

УДК 004.942

Т. С. Залюбовская, В. Н. Сидоренко, Д. О. Гайдуков, А. М. Островская
Кременчугский национальный университет имени Михаила Остроградского, Кременчуг
Университет информационных технологий и менеджмента в Жешове, Польша

МОДЕЛИРОВАНИЕ ПРЕДНАМЕРЕННЫХ АТАК НА ПЕРСОНАЛЬНЫЕ АККАУНТЫ СОЦИАЛЬНОЙ СЕТИ

В работе предлагается концепция защит персональных аккаунтов сообществ социальных сетей, которая, в отличие от существующих, базируется на предварительном имитационном моделировании целенаправленных атак конкретного сообщества с целью определения ведущих и наиболее уязвимых нод сообщества, требующих повышенной защиты, удаление которых приводит к резкому распаду (перколяции) сообщества. В работе проведена серия имитационных экспериментов по целенаправленным атакам на социальные сообщества социальной сети «ВКонтакте» и установлено, что эффект перколяции имеет место как для графа всей сети, так и для отдельных сообществ, найденных с использованием различных известных методов кластеризации. При этом оценка порога перколяции колеблется в пределах 30-50 % целенаправленно удаленных вершин.

Ключевые слова: социальные сети, безмасштабные графы, целенаправленные атаки, перколяция графа.

Т. С. Залюбовська, В. М. Сидоренко, Д. О. Гайдуков, А. М. Островська
Кременчуцький національний університет імені Михайла Остроградського, Кременчук
Університет інформаційних технологій та менеджменту в Жешові, Польща

МОДЕЛЮВАННЯ НАВМИСНИХ АТАК НА ПЕРСОНАЛЬНІ АКАУНТИ СОЦІАЛЬНОЇ МЕРЕЖІ

У роботі пропонується концепція захисту персональних акаунтів спільнот соціальних мереж, яка, на відміну від існуючих, базується на попередньому імітаційному моделюванні цілеспрямованих атак конкретної спільноти з метою визначення провідних та найбільш уразливих нод спільноти, що вимагають підвищеного захисту, видалення яких приводить до різкого розпаду (перколяції) співтовариства. У роботі проведена серія імітаційних експериментів по цілеспрямованим атакам на соціальні спільноти соціальної мережі «ВКонтакте» та встановлено, що ефект перколяції має місце як для графа всієї мережі, так і для окремих спільнот, знайдених з використанням різних відомих методів кластеризації. При цьому оцінка порогу перколяції коливається в межах 30-50 % цілеспрямовано видалених вершин.

Ключові слова: соціальні мережі, безмасштабні графи, цілеспрямовані атаки, перколяція графу.

АКТУАЛЬНОСТЬ РАБОТЫ. В век развитых технологий и средств коммуникаций традиционные «бумажные» формы информационного обмена для основной массы населения отходят на второй план. Как показывают наблюдения, даже телевидение для прогрессивных людей и, особенно для молодого поколения, перестает быть главным источником получения информации в силу низкого качества телепродукции и отсутствия интерактивности. С развитием Internet и мобильных устройств пользователю предоставляются широчайшие возможности как для выбора источников и форм получения информации на заданную тему, так и для обмена информацией, включая фото, аудио и видео. Практика показывает, что основным средством коммуникации среди населения стран мира, имеющего доступ к Internet, являются социальные сети. В связи с этим, социальные сети рассматриваются как

одно из эффективных средств информационного влияния и противоборства, в первую очередь, в бизнесе и политике, как внутри стран, так и в процессе ведения информационных войн между странами.

