



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

14.06.2016



Цели и задачи выпускной квалификационной работы

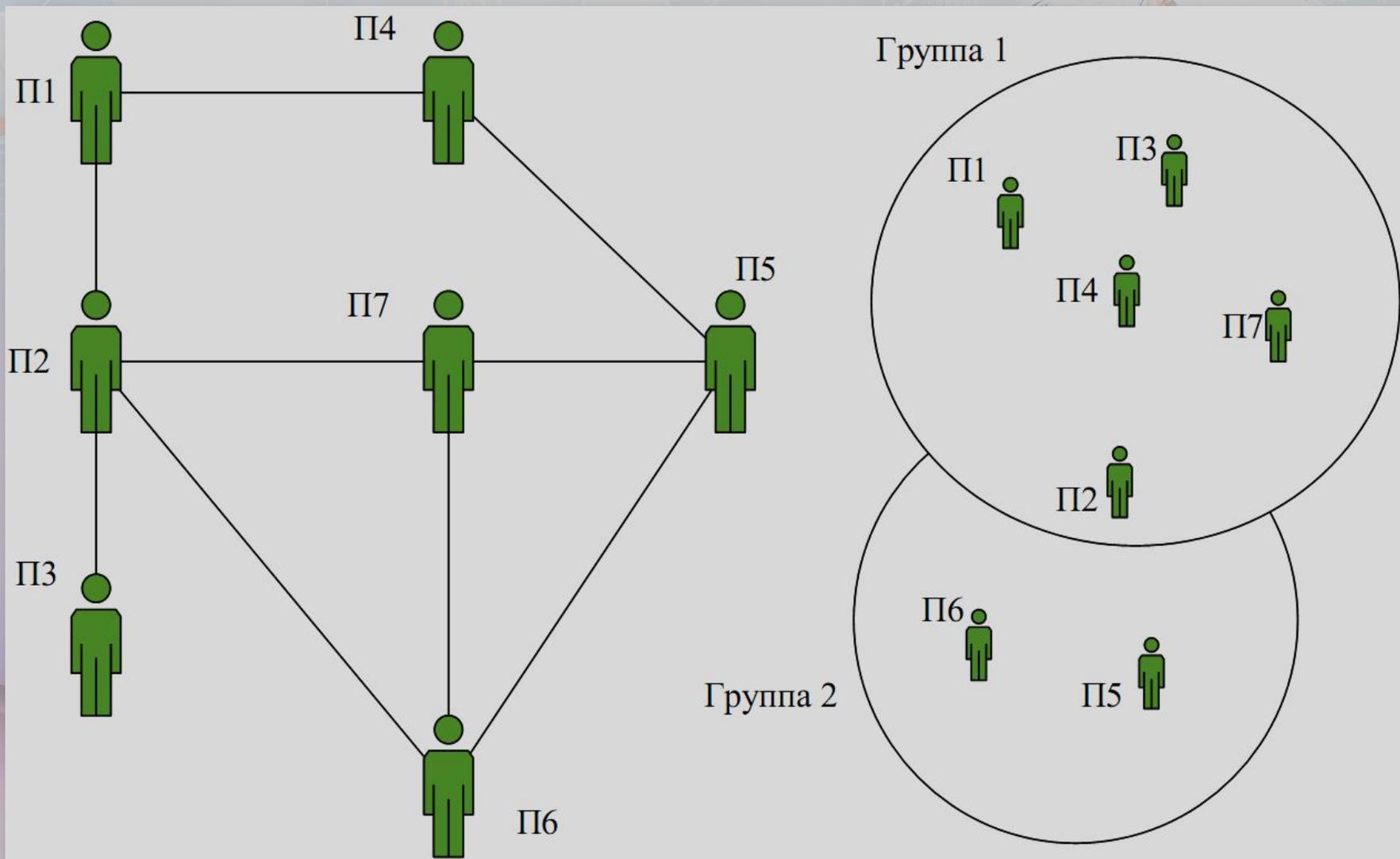
Цель: повышение уровня защищенности результатов анализа данных, публикуемых в социальных сетях.

