Обеспечение конфиденциальности результатов анализа данных в социальных сетях

Докладчик: Файрузов Рустам Алмасович
студент каф. СИБ КНИТУ-КАИ
Научный руководитель: Аникин Игорь Вячеславович
доцент каф. СИБ КНИТУ-КАИ

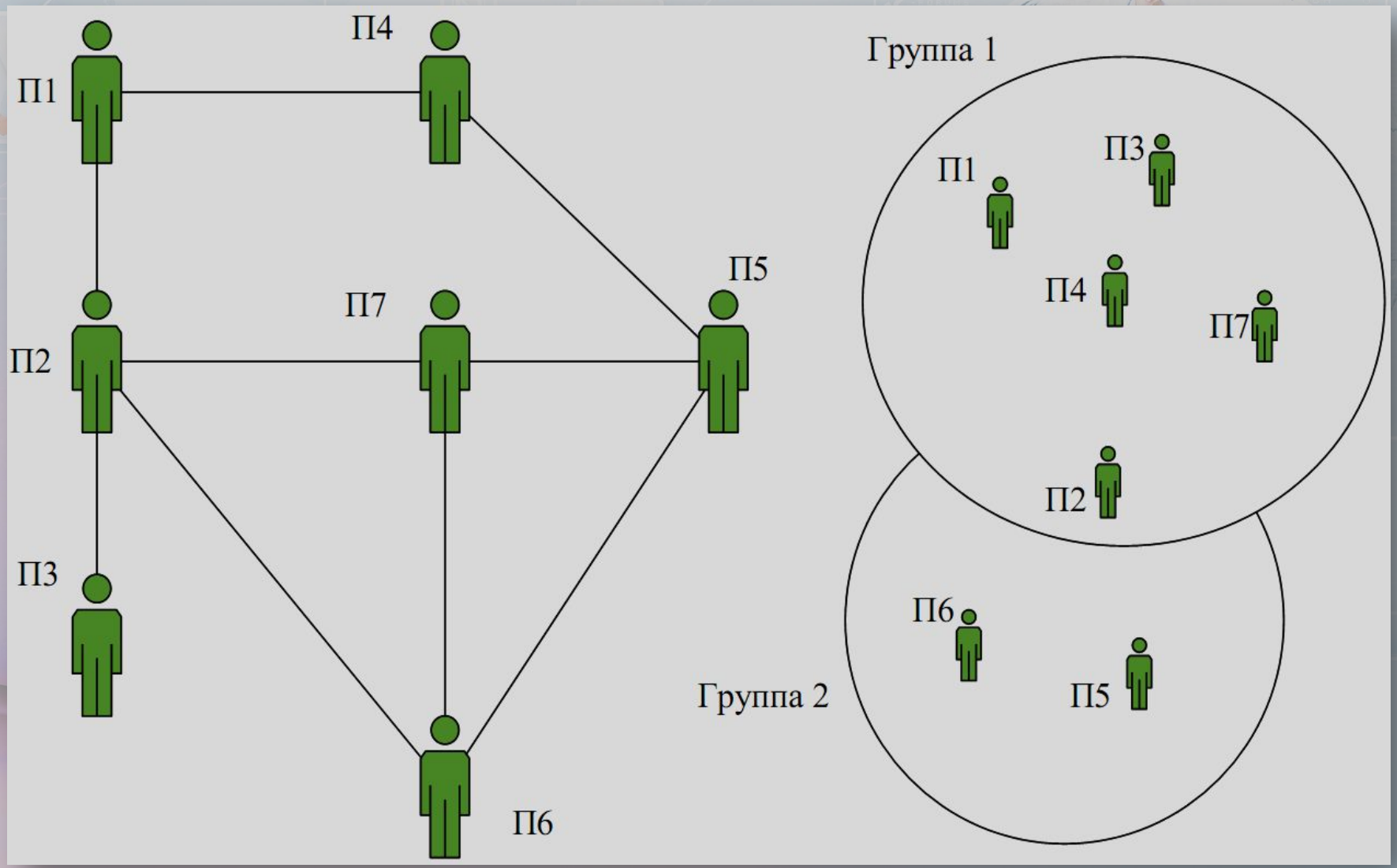
Цели и задачи выпускной квалификационной работы

Цель: повышение уровня защищенности результатов анализа данных, публикуемых в социальных сетях.

Задачи:

- провести анализ социальных сетей и методов обеспечения конфиденциальности пользователя;
- проанализировать методы получения, построения и визуализации графа связей пользователей социальной сети;
- создать метод для обеспечения конфиденциальности результатов анализа данных социальных сетей;
- разработать и протестировать работу программного комплекса обеспечения конфиденциальности результатов анализа данных социальных сетей.

Системно-структурное представление социальных сетей



Виды утечки конфиденциальной информации в социальных сетях

- Разглашение идентичности пользователя;
- Разглашение значений атрибутов профиля;
- Разглашение социальных связей сети.

Методы защиты конфиденциальности в социальных сетях

- *K-анонимность;*
- *L-разнообразие;*
- *T-близости;*
- *ξ-дифференциальная конфиденциальность.*

Методы для сбора данных из различных социальных сетей

- Услуги специализированных компаний и программных продуктов.
- Программные интерфейсы (API-функции).
- Ручной разбор веб-страницы.