В настоящее время существует ряд междисциплинарных научных исследований, посвященных вопросам информационного влияния, управления и противоборства в социальных сетях [1]. Построено большое количество всевозможных моделей. В то же время, рассмотрение социальной сети, как комплексной системы, представимой в виде графа, дает возможность использовать существенные научные наработки из другой междисциплинарной области, посвященной изучению таких систем (Complex Systems), в контексте защиты от нападения на персональные аккаунты. Например, известно [2-5], что так называемые безмасштабные сети (Scale Free Networks), которые включают World Wide Web, Internet, а также социальные сети, отображают высокую степень надежности к случайно направленным атакам. Однако эти же сети являются чрезвычайно уязвимыми к целенаправленным атакам, то есть, к выбору и удалению узлов с высокой степенью, которые играют жизненно важную роль в поддержании связей в сети. Уязвимость характеризуется явлением распада сети на части. В вышеуказанных работах для ассортативных сетей (сетей с положительной корреляционной связью) это явление называется перколяцией – фазовым переходом из состояния, когда сеть характеризуется связным графом, в состояние, когда имеет место образование массы отдельных фрагментов.

С точки зрения рассмотрения защиты аккаунтов социальной сети или целенаправленных атак на них, защиту можно интерпретировать двояко: как непосредственно от физического взлома аккаунтов, что приводит к разрушению сети, так и от информационного влияния, что должно в конечном итоге приводить к эффекту перколяции на информационном уровне. В последнем случае корректнее будет говорить о моделях распространения инфекции, которые по своей природе схожи с моделями перколяции [6-10]. При этом необходимо отметить, что эффект перколяции имеет аномалии в случае растущих сетей [11].

В связи с вышесказанным, вопрос разработки информационных технологий, позволяющих реализовать такого рода модели в задачах информационного влияния, управления и противоборства на уровне конкретного пользователя является весьма актуальным.

Авторами предлагается концепция оптимальной защиты требуемого социального сообщества или группы связанных сообществ, в основе которой лежит предварительное моделирование преднамеренных атак на основе реального графа сообщества по состоянию на текущий момент, с целью определения порога перколяции и ведущих аккаунтов, требующих повышенных мер защиты. Полученные результаты дают информацию для разработки стратегии оптимальной защиты.

Цель работы – повышение надежности аккаунтов социальных сообществ за счет синтеза оптимальной стратегии их защит на основе модели перколяции графа сообщества как составной части информационной технологии.

МАТЕРИАЛ И РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ. Для исследования использовались данные персональных аккаунтов пользователей социальной сети «ВКонтакте» г. Кременчуга в возрасте 17-25 лет. Механизм сбора был реализован посредством разработки программного приложения, взаимодействующего с сервером «ВКонтакте» через предоставляемые методы API.

В качестве инструмента разработки был использован язык высокого уровня Python 2.7.6 с набором специализированных библиотек: Networkx, Numpy, Mayavi и Matplotlib.

На рис. 1 изображен соответствующий ненаправленный граф, каждая нода которого ассоциирована с определенным персональным аккаунтом, а ребра графа представляют соответствующие связи.

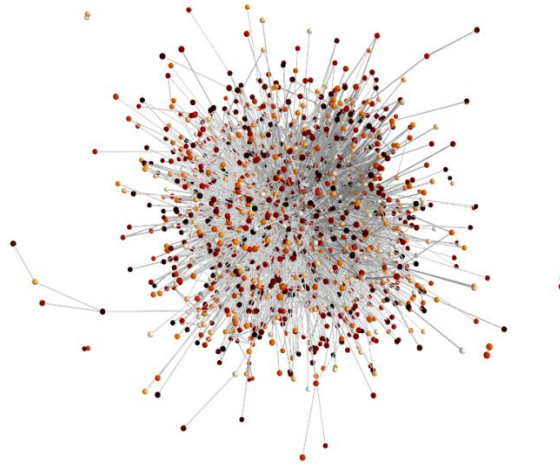


Рисунок 1 – 3D-визуалізація графа зв'язей персональних аккаунтів молодих людей г. Кременчуга в віці 17-25 лет

В таблице 1 приведены основные числовые характеристики графа. Как видно, сеть обладает положительной ассортативностью ($r \approx 0,044 > 0$) и высоким коэффициентом кластеризации сети ($\langle C \rangle \approx 0,238$), что подтверждает результаты, ранее полученные другими авторами.