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

- *К-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);
```




Криптография и традиционные симметричные криптосистемы

Функциональная схема симметричной криптосистемы

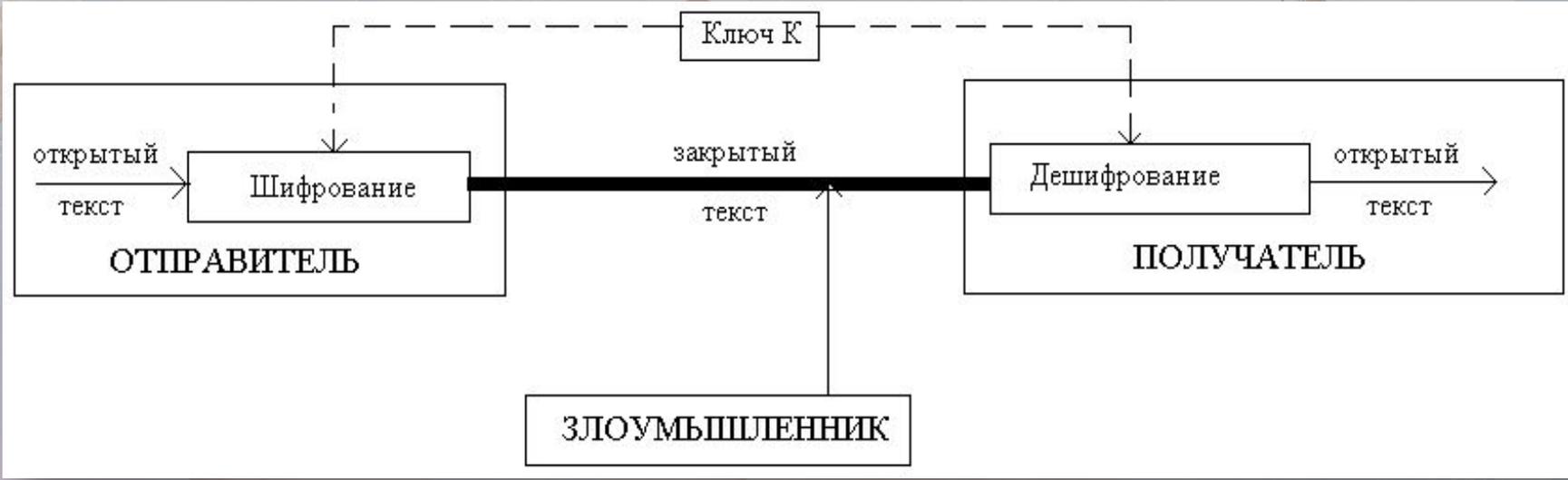
