СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Понятие «социальная сеть» появилось еще 1954 году и ничего общего с Интернетом, конечно, не имело, а изучать это явление начали еще в 30-е годы прошлого столетия. Понятие ввел социолог Джеймс Барнс: «социальная сеть» – это социальная структура, состоящая из группы узлов, которыми являются социальные объекты (люди или организации) и связей между ними (социальных взаимоотношений). Если говорить более простым языком – это некая группа знакомых людей, где сам человек является центром, а его знакомые ветками. Между всеми членами сети есть двусторонние или односторонние связи.

По мере развития общества мы пришли к информационному веку, в котором создали массу видов коммуникации, что повлекло за собой скачок в развитии социальных сетей в пространстве Интернет. «Интернет - это коммуникационный медиум, которые впервые сделал возможным общение многих людей со многими другими в любой момент времени и в глобальном масштабе»[1].

Всего 5-7 лет назад начали активно развиваться социальные сети общего типа: для личного или делового общения. За общими сетями начали развиваться тематические проекты, которые использовали все тот же механизм социальных сетей, но в конкретной ограниченной нише. Этот процесс начался 3-5 лет назад и сейчас перешел в очень активную стадию. Сегодня можно найти социальные сети для ИТишников, туристов, меломанов, фотографов, спортсменов, книголюбов, политиков, ученых и т.д.

Влияние социальных сетей на жизнь людей огромное, многие даже не осознают до конца масштабы этого явления, а ведь социальные сети – это уже самое популярное занятие в Интернете. Сегодня из 100 самых посещаемых сайтов в мире 20 – это классические социальные сети и еще 60 – в той или иной степени социализированы. Более 80% компаний по всему миру использую социальные сети в работе. Около 78% людей доверяют информации из социальных сетей. Социальные сети стали самым центром современного Интернета.

На данный момент социальные сети по сути являются огромной базой данных с самой разнообразной информацией о сотнях миллионов людей по всему миру, которая к тому же неплохо структурирована. В последнее время сети все больше открываются внешнему миру, а многие личные данные пользователей уже доступны для всех желающих. Чем больше человек общается в разнообразных социальных сетях, тем больше информации о нем можно собрать без каких-либо трудов.

В последние 3-4 года тема информационной безопасности и приватности в социальных сетях привлекает много внимания. Это вполне объяснимо: сети все больше открываются внешнему миру, были случаи утечки личных данных, аккаунты пользователей легко взламываются, а у администрации сетей есть доступ к любой информации. Но все это только внешняя часть, которая лежит на поверхности и о которой пишет пресса, однако далеко не полная картина потенциальных угроз.

Самым безобидным, на первый взгляд, вариантом использования личных данных без разрешения пользователя можно считать внутренние механизмы социальных сетей для показа таргетированной рекламы, подбора потенциальных знакомых или отбора потенциально интересного контента. Эти механизмы стали стандартом почти во всех социальных сетях, и никто не скрывает данный факт: все они собирают и анализируют личные данные, которых в любой сети очень много, а потом используют их в коммерческих целях. Более того, социальные сети передают личные данные во внешний мир, и уже официально успели признать этот факт.

Еще более серьезные проблемы может вызвать взлом отдельных аккаунтов и получение доступа ко всей личной информации отдельного пользователя, если цель злоумышленников – определенный человек, или взлома аккаунтов определенной компании в целях промышленного шпионажа.

Отдельно стоит вспомнить о вирусах и фишинге, которые могут незаметно для пользователя воровать логины и пароли и после использовать их для незаконных действий (например, автоматическая рассылка спама от лица пользователя).

Однако самая большая угроза заключается в том, что доступ ко всей личной информации есть у довольно большой группы людей, и они могут в любой момент

еѐ просматривать, даже, если человек удалил что-то из сети. Во-первых, это сотрудники самой социальной сети: у них есть доступ к базам данных, в которых содержится вся информация, а также специальные инструменты входа в аккаунты пользователей, как, например, специальный мастер-пароль в Facebook, который позволяет войти в любой аккаунт. Во-вторых, доступ к информации также имеют правоохранительные органы, такие как ЦРУ в США или ФСБ в России. Не так давно известный разоблачитель Джулиан Ассандж, основатель Wikileaks, заявил, что Facebook имеет специальный интерфейс, который использует разведка США, а в России ранее популярная сеть ВКонтакте уже успела публично признать факты сотрудничества с правоохранительными органами и передачи личных данных. Все это вполне логично: сотрудники социальных сетей не могут не иметь доступ, в этом заключается их работа, а сотрудники правоохранительных органов ловят в сетях преступников, однако это не избавляет от опасности передачи данных третьим лицам, причем часто такими данными могут быть целые психологические портреты или конфиденциальная информация.