Таблица 1 – Числовые характеристики графа (рис. 1)

Количество нод, N	Коэффициент ассортативности, r	Коэффициент кластеризации сети, $\langle C \rangle$
5171	0,0441148073621	0,238117436772

Основываясь на эксперименте, описанном в работе [2], был смоделирован процесс перколяции построенного графа с отслеживанием наибольшего кластера с размером S (рис. 2,а) и среднего кластера с размером $\langle s \rangle$ (рис. 2,б) в зависимости от доли удаленных нод.

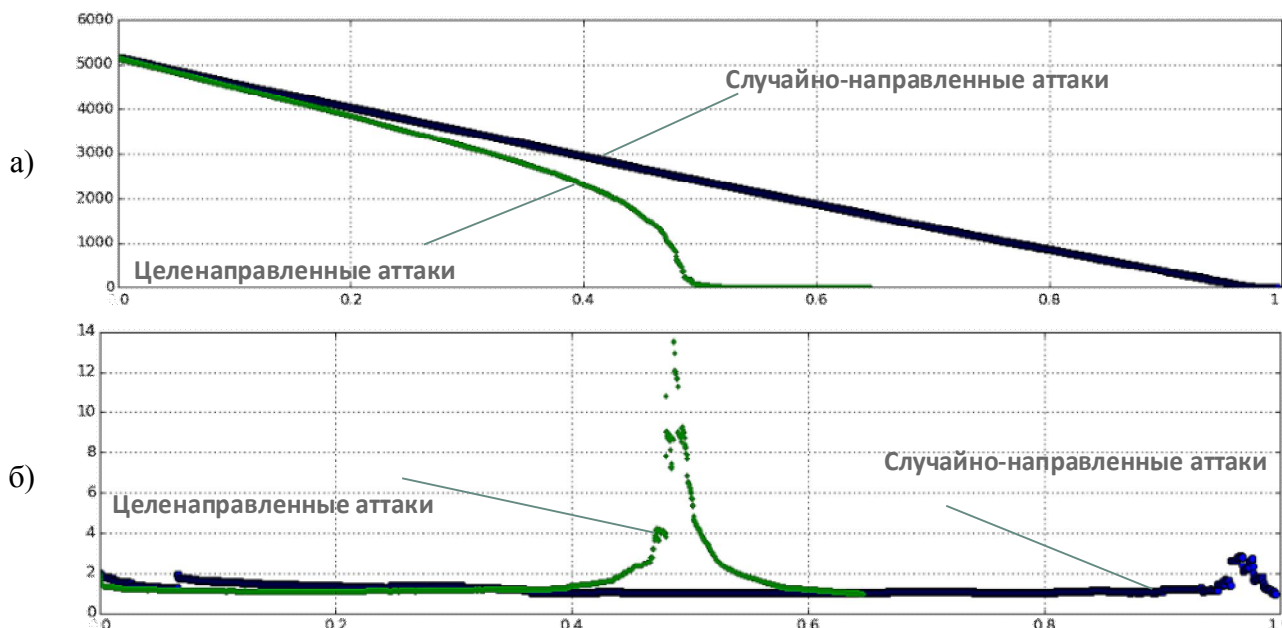


Рисунок 2 – Фрагментация графа: ось y – размер S наибольшего (а) и размер $\langle s \rangle$ среднего кластера (б), ось x – доля удаленных нод

Результаты подтверждают свойства перколяции безмасштабного графа, аналогичные тем, что были получены авторами [2].

Как видно из рисунков, для целенаправленных атак имеет место четко выраженный порог перколяции (эффект разрушения сети) при доле удаленных узлов, равной 0,5.

На следующем этапе был осуществлен поиск и 3D-визуализация (рис. 3,а) сообществ с использованием алгоритма Louvain [12].