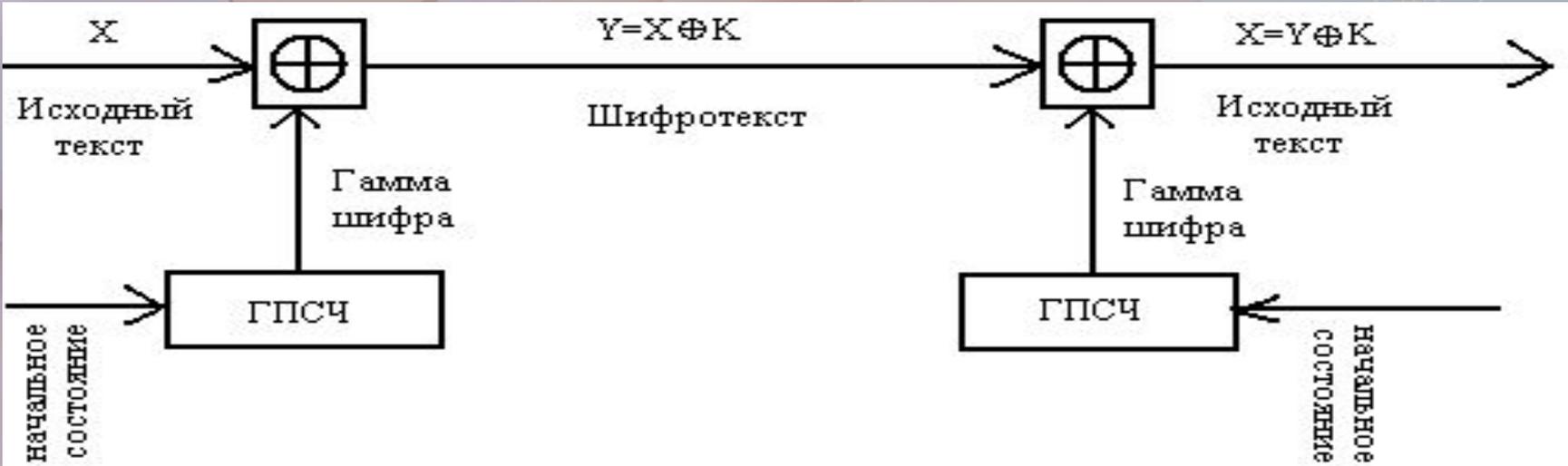


Схема шифрования методом гаммирования





Линейный конгруэнтный метод

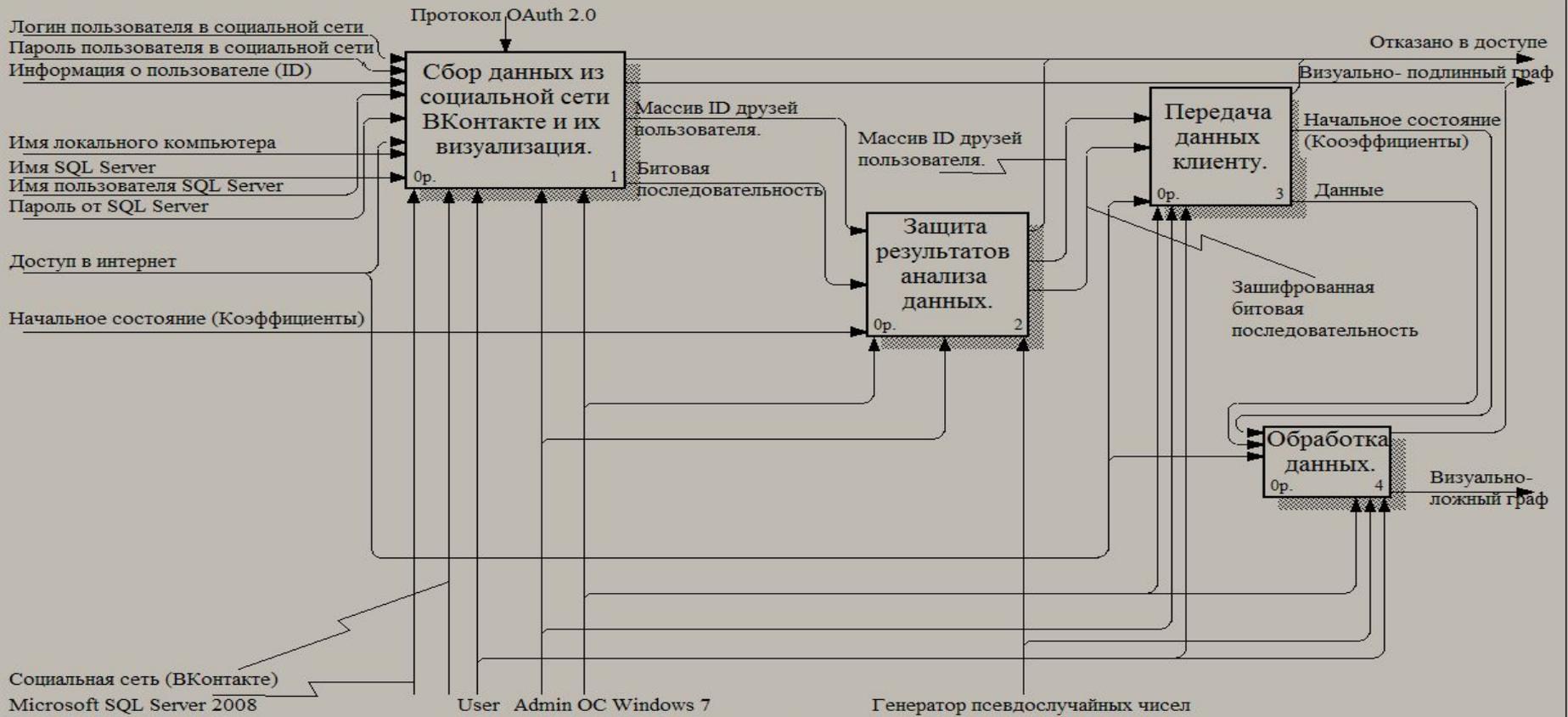
$$Y_i = (a * Y_{i-1} + b) \bmod m$$

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.