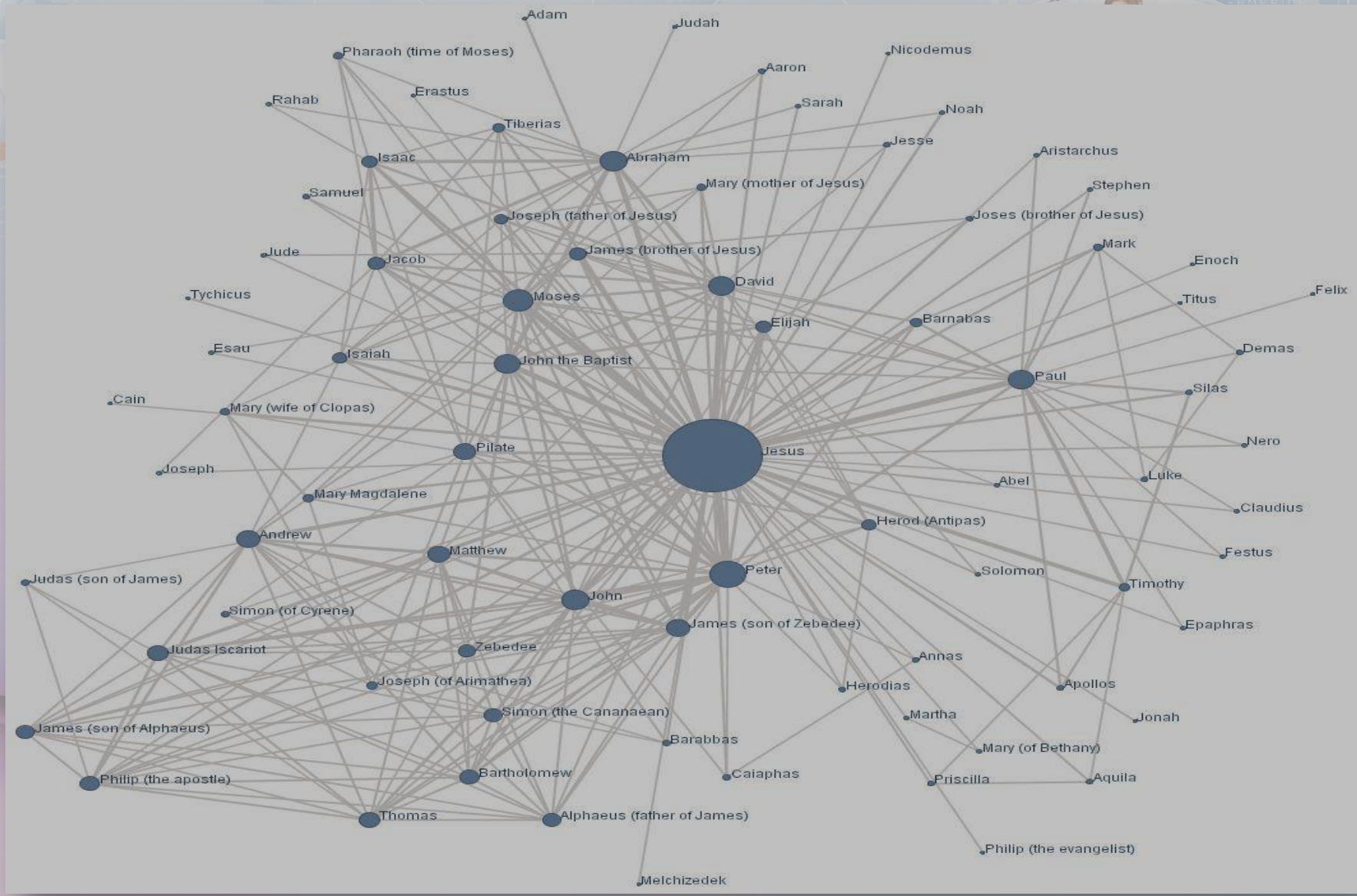
Основная API-функция данной работы

friends.get- Возвращает список идентификаторов друзей пользователя.

Запрос:

string resp = GET_http ("https://api.vk.com/ /method/" + method + "?" + paramss + "=" + user_id + "&access_token=" + token);

Пример визуализации графа связей пользователей социальной сети



Криптография и традиционные симметричные криптосистемы

Функциональная схема симметричной криптосистемы

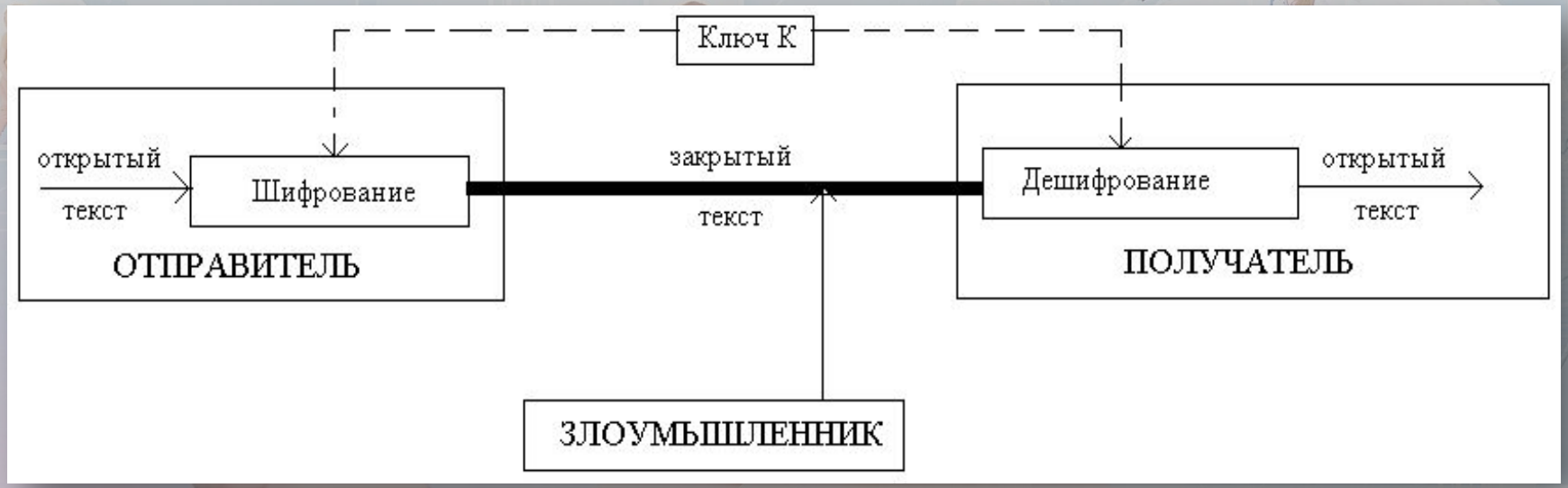
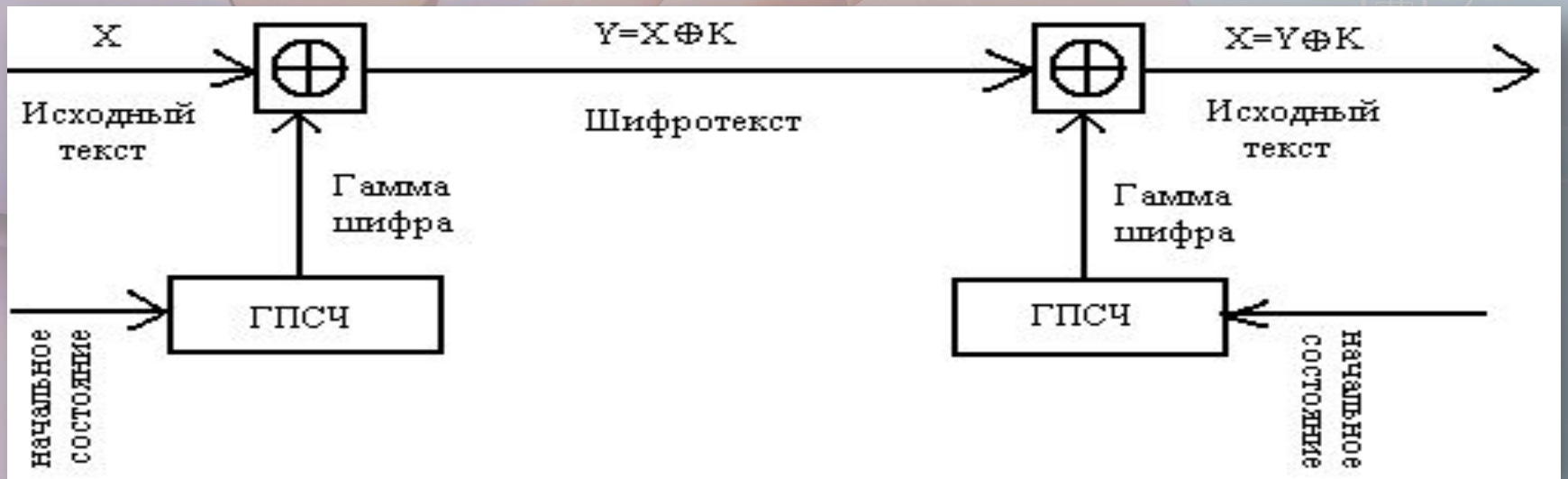