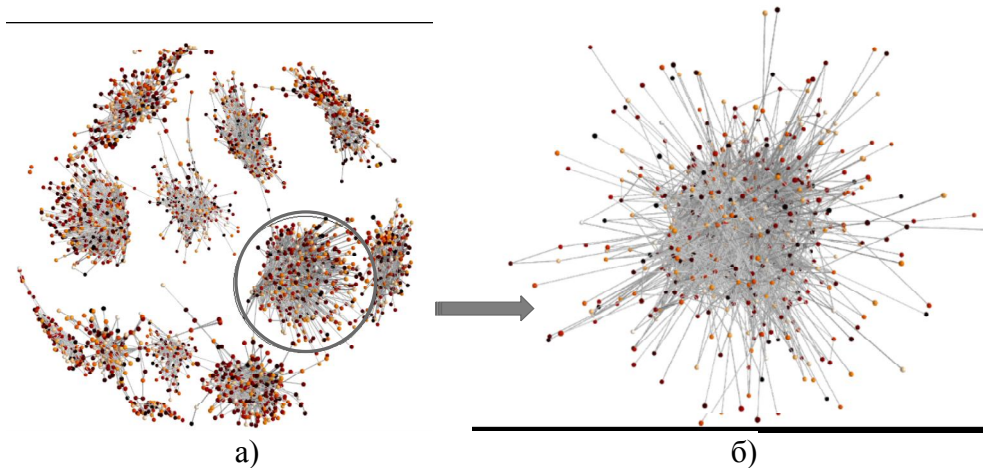


Рисунок 3 – 3D-визуализация графа сообществ (а) и графа сообщества с наибольшим числом узлов (б)

После выделения одного из сообществ (рис. 3,б), были найдены его числовые характеристики (табл. 2) и применена к нему модель процесса перколяции с визуализацией результатов (рис. 4 а,б).

Таблица 2 – Числовые характеристики графа выделенного сообщества (рис. 3)

Количество узлов, N	Диаметр, l	Коэффициент ассортативности, r	Коэффициент кластеризации сети, $\langle C \rangle$
940	7	0,0609364988023	0,281535528823

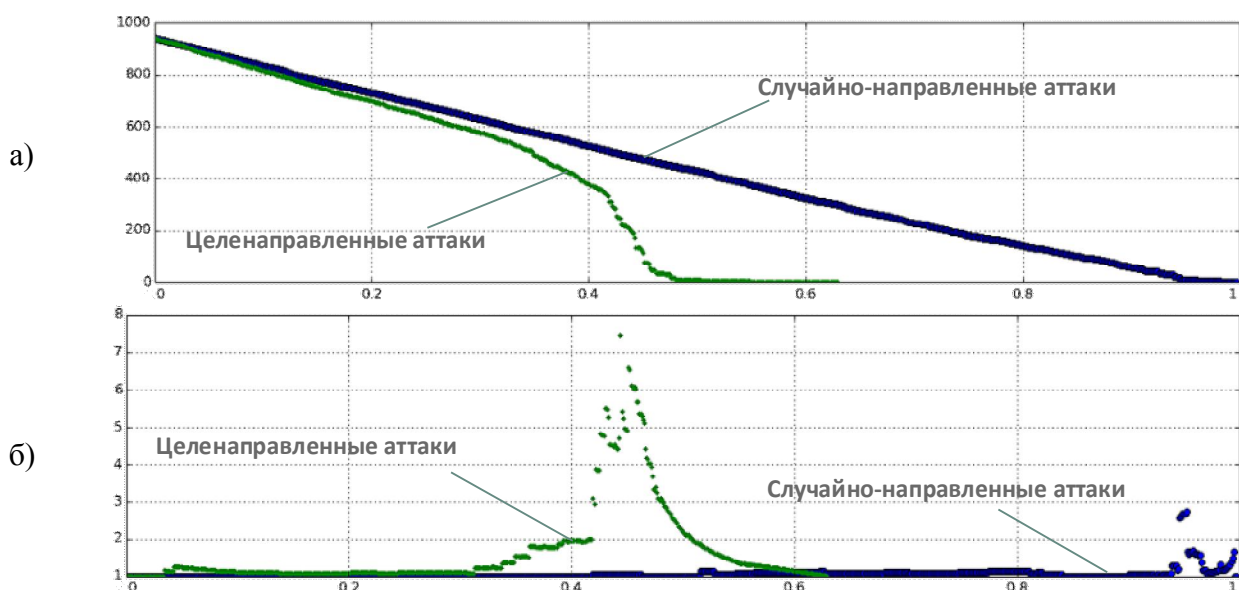


Рисунок 4 – Фрагментация графа: ось y – размер S наибольшего (а) и размер $\langle s \rangle$ среднего кластера (б), ось x – доля удаленных узлов

Как видно при удалении около 45 % нод, граф сообщества начинает резко разрушаться.