USED AT:	AUTHOR: Fajruzov Rustam	DATE: 16.05.2016	WORKING	READER	DATE	CONTEXT:
	PROJECT: Метод для обеспечения конфиденциальности результатов анализа данных социальных сетей.	REV: 10.06.2016	DRAFT			
	NOTES: 1 2 3 4 5 6 7 8 9 10		RECOMMENDED			
			PUBLICATION			A-0

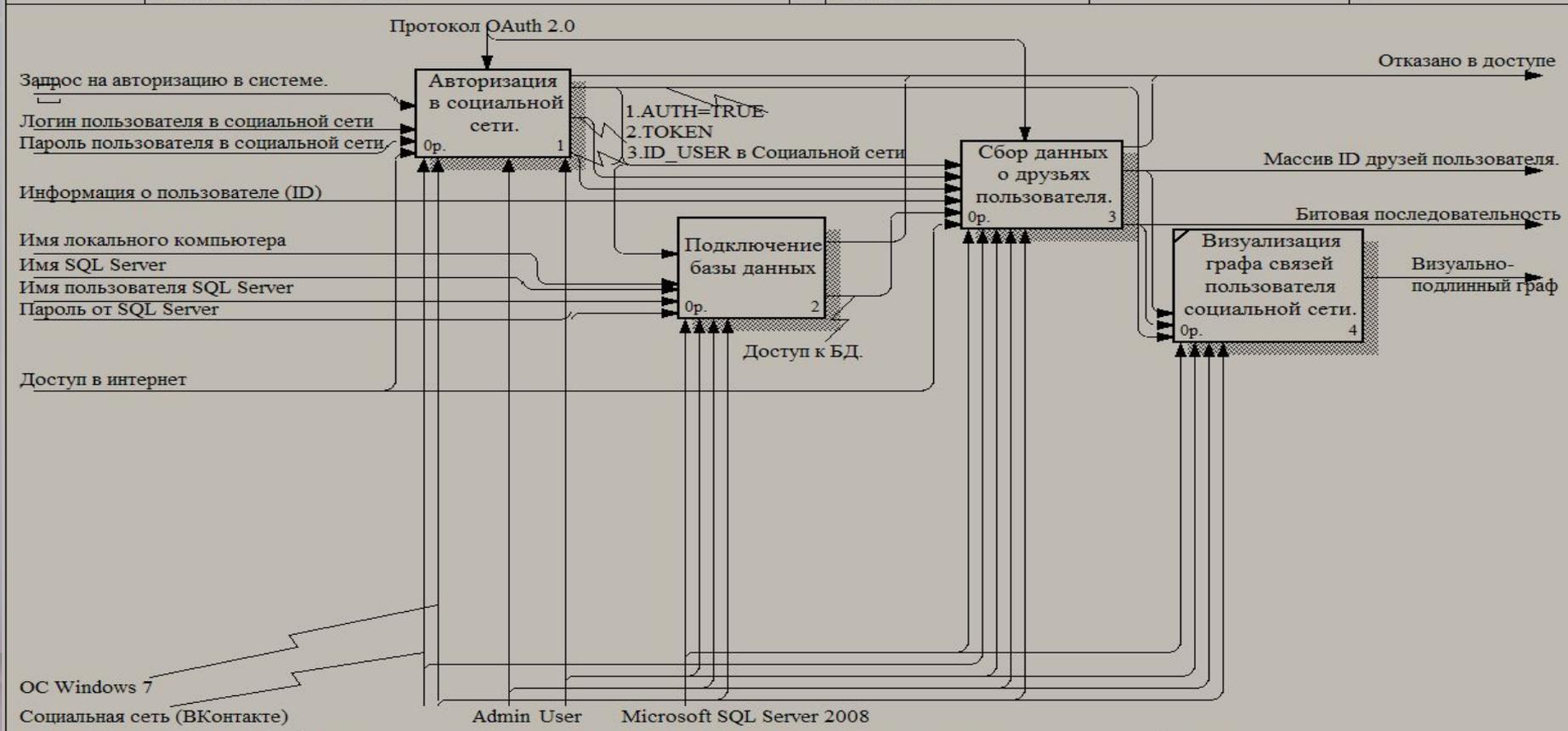


NODE: A0	TITLE: Моделирование метода для обеспечения конфиденциальности результатов анализа данных социальных сетей	NUMBER:
----------	--	---------



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

USED AT:	AUTHOR: Fajruzov Rustam	DATE: 16.05.2016	WORKING	READER	DATE	CONTEXT:
	PROJECT: Метод для обеспечения конфиденциальности результатов анализа данных социальных сетей.	REV: 08.06.2016	DRAFT			<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	NOTES: 1 2 3 4 5 6 7 8 9 10		RECOMMENDED			<input type="checkbox"/> <input type="checkbox"/>
			PUBLICATION			A0



NODE:	A1	TITLE:	Сбор данных из социальной сети ВКонтакте и их визуализация.	NUMBER:	3
-------	----	--------	---	---------	---

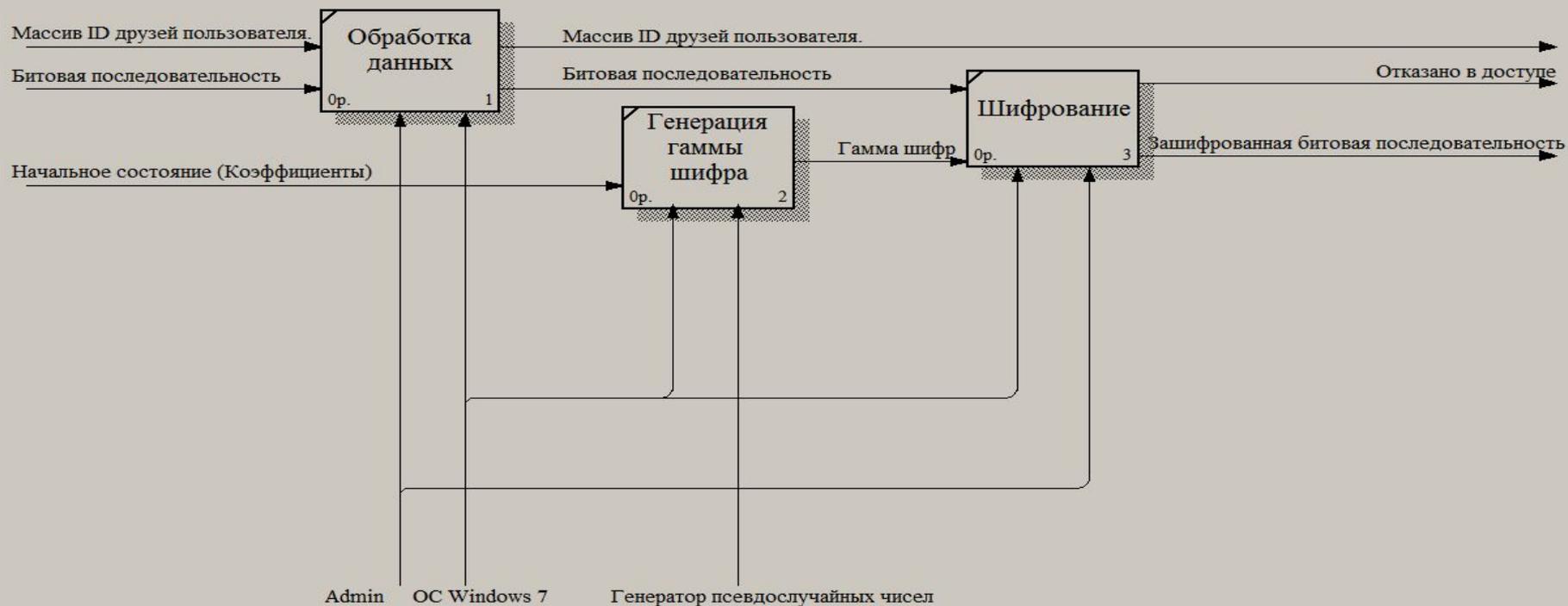
Декомпозиция блока А1 “Сбор данных из соц.сети Вконтакте и их визуализация”