Схема шифрования методом гаммирования

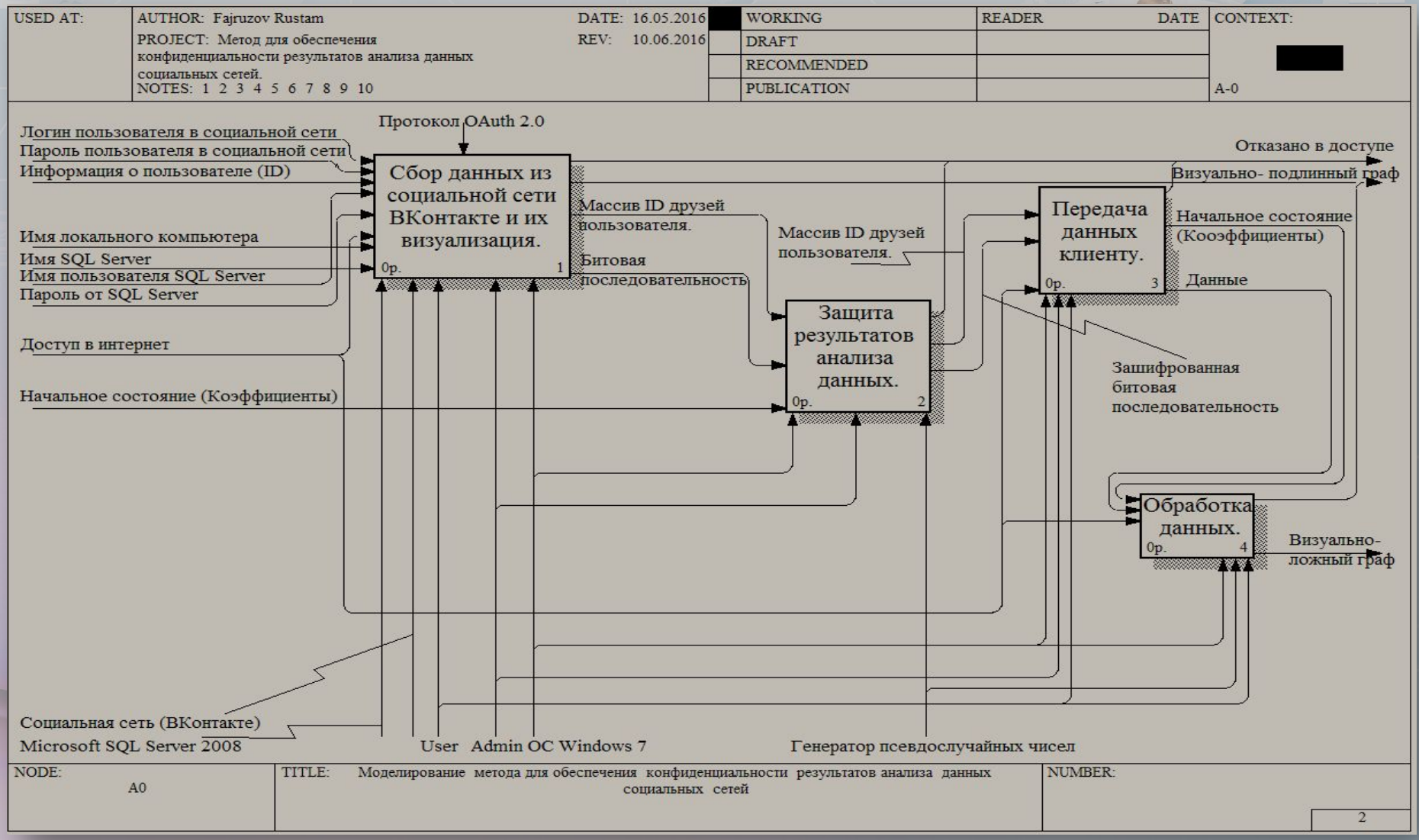


Линейный конгруэнтный метод

$$Y_i=(a*Y_{i-1}+b) \bmod m$$

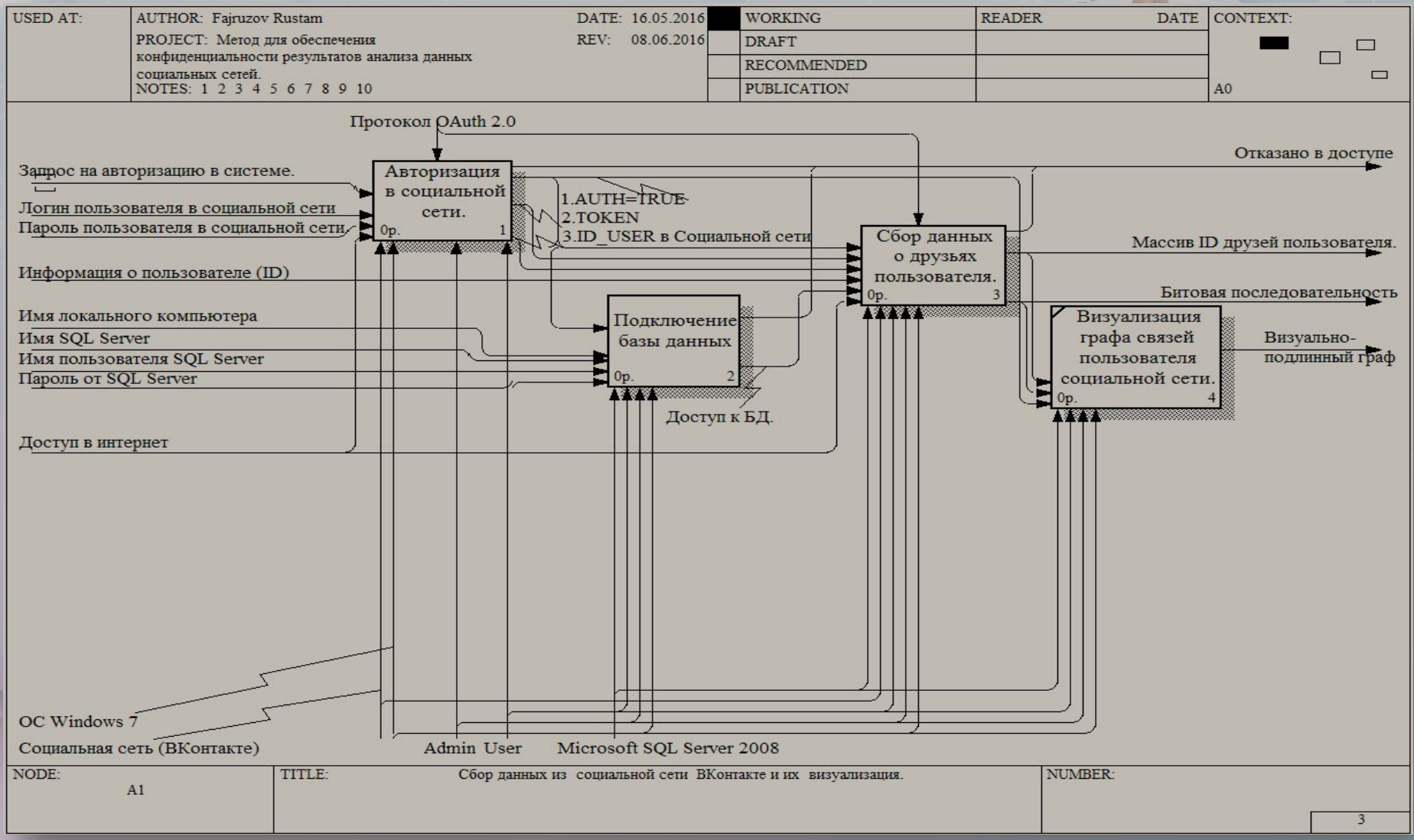
Переполняется при	a	b	m
2^{20}	106	1283	6075
2^{21}	211	1663	7875
2^{22}	421	1663	7875
2^{23}	430	2531	11979
2^{23}	936	1399	6655
2^{23}	1366	1283	6075
2^{24}	171	11213	53125
2^{24}	859	2531	11979
2^{24}	419	6173	29282
2^{24}	967	3041	14406
2^{25}	141	28411	134456
2^{25}	625	6571	31104

Метод, основанный на гаммировании, для обеспечения конфиденциальности результатов анализа данных социальных сетей.