Для оценки порога перколяции разных методов сегментации и для разных сообществ была проведена серия последовательных экспериментов, суть которых заключалась в следующем: для графа, приведенного на рисунке 1, последовательно были применены три известных алгоритма кластеризации – лучшего разбиения, многоуровневых сообществ и на основе собственных векторов. Для каждого выделенного сообщества последовательно проводился имитационный эксперимент по преднамеренным атакам с последующим определением оценки порога перколяции. Как видно из результатов (табл. 3), порог перколяции находится в пределах $\approx 0,3 - 0,5$.

Таблица 3 – Оценки порога перколяции для разных сообществ, полученных разными методами кластеризации

best_partitions(from networkx)			community_multilevel (from igrph)		community_leading_eigen vector (from igrph)	
№ Сообщества	Кол-во нод	Порог перколяции	Кол-во нод	Порог перколяции	Кол-во нод	Порог перколяции
1	946	0,41	967	0,43	1312	0,35
2	940	0,45	939	0,42	1209	0,42
3	520	0,40	521	0,41	1010	0,35
4	485	0,39	463	0,39	896	0,38
5	357	0,39	357	0,38	604	0,38
6	328	0,37	324	0,35	7	0,29
7	294	0,29	300	0,35		
8	274	0,26	245	0,39		
9	222	0,38	222	0,30		
10	201	0,39	219	0,37		
11	189	0,36	192	0,35		
12	168	0,34	171	0,31		
13	117	0,40	114	0,42		
14	60	0,10	62	0,10		
15	56	0,02	61	0,02		

ВЫВОДЫ. Как показывают результаты моделирования, определение порога перколяции позволяет определить долю наиболее уязвимых нод, требующих усиленной защиты от преднамеренных атак. Установлено, что эффект перколяции имеет место как для графа всей сети, так и для отдельных сообществ, найденных с использованием различных известных методов кластеризации. Показано, что оценка порога перколяции колеблется в пределах 30-50 % целенаправленно удаленных вершин. При этом предполагается, что противник владеет аналогичной стратегией и может использовать ее как для физического взлома аккаунтов, так и для распространения «информационной инфекции», что не менее опасно. С другой стороны, если исходить из позиции нападающего в рамках задачи информационного противоборства, то имитационное моделирование по текущим данным дает возможность разработки оптимальной стратегии атаки на определенное сообщество.