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

USED AT:	AUTHOR: Fajruzov Rustam	DATE: 16.05.2016	WORKING	READER	DATE	CONTEXT:
	PROJECT: Метод для обеспечения конфиденциальности результатов анализа данных социальных сетей.	REV: 24.05.2016	DRAFT			<input type="checkbox"/>
	NOTES: 1 2 3 4 5 6 7 8 9 10		RECOMMENDED			<input checked="" type="checkbox"/>
			PUBLICATION			<input type="checkbox"/>

A0



NODE: A2	TITLE: Защита результатов анализа данных.	NUMBER:
----------	---	---------

4

Декомпозиция блока A2 “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

VkCombin v 1.0

SIGN IN DATABASE

SEARCH FOR INFORMATION.

ВВЕДИТЕ ID:
319934356

DEPTH ANALYSIS:
1

START RESEARCH

НАЙДЕНО:
94

ОСТАЛОСЬ:
[Progress bar]

CLEAR LOG

Успешная авторизация пользователя.

4 2:30:05

Log entries:

- [10.06.2016 2:29:35] : Успешная авторизация пользователя 53159969
- [10.06.2016 2:29:41] : Поиск друзей пользователя 319934356
- [10.06.2016 2:29:41] : Проверка авторизации пользователя
- [10.06.2016 2:29:41] : Пользователь авторизован 53159969
- [10.06.2016 2:29:41] : Первое колено друзей
- [10.06.2016 2:29:41] : Анализ завершен.