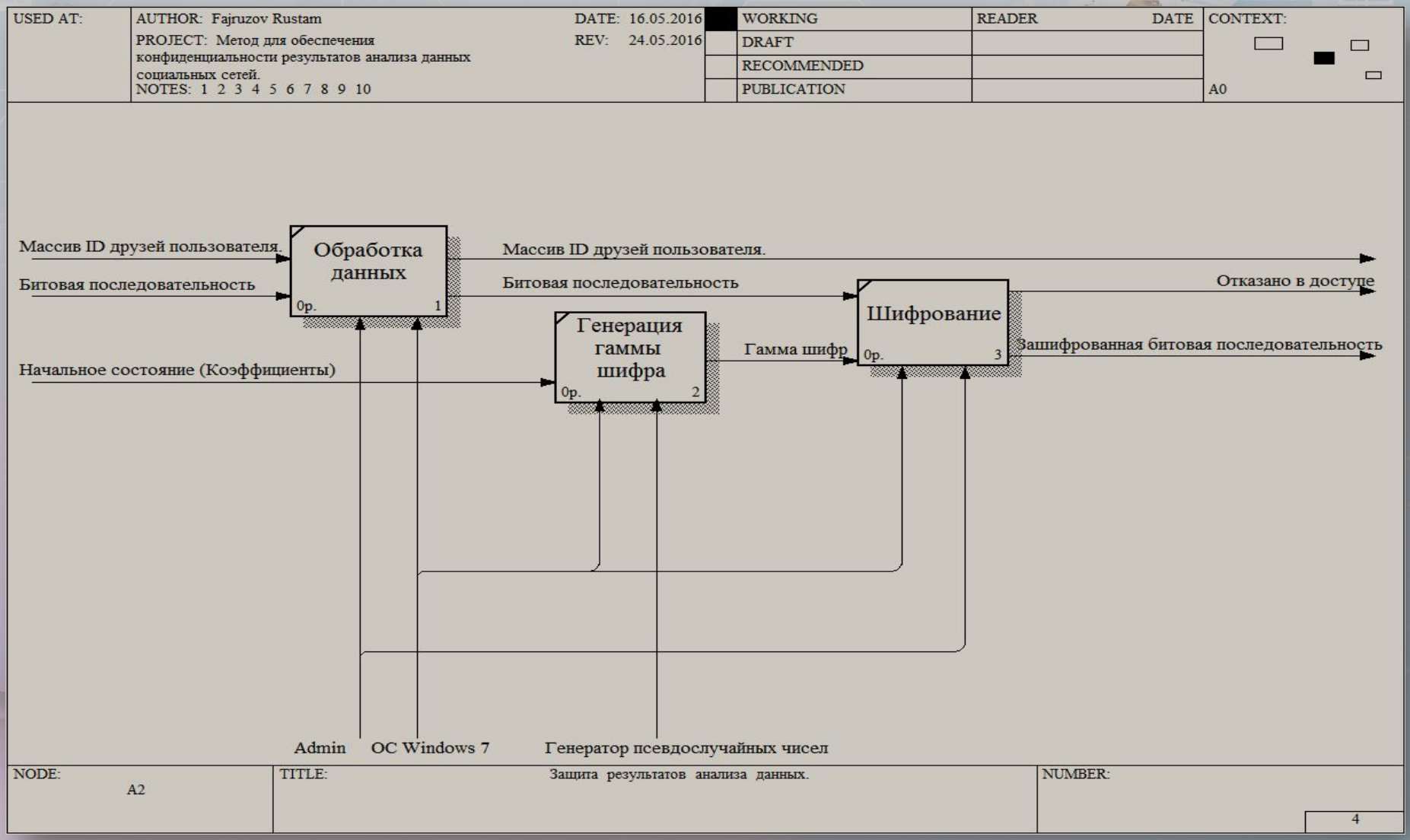
Функциональная схема ПКОКРАД

Метод, основанный на гаммировании, для обеспечения конфиденциальности результатов анализа данных социальных сетей.



Декомпозиция блока A1 “Сбор данных из соц.сети Вконтакте и их визуализация”

Метод, основанный на гаммировании, для обеспечения конфиденциальности результатов анализа данных социальных сетей.

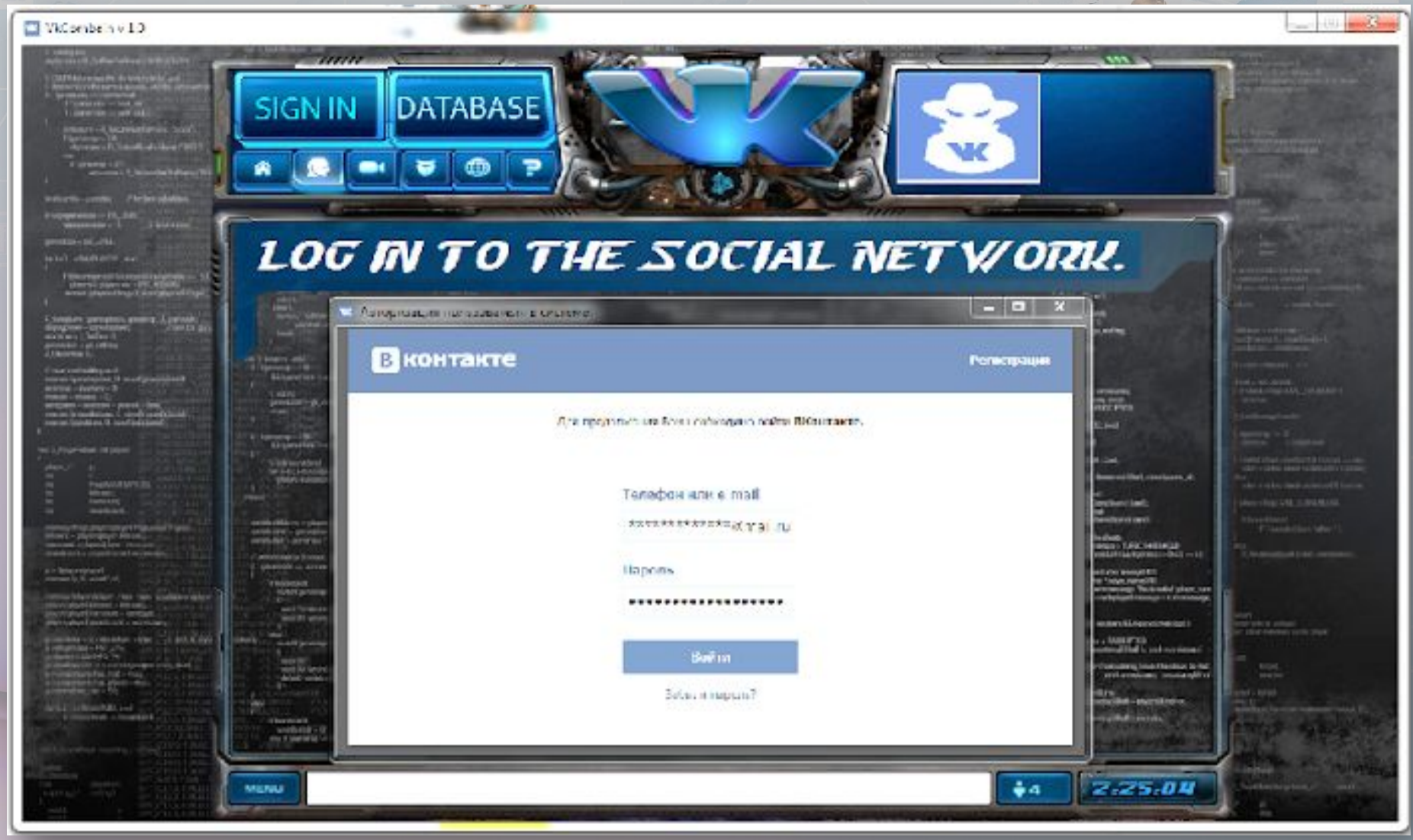


Декомпозиция блока А2 “Защита результатов анализа данных”