Предложенный подход дает возможность разработки информационной технологии как защиты персональных аккаунтов социальных сетей, так и эффективного противодействия в задачах информационного влияния, управления и противоборства.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили. – М. : Физматлит, 2010. – 228 с.
2. Albert R. Error and Attack Tolerance of Complex Network / Réka Albert, Hawoong Jeong, Albert-László Barabási // *Nature. International weekly journal of science.* – 2000. – Iss. 406. – PP. 378–382.
3. Callaway D. S. Network Robustness and Fragility: Percolation on Random Graphs / Duncan S. Callaway, M. E. J. Newman, Steven H. Strogatz, Duncan J. Watts // *Physical Review Letters.* – 2000. – Vol. 85. – N. 25. – PP. 5468–5471.
4. Newman E. J. Finding and Evaluating Community Structure in Networks / E. J. Newman, M. Girvan // *Physical Review E.* – 2004. – Vol. 69. – Iss. 2. – 15 p.
5. Dorogovtsev S. N. Evolution of Networks. From Biological Nets to the Internet and WWW / S. N. Dorogovtsev, J. F. F. Mendes. – Oxford : Oxford University Press, 2003. – 264 p.
6. Pastor-Satorras R. Epidemic Spreading in Scale-Free Networks / Romualdo Pastor-Satorras, Alessandro Vespignani // *Physical Review Letters.* – 2001. – Vol. 86. – N. 14. – PP. 3200–3203.
7. Pastor-Satorras R. Epidemic Dynamics and Endemic States in Complex Networks / Romualdo Pastor-Satorras, Alessandro Vespignani // *Physical Review E.* – 2001. – Vol. 63. – Iss. 6. – 8 p.
8. Pastor-Satorras R. Immunization of Complex Networks / Romualdo Pastor-Satorras, Alessandro Vespignani // *Physical Review E.* – 2002. – Vol. 65. – Iss. 3. – 9 p.
9. Moreno Y. Epidemic Outbreaks in Complex Heterogeneous Networks / Y. Moreno, R. Pastor-Satorras, A. Vespignani // *The European Physical Journal B.* – 2002. – Vol. 26. – PP. 521–529.
10. Dezső Z. Halting Viruses in Scale-Free Networks / Zoltán Dezső, Albert-László Barabási // *Physical Review E.* – 2002. – Vol. 65. – Iss. 5. – 4 p.
11. Callaway D. S. Are Randomly Grown Graphs Really Random? / Duncan S. Callaway, John E. Hopcroft, Jon M. Kleinberg, M. E. J. Newman, Steven H. Strogatz // *Physical Review E.* – 2001. – Vol. 64. – Iss. 4. – 7 p.
12. De Meo P. Generalized Louvain Method for Community Detection in Large Networks / P. De Meo, E. Ferrara, G. Fiumara, A. Proveti // *Proceedings of the 11th International Conference On Intelligent Systems Design And Applications, November 22–24, 2011.* – IEEE, 2011. – PP. 88–93.

T. Zaliubovska, V. Sydorenko, D. Haidukov, A. Ostrovska

Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk

University of Information Technology and Management in Rzeszow, Poland

MODELING INTENTIONAL ATTACKS ON PERSONAL ACCOUNTS OF SOCIAL NETWORK

A conception of personal accounts' protection from social networks is proposed. In contrast to existent, it is based on a preliminary simulation modeling of target attacks on a particular community for the purpose of identification leading and the most vulnerable vertices of the community. Such vertices need an enhanced protection, because their deletion leads to the dramatic collapse (percolation) of the community. A number of simulated experiments with target attacks on communities of the social network "VKontakte" were done. It was ascertained that the effect of percolation occurs both for a graph of all the network and certain communities, that were found with use of different known clustering algorithms. In our case the estimation of percolation threshold varies within 30-50% target deleted vertices.

Keywords: social networks, scale-free graphs, target attacks, percolation.

REFERENCES

1. Gubanov, D.A., Novikov, D.A. and Chkhartishvili, A.G. (2010), *Sotsial'nye seti: modeli informatsionnogo vliyaniya, upravleniya i protivoborstva* [Social Networks: models of informational influence, control and confrontation], Fizmatlit, Moscow. [in Russian]
2. Albert, R., Jeong, H. and Barabási, A.-L. (2000), Error and Attack Tolerance of Complex Network, *Nature. International weekly journal of science*, Iss. 406, pp. 378-382.
3. Callaway, D.S., Newman, M.E.J., Strogatz, S.H. and Watts, D.J. (2000), Network Robustness and Fragility: Percolation on Random Graphs, *Physical Review Letters*, Vol. 85, no. 25, pp. 5468-5471.
4. Newman, E.J. and Girvan, M. (2004), Finding and Evaluating Community Structure in Networks, *Physical Review E*, Vol. 69, Iss. 2, 15 p.
5. Dorogovtsev, S. N. and Mendes, J.F.F. (2003), *Evolution of Networks. From Biological Nets to the Internet and WWW*, Oxford University Press, Oxford.
6. Pastor-Satorras, R. and Vespignani, A. (2001), Epidemic Spreading in Scale-Free Networks, *Physical Review Letters*, Vol. 86, no. 14, pp. 3200-3203.
7. Pastor-Satorras, R. and Vespignani, A. (2001), Epidemic Dynamics and Endemic States in Complex Networks, *Physical Review E*, Vol. 63, Iss. 6, 8 p.
8. Pastor-Satorras, R. and Vespignani, A. (2002), Immunization of Complex Networks, *Physical Review E*, Vol. 65, Iss. 3, 9 p.
9. Moreno, Y., Pastor-Satorras, R. and Vespignani, A. (2002), Epidemic Outbreaks in Complex Heterogeneous Networks, *The European Physical Journal B*, Vol. 26, pp. 521-529.
10. Dezsó, Z. and Barabási, A.-L. (2002), Halting Viruses in Scale-Free Networks, *Physical Review E*, Vol. 65, Iss. 5, 4 p.
11. Callaway, D.S., Hopcroft, J.E., Kleinberg, J.M., Newman, M.E.J. and Strogatz, S.H. (2001), Are Randomly Grown Graphs Really Random?, *Physical Review E*, Vol. 64, Iss. 4, 7 p.
12. De Meo, P., Ferrara, E., Fiumara, G. and Provetti A. (2011), Generalized Louvain Method for Community Detection in Large Networks, *Proceedings of the 11th International Conference On Intelligent Systems Design And Applications*, November 22-24, 2011, pp. 88-93.

