос выплаты при недостаточном балансе смарт-контракта		Возвращается ошибка: revert Not enough balance. Please retry later.	pass
25	Проверка реферальной системы - 1 уровень			pass
26	Проверка динамического максимального лимита на 1 перевод	Перевести на 10 день сумму в 50.01eth	Сумма успешно переведена на баланс системы	pass
27	Проверка динамического максимального лимита на суточный перевод	Перевести на 10 день сумму в 50.5eth	Сумма успешно переведена на баланс системы	pass
28	Депозит закончился, но кто-то делает депозит и указывает этот кошелёк в качестве реферера		Депозит зачислен на счёт нового пользователя, реферальные зачислены	pass
29	Пользователь должен получить возврат вносимых средств на депозит, при вводе в качестве реферального своего кошелька, с удержанием 10% штрафа		Деньги возвращены пользователю, штраф начислен на баланс системы	pass
30	Пользователь должен получить возврат вносимых средств на депозит, при вводе в качестве реферала свой кошелек, с удержанием 10% штрафа, в том числе когда срок депозита закончился		Деньги возвращены пользователю, штраф начислен на баланс системы	pass
31	Проверить начисление реферального	1 - При отправке первого депозита указать кошелек	1) Овнер должен получить премию в	pass

	вознаграждения в размере (5%/1%/1%/1%/2%) для базового контракта	овнера как реферала 2 - При отправки 2-го депозита с кошелька 2, указать реферала кошелек 1 предыдущего отправителя 3 - При отправки 3 депозита с кошелька 3, указать реферала адресный кошелек 2-го отправителя 4 - При отправки 4 депозита с кошелька 4, указать реферала адресный кошелек 3-го отправителя 5 - При отправки 5 депозита с кошелька 5, указать реферала адресный кошелек 4-го отправителя 6 - При отправки 6 депозита с кошелька 6, указать реферала адресный кошелек 5-го отправителя	размере 5% от суммы вносимого депозита +5% комиссии 2) Премию в размере 5% от суммы вносимого депозита должен получить владелец 1 кошелька, а собственнику должно быть начислено 1% от суммы вносимых средств +5% комиссии 3) Премию в размере 5% от суммы вносимого депозита должен получить владелец 2 кошелька, а овнеру должно начислиться 1% от суммы вносимых средств +5% комиссии 4) Премию в размере 5% от суммы вносимого депозита должен получить владелец 3 кошелька, а собственнику должно быть начислено 1% от суммы вносимых средств +5% комиссии 5) Премию в размере 5% от суммы вносимого депозита должен получить владелец 4 кошелька, а собственнику должно быть начислено 2% от суммы вносимых средств +5% комиссии 6) Премию в размере 5% от суммы вносимого депозита должен получить владелец 5 кошелька, а собственнику должно быть начислено 2% от суммы вносимых средств +5% комиссии	
32	Овнер не должен получать реферальные начисления после 5	1 - При отправке первого депозита указать кошелек овнера как реферала	Овнер должен получить только 5% комиссии	pass

	уровня	2 - При отправки 2-го депозита с кошелька 2, указать реферала кошелек 1 предыдущего отправителя 3 - При отправки 3 депозита с кошелька 3, указать реферала адресный кошелек 2-го отправителя 4 - При отправки 4 депозита с кошелька 4, указать реферала адресный кошелек 3-го отправителя 5 - При отправки 5 депозита с кошелька 5, указать реферала адресный кошелек 4-го отправителя 6 - При отправки 6 депозита с кошелька 6, указать реферала адресный кошелек 5-го отправителя		
33	Дневной лимит должен увеличиваться ежедневно			pass
34	Проверить начисление вознаграждения на 400 день		Пользователь должен получить вознаграждение в 2 раза больше от вносимых средств	pass

Ссылка на производимые кейсы:
https://docs.google.com/spreadsheets/d/1Usj94doyz3g4QUNrOgF7P1EgPpvr-jUGBVcRw6WBLuM/edit#gid=1511536476

Результат аудита

Критические уязвимости: 0
Ошибки и проблемы: 0
Возможности оптимизации: 1
Возможности снизить стоимость транзакций и уменьшить количество строк кода.
Примечания и рекомендации: 0
Результаты оптимизации: была реализован алгоритм вычисления лимитов контракта на основе квадратичной оптимизации, что позволило уйти от рекурсивных вычислений и сократить стоимость транзакций.

Заключение по контракту KASSA 200/50

За время проведения тестирования контракта 0x72fa6623cc0800bc180639d60c33c95426d76576 ошибок не обнаружено.

Контракт KASSA 100/30

Результат Аудита от 11.12.2018 по контракту 0xb0601ee3d8ed87a7f7cd9264ec5d02fe5ae30c97

Описание программы KASSA 100/30

Срок работы депозита: 100 дней (доход +30% от суммы взноса)
Сумма начисления в сутки: 1.30%
Сумма удержания в фонд проекта: 8%
Реферальные пригласителю: 7%
Минимальная сумма взноса: 0.25 ETH
Максимальная сумма взноса: 15 ETH

Лимит на ввод средств в сутки:
лимит растет каждый день на 2% до 100 ETH и потом останавливается на достигнутом уровне. Общий лимит на взносы в систему устанавливается с 50 ETH и растет 1% в день до достижения уровня в 100 ETH. Установлен общий порог лимитов, который снимается при достижении общей суммы депозитов более 3000 ETH.