Работа на программном комплексе ПКОКРАД

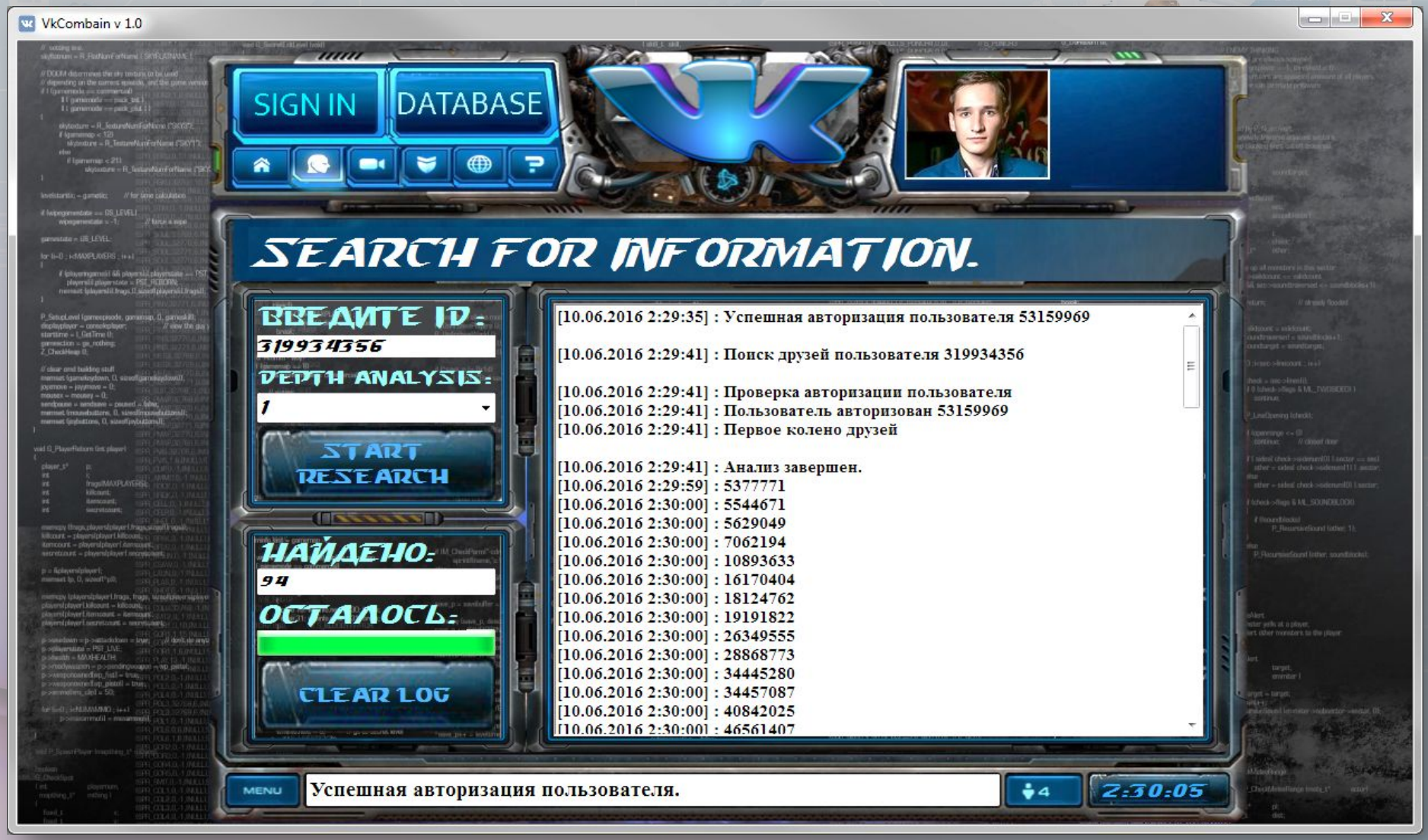
Внешний интерфейс программного комплекса

