Разработка и исследование системы аутентификации на основе технологии блокчейн

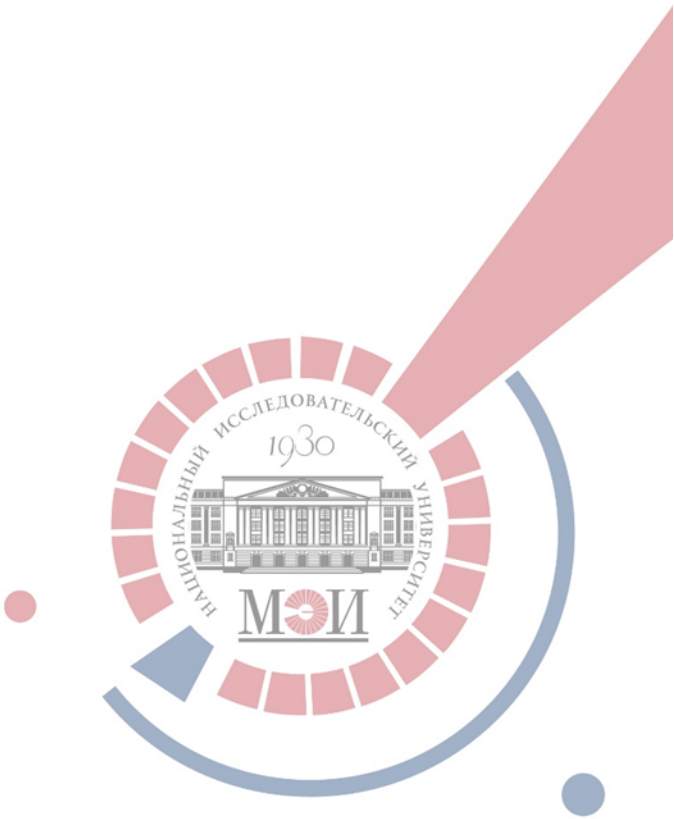
Выполнил: Пайков А.С.
Научный руководитель: Рытов А.А.