- [10.06.2016 2:29:59] : 5377771
- [10.06.2016 2:30:00] : 5544671
- [10.06.2016 2:30:00] : 5629049
- [10.06.2016 2:30:00] : 7062194
- [10.06.2016 2:30:00] : 10893633
- [10.06.2016 2:30:00] : 16170404
- [10.06.2016 2:30:00] : 18124762
- [10.06.2016 2:30:00] : 19191822
- [10.06.2016 2:30:00] : 26349555
- [10.06.2016 2:30:00] : 28868773
- [10.06.2016 2:30:00] : 34445280
- [10.06.2016 2:30:00] : 34457087
- [10.06.2016 2:30:00] : 40842025
- [10.06.2016 2:30:00] : 46561407

Сбор данных из социальной сети



Работа на программном комплексе ПКОКРАД

VkCombin v 1.0

SIGN IN DATABASE

VK

VISUALIZATION OF RESULTS.

VISUALIZE

STOP VISUALIZATION

REFRESH THE PAGE

SEND INFORMATION

ВЫБЕРИТЕ КОЭФФИЦИЕНТЫ:

START THE ENCRYPTION

Успешная авторизация пользователя.

4 2:46:20

Визуализация графа связей пользователей социальной сети



Работа на программном комплексе ПКОКРАД

VkCombin v 1.0

SIGN IN **DATABASE**

DATA PROTECTION.

КОЭФФИЦИЕНТ А:
171

КОЭФФИЦИЕНТ В:
11213

КОЭФФИЦИЕНТ М:
53125

СТЕРИДИРОВАНО:
281

НАЧАЛЬНОЕ ЗНАЧЕНИЕ:
12345

START THE GENERATION

VIEW GRAPH

Успешная авторизация пользователя.

2:47:46

10.06.2016 2:47:42] : Начало генерации.

10.06.2016 2:47:42] : a= 171 b=11213 m= 53125

10.06.2016 2:47:42] : a= 171 b=11213 m= 53125

1. 1100010010011101
2. 10111010000010
3. 110111011100101
4. 111101001111101
5. 111011010011
6. 1010001101000110
7. 1001101111110001
8. 1001001101001000
9. 1110111000001000
10. 11110100111011
11. 1000101000111100
12. 1100010100111
13. 110110011110110
14. 110011101100010
15. 1000111001110001
16. 111100101111111
17. 1000001110101110
18. 1100101101110100
19. 1011001010000110
20. 1000001111110000
21. 111000100001111
22. 100110110000001

Модуль генерации гаммы шифра



Работа на программном комплексе ПКОКРАД

VkCombin v 1.0

SIGN IN DATABASE

VK

VISUALIZATION OF RESULTS.

VISUALIZE

STOP VISUALIZATION

REFRESH THE PAGE

SEND INFORMATION

ВЫБЕРИТЕ КОЭФФИЦИЕНТЫ:

7. a=171; b=11213; m=53125; ▾

START THE ENCRYPTION

Успешная авторизация пользователя.

4 2:49:04

Визуализация зашифрованного графа связей пользователей социальной сети



Работа на программном комплексе ПКОКРАД

SIGN IN **DATABASE**

CLIENT ZONE.