Залюбовська Тетяна Сергіївна,
магістрантка кафедри «Комп'ютерні та інформаційні системи»,
Кременчуцький національний університет імені Михайла Остроградського,
вул. Першотравнева, 20, м. Кременчук
Полтавської обл., Україна, 39600.
Тел. +38(05366) 3-01-45.
E-mail: samorodok98@gmail.com



Zaliubovska Tetiana Serhiivna,
Student of Master Degree of Computer and Information Systems Department,
Kremenchuk Mykhailo Ostrohradskyi National University,
vul. Pershotravneva, 20, Kremenchuk,
Poltava Region, Ukraine, 39600.
Tel. +38(05366) 3-01-45.
E-mail: samorodok98@gmail.com

Сидоренко Валерій Миколайович,
к.техн.н., доцент,
доцент кафедри «Комп'ютерні та інформаційні системи»,
Кременчуцький національний університет імені Михайла Остроградського,
вул. Першотравнева, 20, м. Кременчук
Полтавської обл., Україна, 39600.
Тел. +38(05366) 3-01-45.
E-mail: vnsidorenko@gmail.com



Sydorenko Valerii Mykolaiovych,
Cand.Sc. (Eng.), Associate Professor,
Associate Professor of Computer and Information Systems Department,
Kremenchuk Mykhailo Ostrohradskyi National University,
vul. Pershotravneva, 20, Kremenchuk,
Poltava Region, Ukraine, 39600.
Tel. +38(05366) 3-01-45.
E-mail: vnsidorenko@gmail.com

Гайдуков Денис Олександрович,
magiistrant katedry «Stosunki
międzynarodowe»,
Wyższa Szkoła Informatyki i Zarządzania z
siedzibą w Rzeszowie,
ul. Sucharskiego, 2, Rzeszów, Podkarpackie
Region, Rzeczpospolita Polska, 35-225.
Tel. 17 866 11 11.
E-mail: w48071@student.wsiz.rzeszow.pl



Haidukov Denys Oleksandrovych,
Student of Master Degree of International
Relations Department,
University of Information Technology and
Management in Rzeszow,
ul. Sucharskiego, 2, Rzeszow, Podkarpackie
voivodeship, Poland, 35-225.
Tel. 17 866 11 11.
E-mail: w48071@student.wsiz.rzeszow.pl

Островська Анна Михайлівна,
студентка кафедри «Комп'ютерні та
інформаційні системи»,
Кременчуцький національний університет
імені Михайла Остроградського,
вул. Першотравнева, 20, м. Кременчук
Полтавської обл., Україна, 39600.
Тел. +38(05366) 3-01-45.
E-mail: afialka777@gmail.com



Ostrovska Anna Mykhailivna,
Student of Computer and Information Systems
Department,
Kremenchuk Mykhailo Ostrohradskiy
National University,
vul. Pershotravneva, 20, Kremenchuk,
Poltava Region, Ukraine, 39600.
Tel. +38(05366) 3-01-45.
E-mail: afialka777@gmail.com

Стаття надійшла: 10.06.2014