Информационные атаки

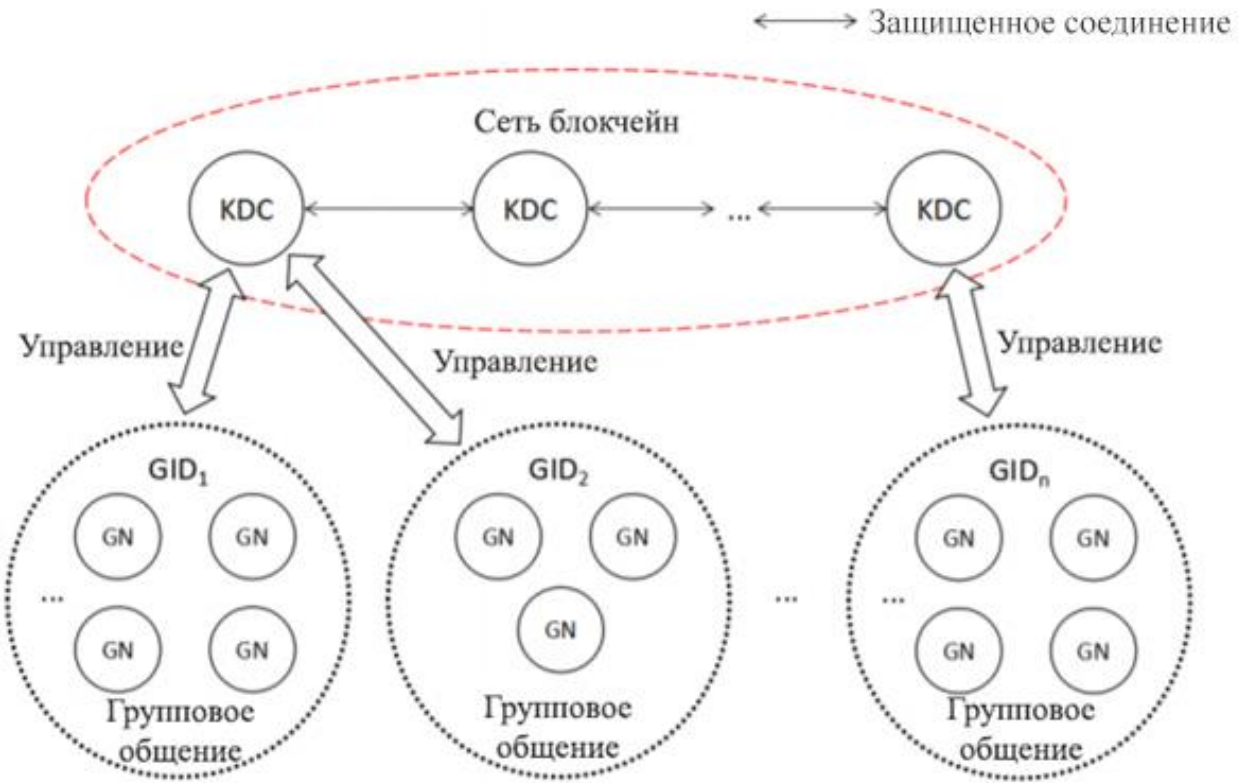
Разновидности информационных атак

1. Вторжение в узел;
2. Внедрение зависимостей узла;
3. Атака захвата узла;
4. Атака с прослушиванием;
5. Клонирование узла;
6. Радиочастотные помехи;
7. Атака с повтором;
8. Атака подмены устройств;
9. Приступ лишения сна;
10. Атака временного отключения;
11. Атака с неавторизированным доступом;
12. Аутентификация и авторизация;
13. Атака перевыполнения буфера;
14. DDoS – атака;
15. Атака с передачей большой полезной нагрузки;
16. Имитация поведения устройства;
17. Управление разрешениями;
18. Наводнение полезной нагрузки;
19. SQLi;
20. DoS – атака;
21. Атака Сибиллы;
22. Воронка;
23. Атака черной дыры;
24. Атака анализа трафика;
25. Атака “Человек посередине”;
26. Атака с использование словаря;
27. Атака с использование радужной таблицы.

Разработка математической модели



Математическая модель сети



Предлагаемый протокол

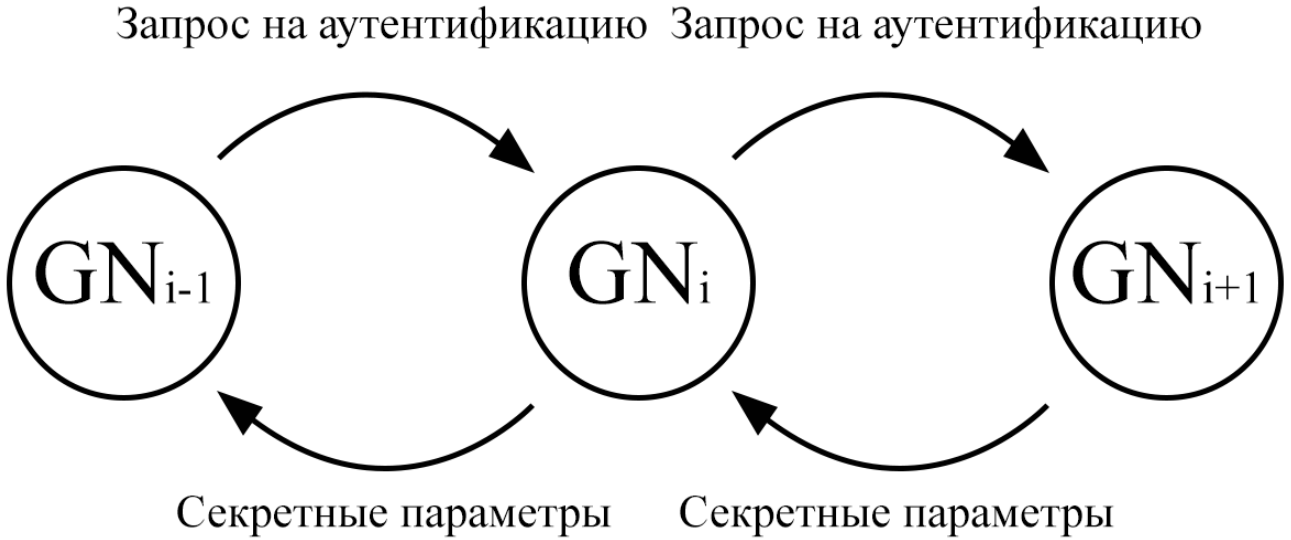
Основные фазы работы протокола:

1. Фаза идентификации;
2. Фаза регистрации;
3. Фаза аутентификации;
4. Фаза генерации группового ключа.