VISUALIZE

STOP VISUALIZATION

REFRESH THE PAGE

ВЫБЕРИТЕ КОЭФФИЦИЕНТЫ:

START THE DECRYPTION

MENU **Успешная авторизация пользователя.** **4** **2:50:20**

Визуализация полученных данных клиентом



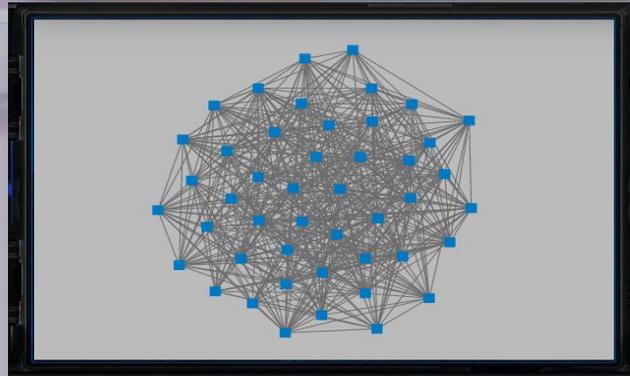
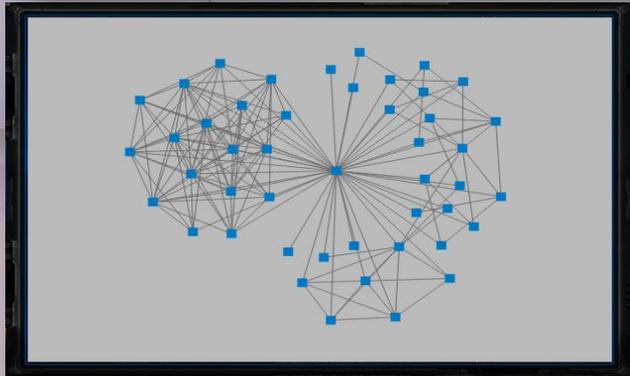
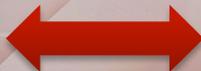
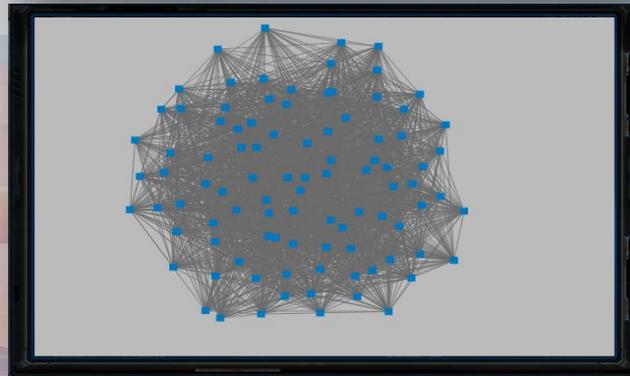
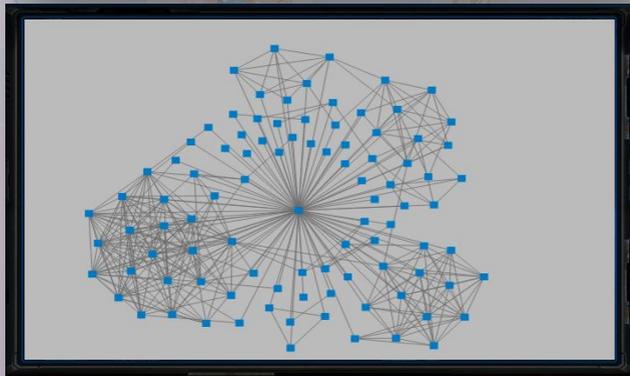
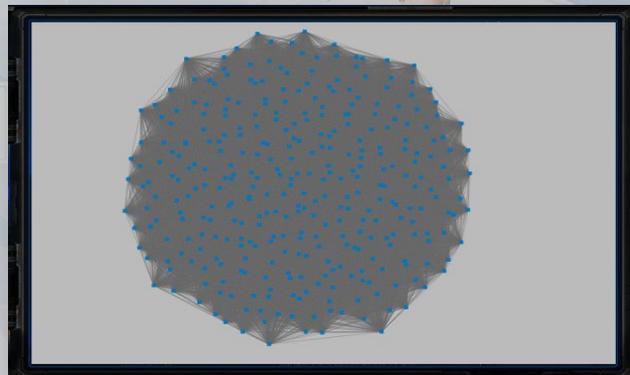
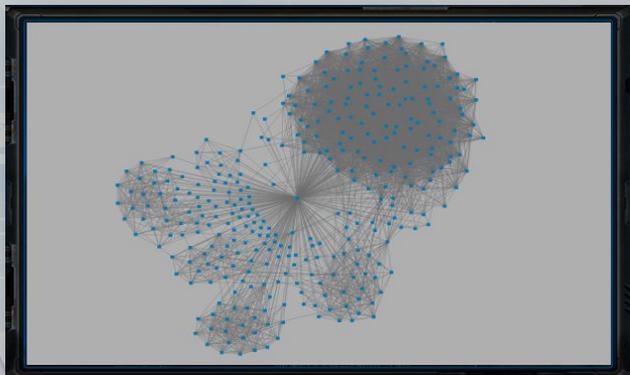
Работа на программном комплексе ПКОКРАД

The screenshot displays the POKRAD software interface, which is designed to look like a futuristic control panel. At the top, there are buttons for "SIGN IN" and "DATABASE", along with a profile picture of a man. Below this is a large central area labeled "CLIENT ZONE" containing a network graph visualization of a social network. To the right of the graph are several control buttons: "VISUALIZE", "STOP VISUALIZATION", "REFRESH THE PAGE", and "ВЫБЕРИТЕ КОЭФФИЦИЕНТЫ:" (Select Coefficients:). Below the selection buttons, there is a dropdown menu showing "7. a=171; b=11213; m=53125;". At the bottom right, there is a button labeled "START THE DECRYPTION". At the bottom left, there is a "MENU" button and a status bar displaying "Успешная авторизация пользователя." (Successful user authentication). A digital clock at the bottom right shows "2:51:22".