Реферальные пригласителю:
Личник (1 линия): 7%

Выполненные тестовые кейсы

Тестирование выполнялось как вручную, так и с использованием автоматических скриптов. Контракт тестировался в режиме ускоренного времени.

KASSA Fast				
1	**Кейс**	**Шаги**	**Ожидаемый Результат**	**Статус**

2	Перевод средств на депозит с одного кошелька с минимально допустимой суммой	Перевести с кошелька сумму 1 eth на депозит с указанием реферала	Средства зачислены на счет контракта	pass
3	Перевод средств на депозит с одного кошелька ниже минимально допустимой суммы (0.99)	Перевести с кошелька сумму 0.99 eth на депозит с указанием реферала	Средства остаются на счету системы	pass
4	Перевод средств в размере 1 eth на депозит в первый раз с указанием овнера как реферала	После активации кошелька при первом переводе средств на депозит указать овнера как реферала	Средства зачислены на счет контракта. Комиссия и реферальный бонус начислен на счет овнера	pass
5	Перевод средств на депозит с одного кошелька с максимально допустимой суммой с указанием реферала	Перевести с кошелька сумму в 50 eth на депозит с указанием реферала	Средства зачислены на счет системы в размере 50 eth комиссия в размере 5% зачислена на счет овнера, реферальные 5% зачислены рефералу	pass
6	Перевод средств на депозит овнера свыше максимальной суммы	Перевести с кошелька сумму в 10 eth на депозит с указанием реферала	Средства возвращаются на счет пользователя с удержанием штрафа 10%	pass
7	Перевод средств на депозит овнера ниже минимальной суммы	Перевести с кошелька сумму в 0.99 eth на депозит с указанием реферала	Средства остаются на балансе системы	pass
8	Запросить вывод процентов сразу после пополнения	Перевести с кошелька сумму в 1 eth на депозит с указанием реферала Запросить вывод выплат.	Взымается только комиссия за вызов метода	pass
9	Пополнить депозит с одного кошелька на 0.99	Перевести с кошелька сумму в 0.99 eth на депозит с указанием реферала	Сумма переведена на счет системы процент за транзакцию снят	pass
10	Пополнить депозит с одного кошелька на 50.001	Перевести с кошелька сумму в 50.01 eth на депозит с указанием реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
11	Пополнить депозит с нескольких кошельков для достижения дневного лимита	Перевести с 5 разных кошельков сумму в 10.eth на депозит с указанием реферала	Для 6-го перевода средства возвращаются на счет пользователя с удержанием штрафа 10%	pass

12	Перевод средств в размере 1 eth на депозит без указания реферала	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
13	Пользователь должен получить возврат вносимых средств на депозит при вводе неверной реферальной ссылки с удержанием 10% штрафа	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
14	Убедиться что штраф не превышает 10%	Перевести с кошелька сумму в 1 eth на депозит без указания реферала	Сумма возвращается на счет пользователя с удержанием штрафа в 10%	pass
15	Убедиться , что пользователь может получать несколько реферальных начислений	Указать у нескольких пользователей одного и того же реферала	Реферальные приходят с каждого депозита	pass
16	Убедиться , что пользователь может получать несколько реферальных начислений одного типа (5%)	Указать у нескольких пользователей одного и того же реферала	Реферальные 5% приходят с каждого нового депозита	pass
17	Убедиться что комиссия системы не превышает 5%	отправить 10 eth	Комиссия системы 0.5 eth	pass
18	Убедиться, что реферальная комиссия не превышает 5%	Отправить несколько депозитов с разных кошельков с указанием одного и того же реферала	Реферальные вознаграждения 5% с каждого депозита	pass
19	Проверить суточный лимит не должен превышать 50 eth	Отправить несколько депозитов с разных кошельков с указанием реферала на общую сумму 51 eth	При последней переводе депозита осуществляется автовозврат средств с удержанием штрафа 10%	pass
20	Поверить, что суточный лимит не изменится, если участник отправит больше максимально допустимой суммы		Выполняется полный возврат средств с удержанием штрафа	pass
21	Автовыплата реферальных по достижению порога в		Средства начислены на счет пользователя	pass