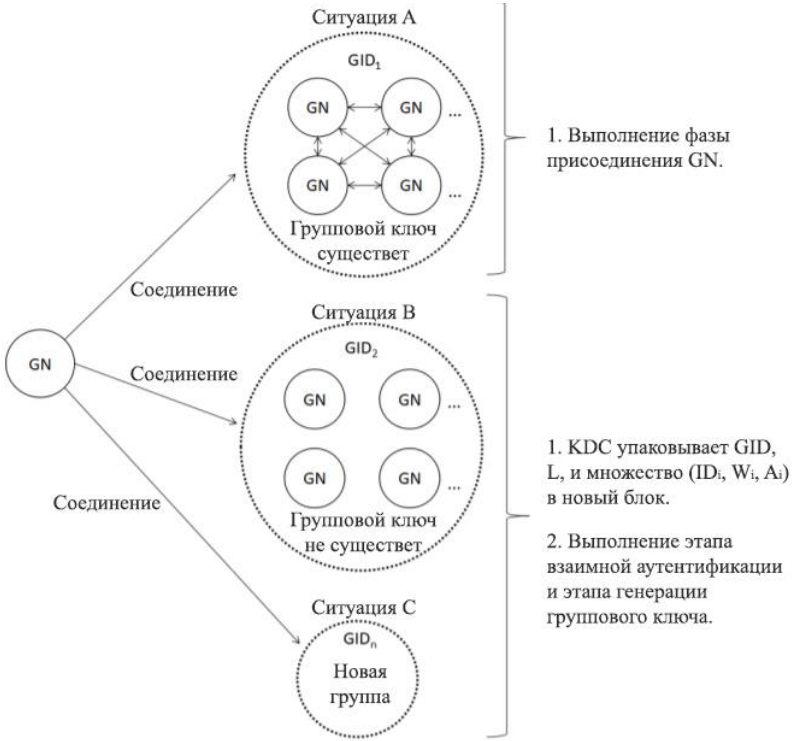
Дополнительные фазы работы протокола:

1. Фаза добавления нового узла к группе;
2. Фаза удаления узла из группы;
3. Процесс обнаружения внутреннего злоумышленника.