Работа на программном комплексе ПКОКРАД



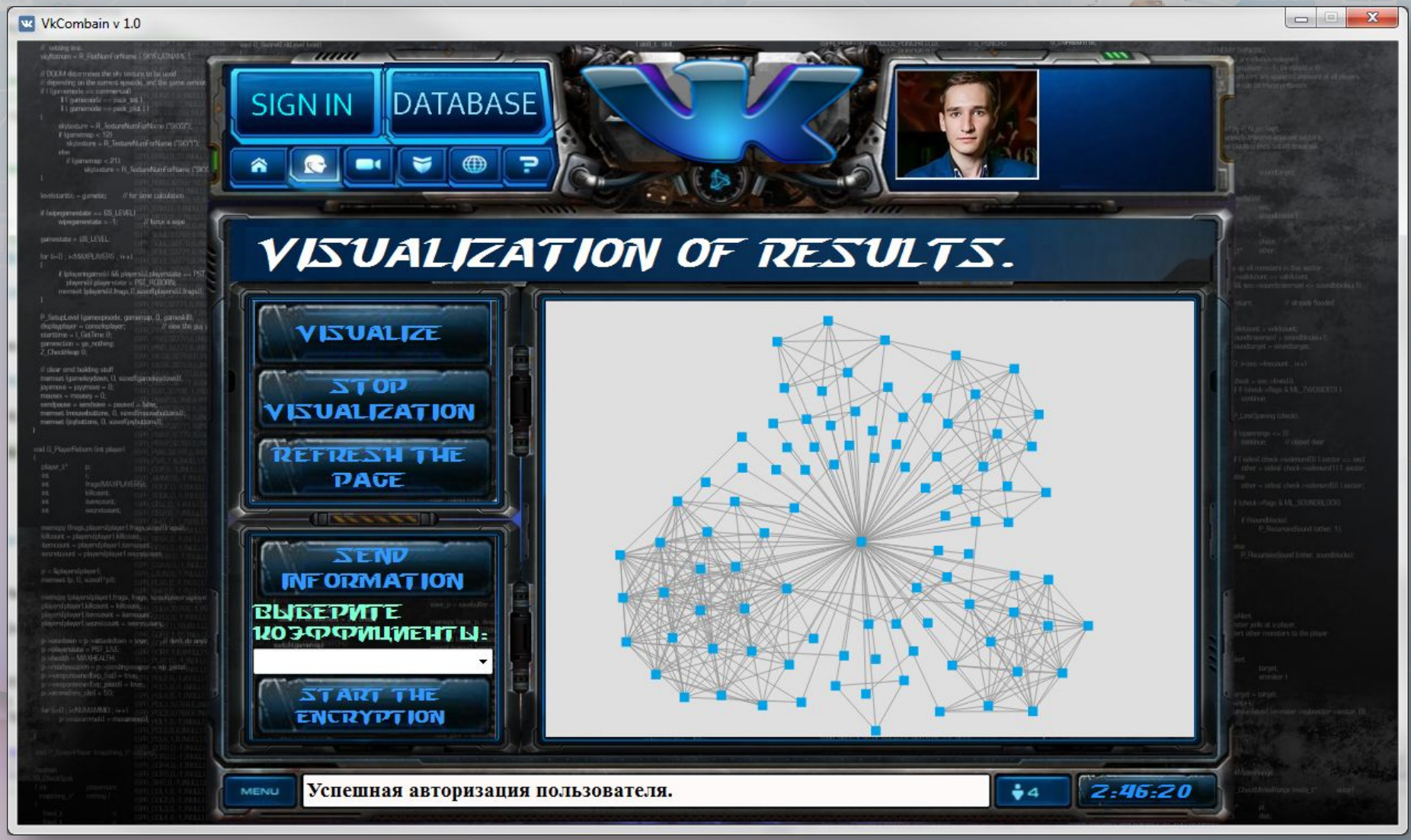
Окно авторизации пользователя

Работа на программном комплексе ПКОКРАД



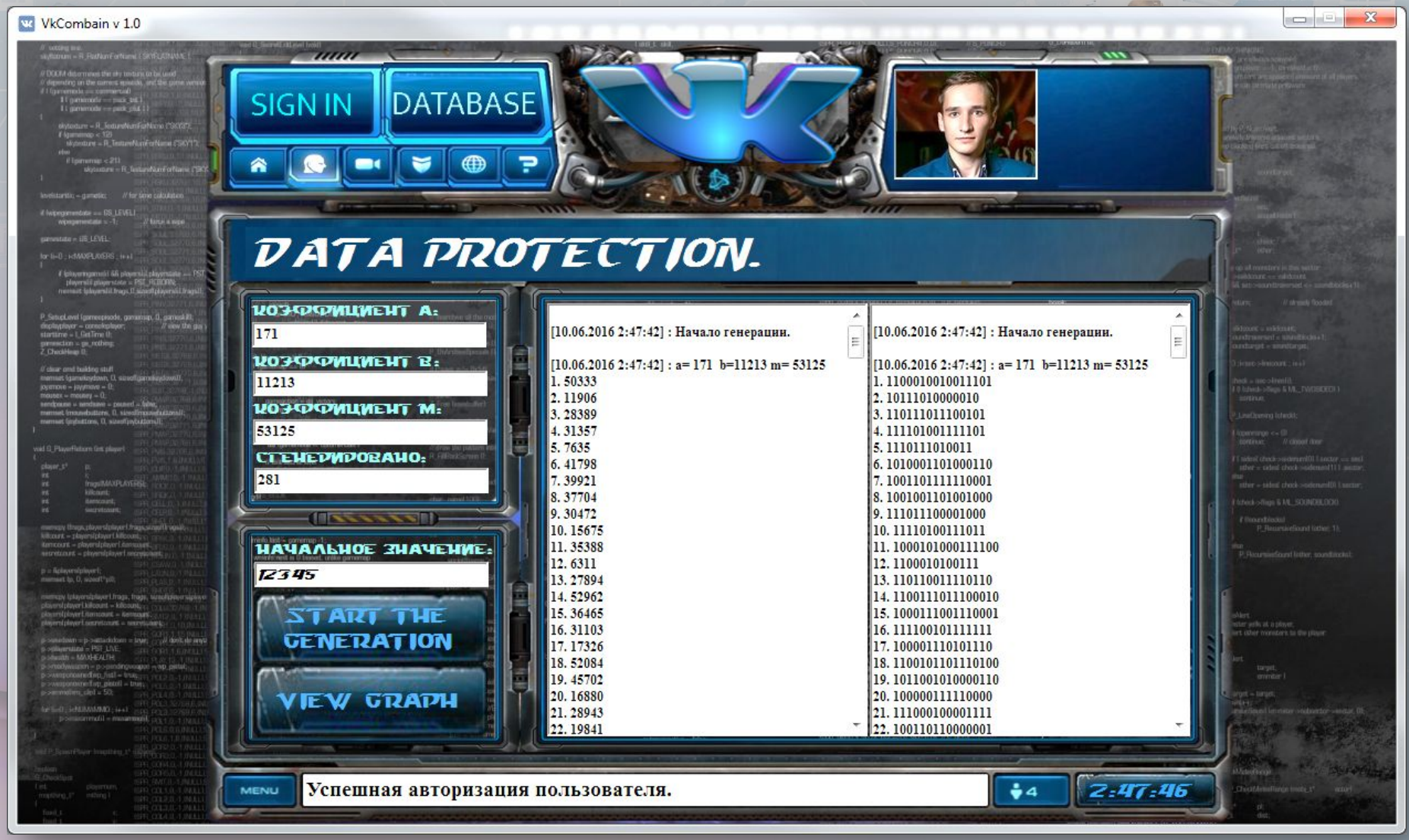
Сбор данных из социальной сети

Работа на программном комплексе ПКОКРАД



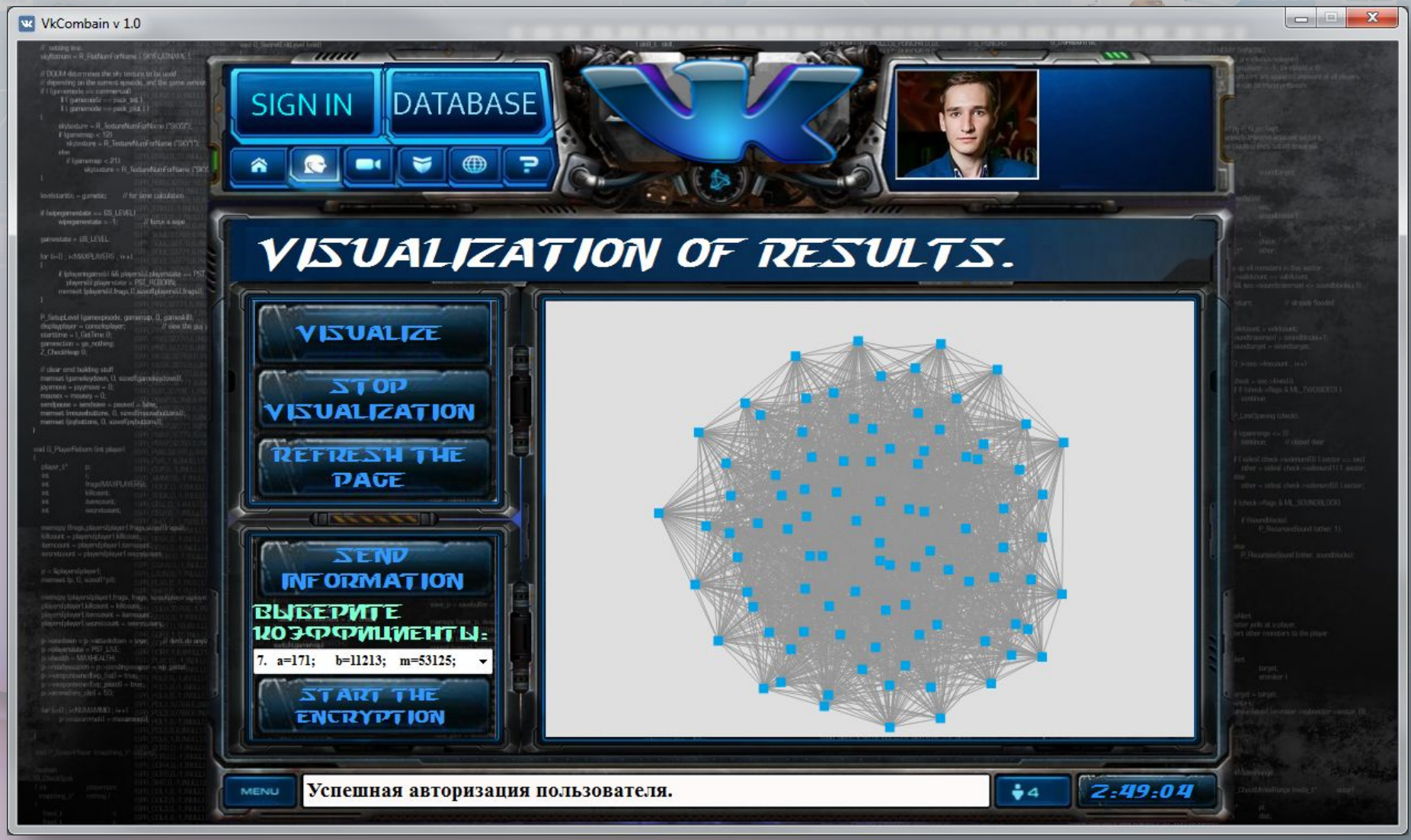
Визуализация графа связей пользователей социальной сети