	0.015 ETH			
22	Запрос на выплаты: перевод на адрес смарт-контракта 0 eth с необходимым количеством газа		На счет пользователя приходит сумма процентов с учетом прошедшего времени с момента депозита	pass
23	Запрос выплаты: перевод на адрес смарт-контракта 0 eth в день пополнения депозита		Взымается только комиссия за вызов метода	pass
24	Запрос выплаты при недостаточном балансе смарт-контракта		Возвращается ошибка: revert Not enough balance. Please retry later.	pass
25	Проверка реферальной системы - 1 уровень			pass
26	Проверка динамического максимального лимита на 1 перевод	Перевести на 10 день сумму в 50.01eth	Сумма успешно переведена на баланс системы	pass
27	Проверка динамического максимального лимита на суточный перевод	Перевести на 10 день сумму в 50.5eth	Сумма успешно переведена на баланс системы	pass
28	Депозит закончился, но кто-то делает депозит и указывает этот кошелёк в качестве реферера		Депозит зачислен на счёт нового пользователя, реферальные зачислены	pass
29	Пользователь должен получить возврат вносимых средств на депозит, при вводе в качестве реферального своего кошелька, с удержанием 10% штрафа		Деньги возвращены пользователю, штраф начислен на баланс системы	pass
30	Пользователь должен получить возврат вносимых средств на депозит, при вводе в качестве реферала свой кошелек, с удержанием 10% штрафа, в том числе когда срок депозита закончился		Деньги возвращены пользователю, штраф начислен на баланс системы	pass

31	Проверить начисление реферального вознаграждения в размере (5%/1%/1%/1%/2%) для базового контракта	1 - При отправке первого депозита указать кошелек овнера как реферала 2 - При отправки 2-го депозита с кошелька 2, указать реферала кошелек 1 предыдущего отправителя 3 - При отправки 3 депозита с кошелька 3, указать реферала адресный кошелек 2-го отправителя 4 - При отправки 4 депозита с кошелька 4, указать реферала адресный кошелек 3-го отправителя 5 - При отправки 5 депозита с кошелька 5, указать реферала адресный кошелек 4-го отправителя 6 - При отправки 6 депозита с кошелька 6, указать реферала адресный кошелек 5-го отправителя	1) Овнер должен получить премию в размере 5% от суммы вносимого депозита +5% комиссии 2) Премию в размере 5% от суммы вносимого депозита должен получить владелец 1 кошелька, а собственнику должно быть начислено 1% от суммы вносимых средств +5% комиссии 3) Премию в размере 5% от суммы вносимого депозита должен получить владелец 2 кошелька, а овнеру должно начислиться 1% от суммы вносимых средств +5% комиссии 4) Премию в размере 5% от суммы вносимого депозита должен получить владелец 3 кошелька, а собственнику должно быть начислено 1% от суммы вносимых средств +5% комиссии 5) Премию в размере 5% от суммы вносимого депозита должен получить владелец 4 кошелька, а собственнику должно быть начислено 2% от суммы вносимых средств +5% комиссии 6) Премию в размере 5% от суммы вносимого депозита должен получить владелец 5 кошелька, а собственнику должно быть начислено 2% от суммы вносимых средств +5% комиссии	pass
32	Овнер не должен	1 - При отправке первого	Овнер должен получить	pass

	получать реферальные начисления после 5 уровня	депозита указать кошелек овнера как реферала 2 - При отправки 2-го депозита с кошелька 2, указать реферала кошелек 1 предыдущего отправителя 3 - При отправки 3 депозита с кошелька 3, указать реферала адресный кошелек 2-го отправителя 4 - При отправки 4 депозита с кошелька 4, указать реферала адресный кошелек 3-го отправителя 5 - При отправки 5 депозита с кошелька 5, указать реферала адресный кошелек 4-го отправителя 6 - При отправки 6 депозита с кошелька 6, указать реферала адресный кошелек 5-го отправителя	только 5% комиссии	
33	Дневной лимит должен увеличиваться ежедневно			pass
34	Проверить начисление вознаграждения на 400 день		Пользователь должен получить вознаграждение в 2 раза больше от вносимых средств	pass

Ссылка на производимые кейсы:
https://docs.google.com/spreadsheets/d/1Usj94doyz3g4QUNrOgF7P1EgPpvr-jUGBVcRw6WBLuM/edit#gid=0

Результат аудита

Критические уязвимости: 0
Ошибки и проблемы: 0
Возможности оптимизации: 1
Возможности снизить стоимость транзакций и уменьшить количество строк кода.
Примечания и рекомендации: 0
Результаты оптимизации: была реализован алгоритм вычисления лимитов контракта на основе квадратичной оптимизации, что позволило уйти от рекурсивных вычислений и сократить стоимость транзакций.

Заключение по контракту KASSA 100/30

В процессе тестирования контракта 0xb0601ee3d8ed87a7f7cd9264ec5d02fe5ae30c97 ошибок не обнаружено.

Краткое заключение по итогам аудита

В данных контрактах критических уязвимостей и бэкдоров не обнаружено, функционал контракта безопасен и может быть использован для оборота криптовалютных средств.

В коде контракта не выявлено никаких механизмов для изменения кода контракта после его публикации.

Следует отметить, что возможность выплаты процентов с каждого из перечисленных выше контрактов зависит от суммы депозитов поступивших на счет кошелька и размера обязательств по выплатам. Если на балансе контракта недостаточно криптовалютных средств, то в выплате будет отказано. Это заложено в логике контрактов.

Примечание:

Данный аудит носит ознакомительный характер и не является призывом к участию в проекте. Аудит оценивает исключительно техническое качество исходного кода и соответствие разработанного кода предоставленному техническому заданию.