Процесс упрощенной аутентификации



Взаимодействие общих узлов



Критические составляющие системы

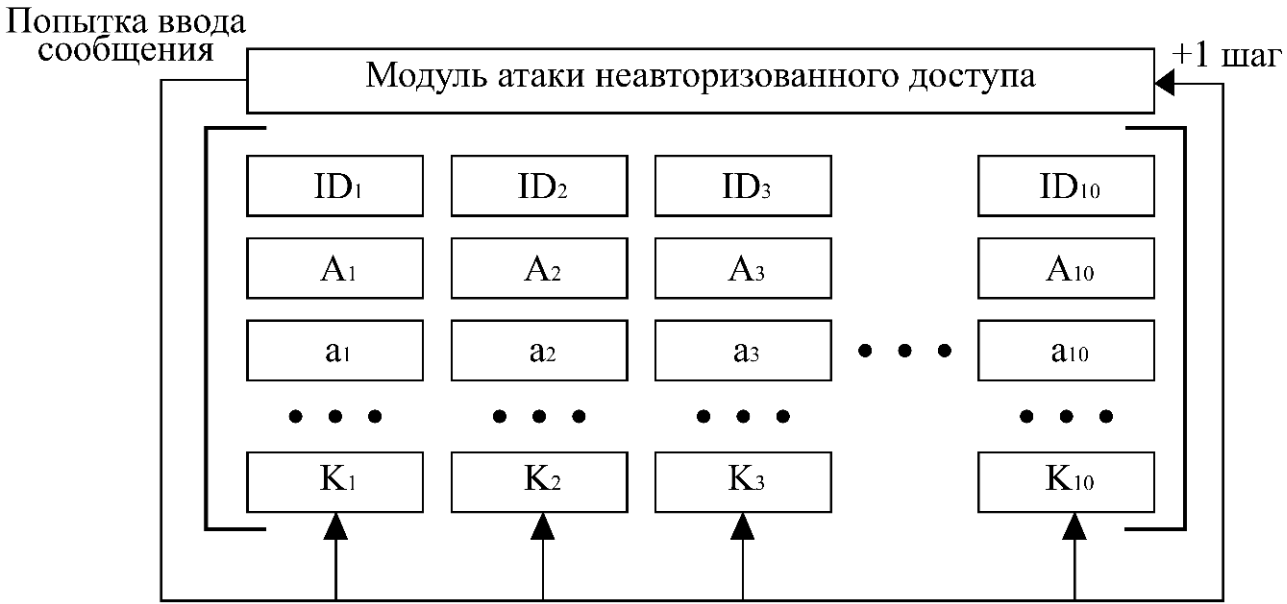
Компоненты подверженные риску

Основные составляющие системы аутентификации подверженные риску:

1. Критические компоненты архитектуры системы;
2. Процессы аутентификации;
3. Сеть блокчейн.

Разработка модификаций системы

Эмуляция информационных атак



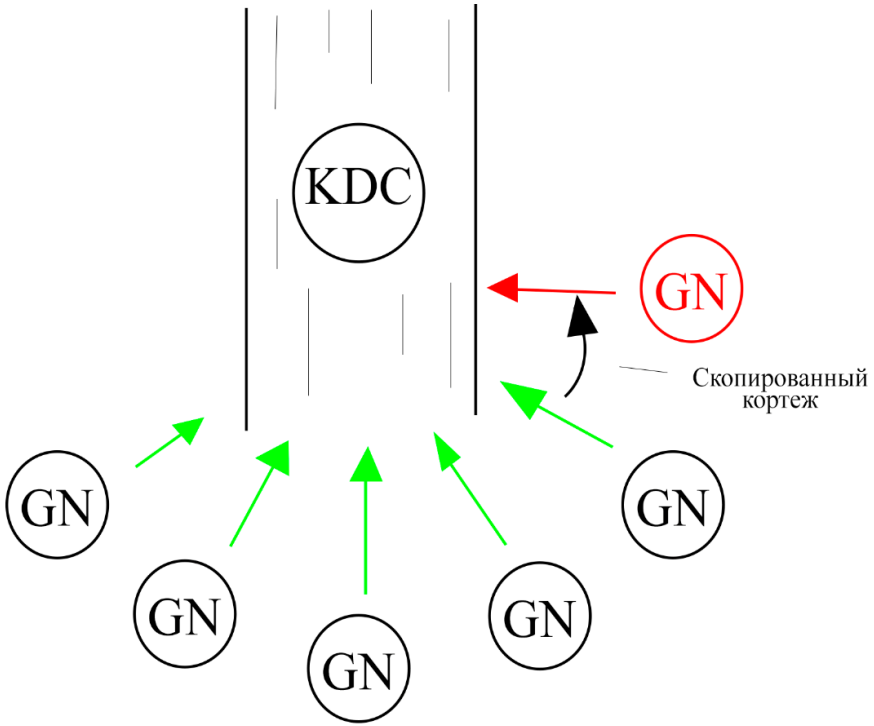
Результаты работы исходной системы

Информационная атака	Вероятность успеха
Атака неавторизированного доступа	99.9%
Атака “Человек по середине”	99.9%
Атака с повтором	99.8%
Атака с использованием словаря	99.7%
Атака с использованием радужной таблицы	99.6%

Внедрение модификаций

Внедренные модификации системы:

1. Ограничение попыток ввода;
2. Групповая идентификация;
3. Введение минимальный размер данных для генерации секретных параметров;
4. Использование более сложного алгоритма хэширования;
5. Добавление дополнительного кортежа данных, пересылаемых в сеть блокчейн