Работа на программном комплексе ПКОКРАД



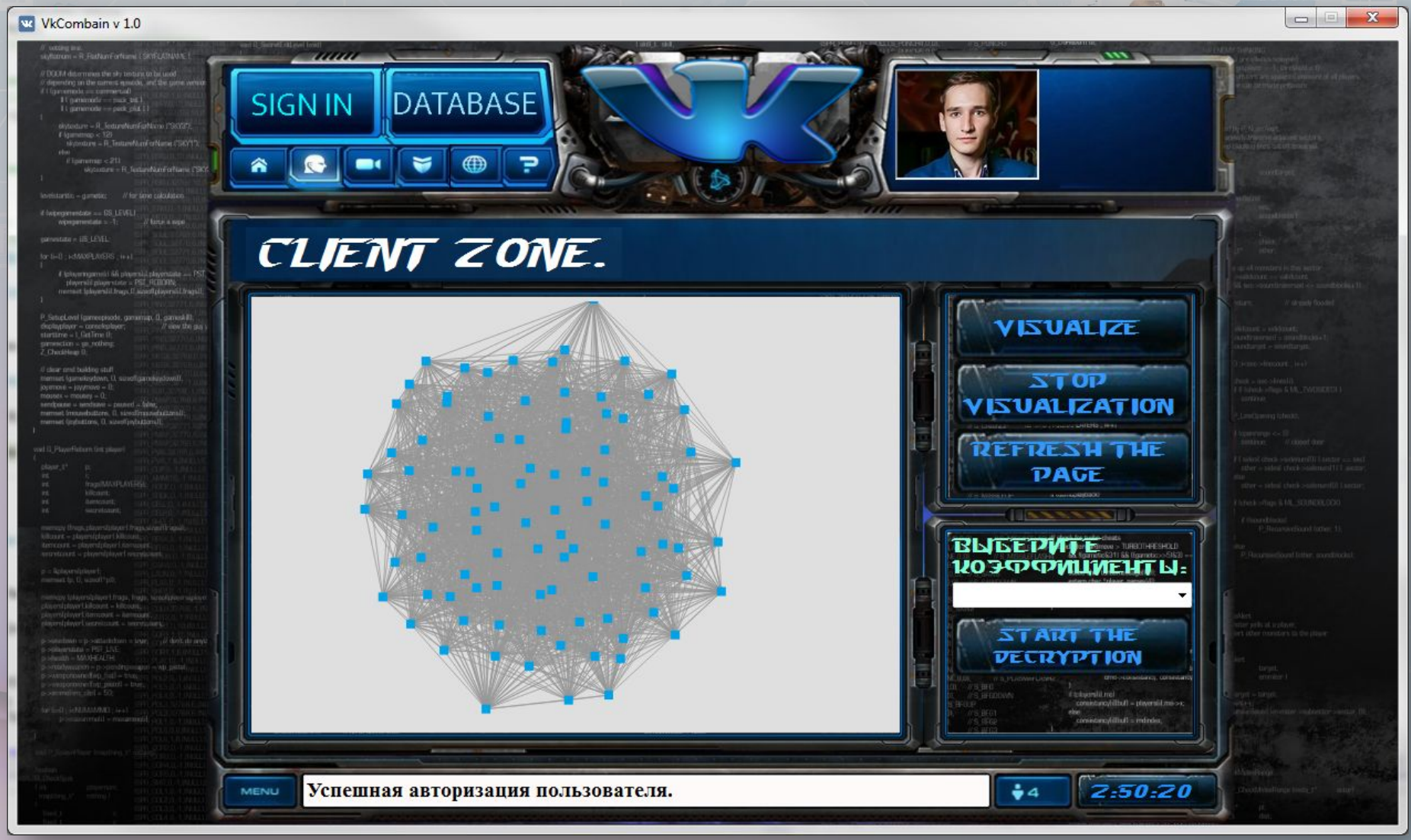
Модуль генерации гаммы шифра

Работа на программном комплексе ПКОКРАД



Визуализация зашифрованного графа связей пользователей социальной сети

Работа на программном комплексе ПКОКРАД

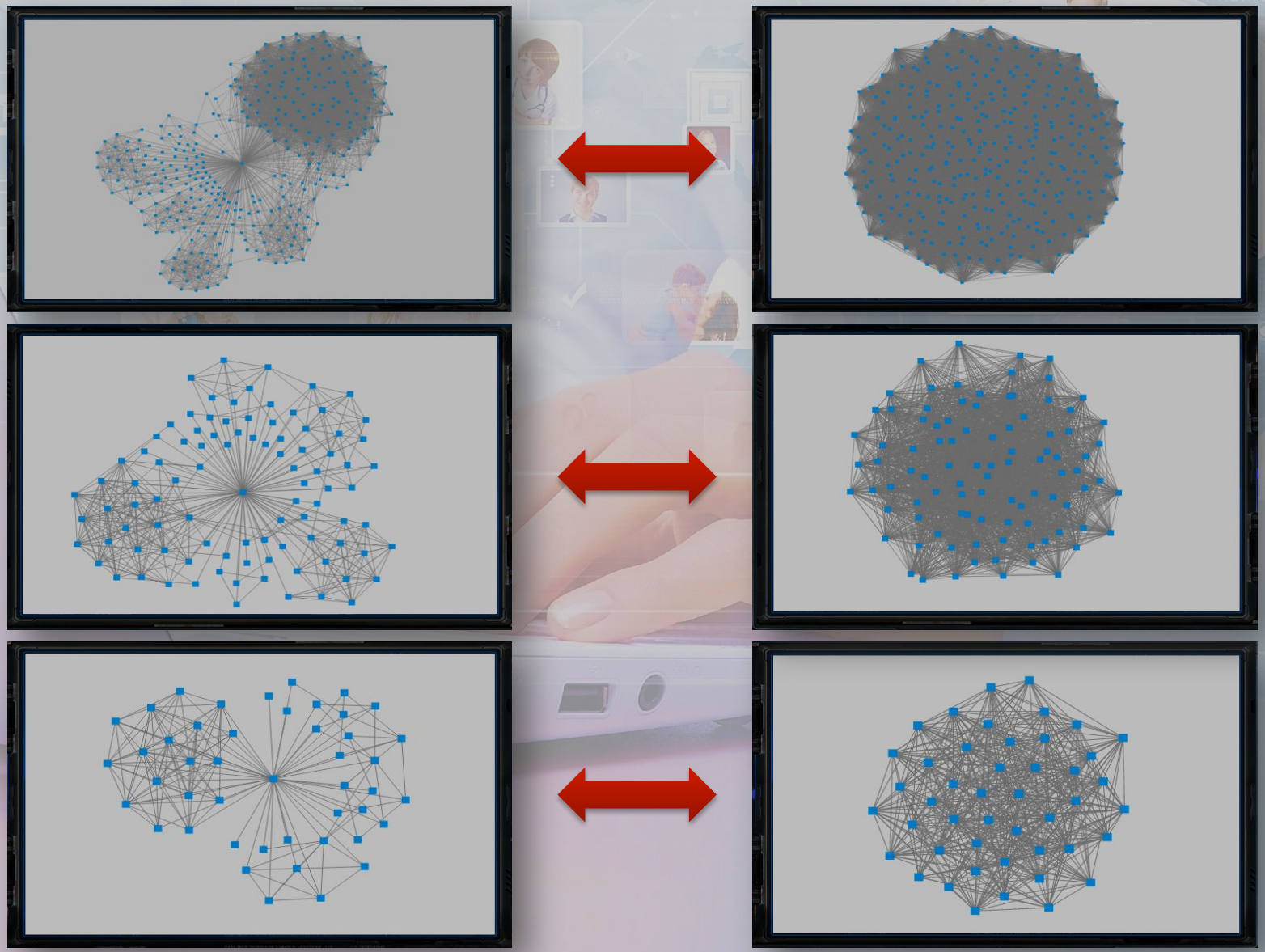


Визуализация полученных данных клиентом

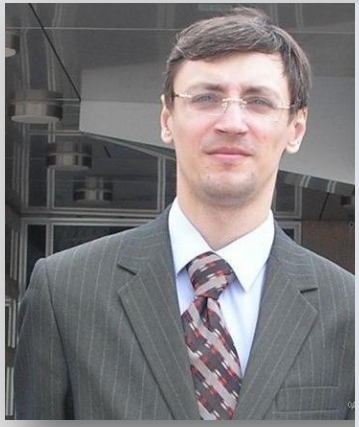
Работа на программном комплексе ПКОКРАД

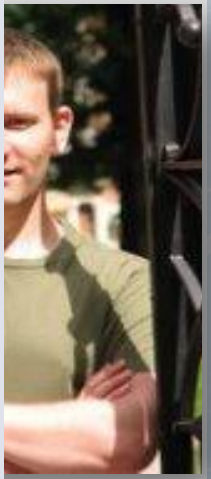
Визуализация дешифрованного графа связей пользователей социальной сети

Результаты работы программного комплекса ПКОКРАД



Улучшение программного комплекса ПКОКРАД

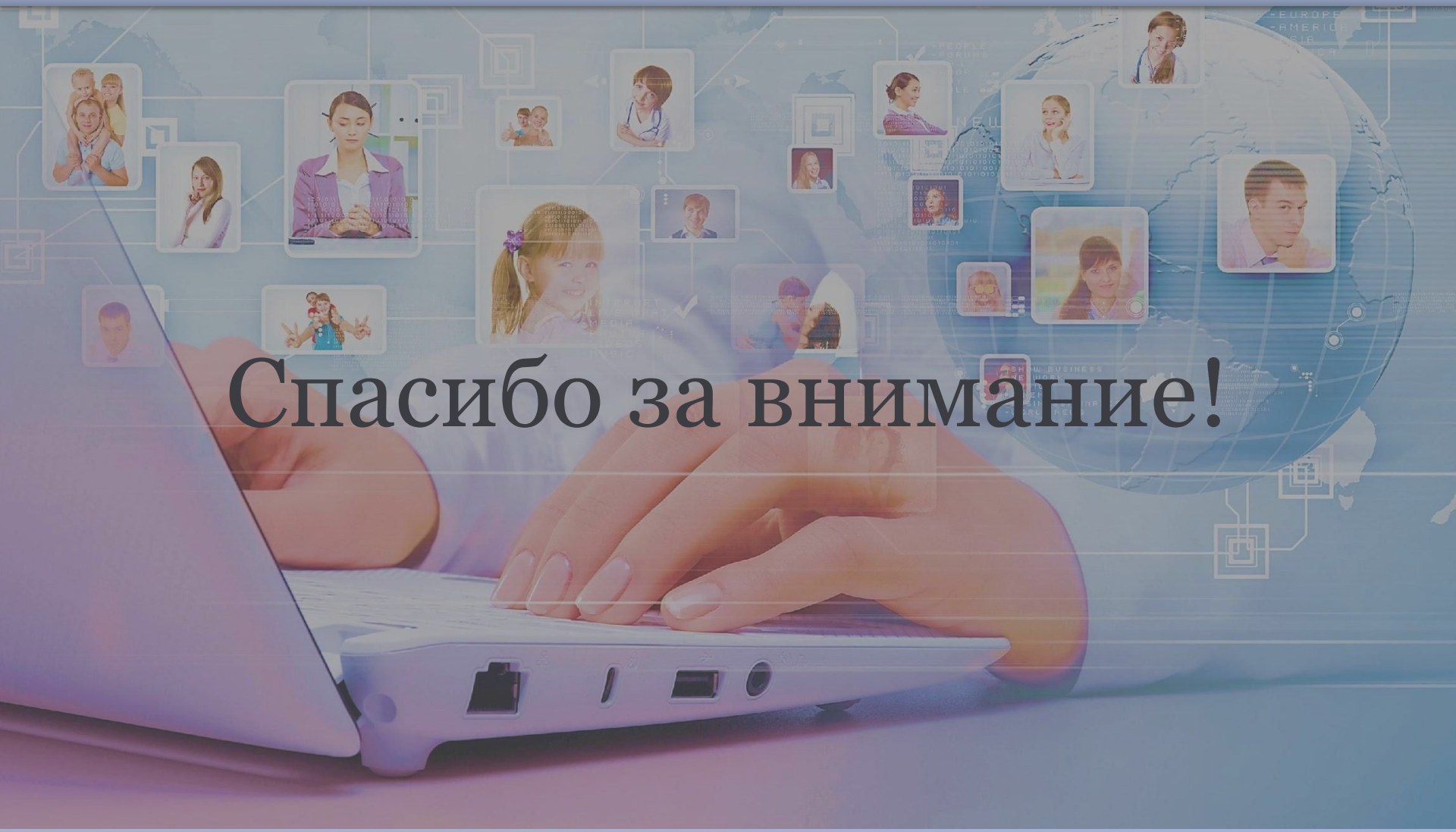




Заключение

Решенные задачи:

- анализа социальных сетей и методов обеспечения конфиденциальности пользователя;
- анализа методов получения , построения и визуализации результатов анализа данных социальных сетей (социальный граф) ;
- разработка метода, основанного на гаммировании, для обеспечения конфиденциальности результатов анализа данных социальных сетей;
- разработка и тестирование программного комплекса.



Спасибо за внимание!

Обеспечение конфиденциальности результатов анализа данных в социальных сетях

Докладчик: Файрузов Рустам Алмасович
студент каф. СИБ КНИТУ-КАИ
Научный руководитель: Аникин Игорь Вячеславович
доцент каф. СИБ КНИТУ-КАИ