Визуализация дешифрованного графа связей пользователей социальной сети



Результаты работы программного комплекса ПКОКРАД





Улучшение программного комплекса ПКОКРАД

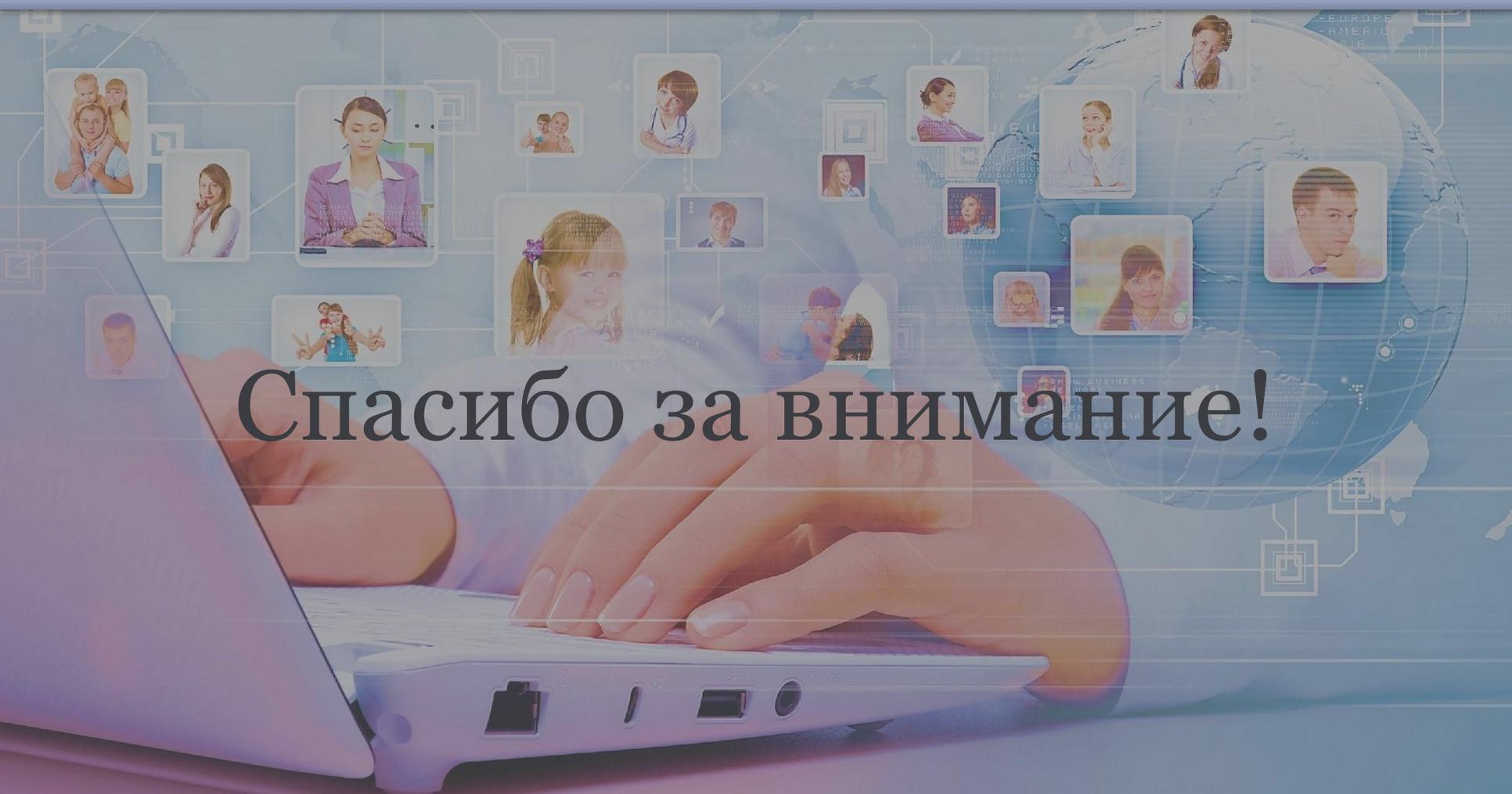




Заключение

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

14.06.2016