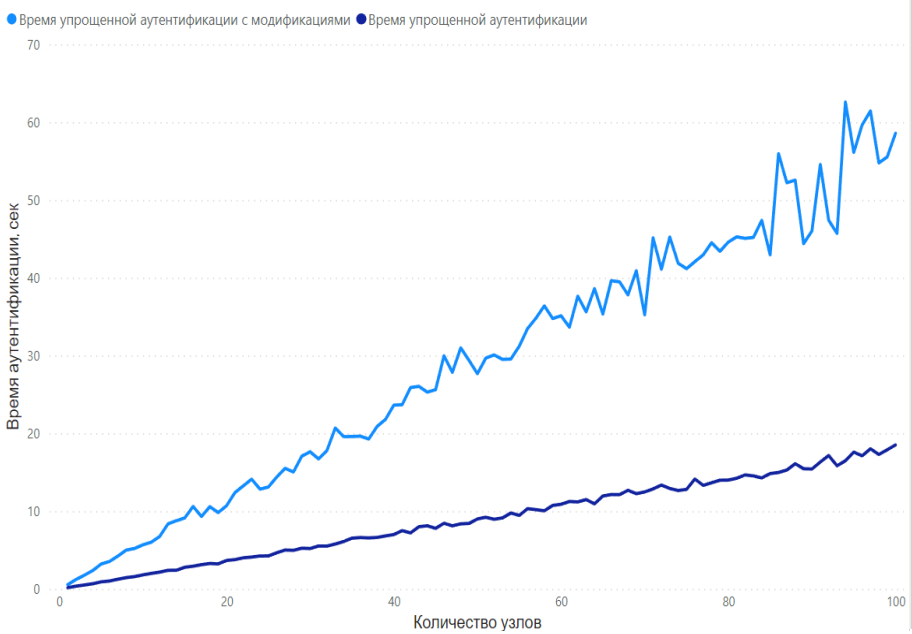


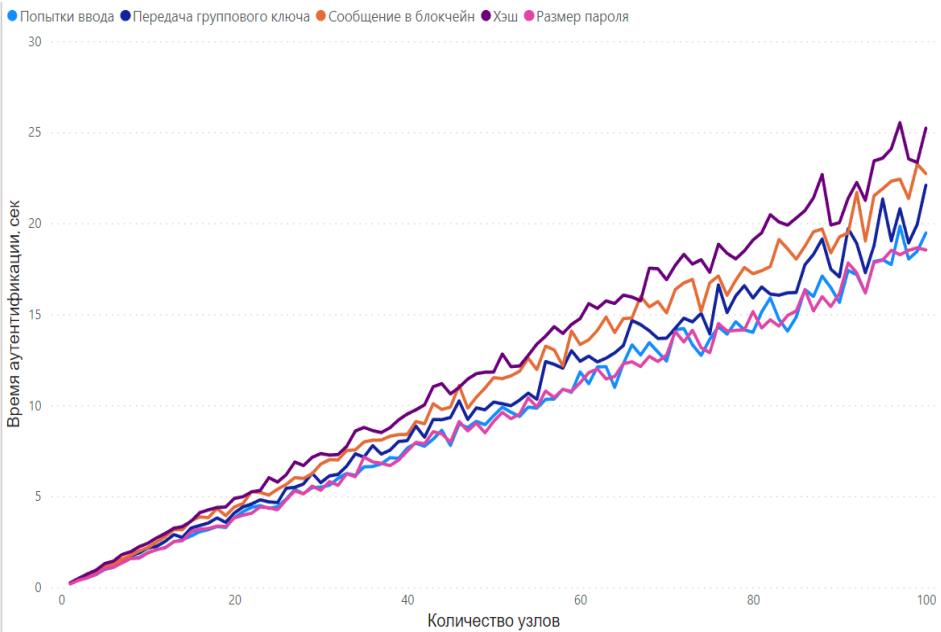
Результаты тестирования модифицированной системы

Результаты работы модифицированной системы

Информационная атака	Вероятность успеха
Атака неавторизированного доступа	0.1%
Атака “Человек по середине”	0.1%
Атака с повтором	0.1%
Атака с использованием словаря	0.2%
Атака с использованием радужной таблицы	0.3%

Влияние модификаций на время работы системы





ЗАКЛЮЧЕНИЕ

СПАСИБО ЗА ВНИМАНИЕ!