В последнее время пользователи все меньше доверяют социальным сетям и все чаще начинают фильтровать информацию, которую готовы доверить сети, давать ложную информацию или вообще удаляются из сети, однако даже удаление не дает уверенности: часто информация сохраняется на серверах компании и может использоваться в дальнейшем, в частности так делает Facebook, ВКонтакте и другие сети.

Интернет-зависимость – это уже давно признанное психологическое заболевание, а зависимость от социальных сетей - еѐ новая форма. Причины этого явления вполне объяснимы: у каждого человека есть явные и скрытые потребности, которые он стремится удовлетворить, это может быть потребность в общении, самореализации, экономии времени или еще чего-то, а социальная сеть дает ощущение удовлетворения этих потребностей. Однако по сути это уход от реальности, подмена реального на виртуальное, которое только дает ощущение удовлетворения потребностей, а на самом деле Интернет не может заменить реальной жизни, и поэтому человеку хочется еще и еще, и еще, но чем больше он

получает «общения» через Интернет, тем больше его хочется, а потребности все также остаются неудовлетворенными, по крайней мере, большинство из них.

Подобная зависимость постепенно развивается, человек «подсаживается на сеть», и чем больше времени он ею пользуется, тем сложнее ему жить реальной жизнью. Почувствовать это сложно, нужно на несколько дней оторваться от компьютера, и только тогда возникнет целый букет чувств, начиная от сильного желания зайти в Интернет и заканчивая серьезной депрессией, это и есть симптомы зависимости. Зависимость приводит к множеству проблем: появляются комплексы, депрессия, страхи, перепады настроения и даже сексуальные расстройства.

Это психологическое заболевание и, как любая болезнь, требует лечения. Лечить любые психологические проблемы сложно, а тем более зависимости.

Таким образом, актуальность исследования обусловлена следующим:

1. ростом популярности социальных сетей по интересам;
2. ростом силы, частоты и продолжительности воздействия вредоносного контента как средства информационного оружия;
3. ростом неграмотности пользователей в информационной сфере, что приводит к проблемам, связанным с негативным воздействием вредоносного контента, который оказывает информационно-психологическое воздействие не только на взрослых пользователей, но и детей.

Степень разработанности темы исследования. В настоящееврема существует достаточное количество литературных источников, посвященных анализу и проблемам специализированных социальных сетей, в том числе и социальным сетям по интересам. В имеющейся литературе рассмотрены такие вопросы, как:

- общая информация о сетях по интересам [10,11,12,7,13,14,15,16,17…24]
- популярные сети по интересам [32,33,34,35,36];
- преимущества и недостатки социальных сетей по интересам [32,33,34,35,36];
- построение сети, базирующейся на интересах, на основе графа и вычисление связей в нем [37];

-построение графа, определения взвешенности графа и ценности его информации [38];

- особенности социальных сетей, связывающих людей с похожими интересами [39];

- угрозы и риски вредоносного контента, распространяемого в сетях [41,42,43,44,3,45,46,47,48,49,50,51,52,4,53,54];

- меры, средства и модели противодействия контенту [55,56,57,58,45,59,60,61];

- оценка, анализ и управление рисками [62,63,64,59,65,66].

Несмотря на большой объем литературы, в данной области мало исследовались вопросы социальных сетей по интересам и распространения вредоносного контента в таких сетях, а так же вопросы оценки и регулирования риска, возникающего в результате воздействия вредоносного контента, средств и мер защиты от деструктивного воздействия. Таким образом, совершенствование методологии риск-анализа в целях повышения защищенности пользователей социальных сетей по интересам от воздействия вредоносного контента представляется актуальным.

Объектом исследования является социальная сеть по интересамScientificcollaboration, в отношении которойоказывает воздействие вредоносный контент.

Предметом исследованияявляется микромодель процесса распространения вредоносного контента для социальной сети по интересамScientificcollaboration.

Цель исследования состоит в анализе и подготовке рекомендаций по управлению эпидемическими процессами,возникающимив случае распространения деструктивного контента в популярных тематиках социальной сети Scientificcollaboration.Для достижения цели представляется необходимым решить следующие **задачи**:

1. Анализ, структурно-функциональные особенности испецификация контента в социальной сетиScientificcollaboration;

2. Сбор статистических данных в виде трехместного предиката, моделированиесоциальной сети Scientificcollaboration.Получение матриц: послойной

внутрисетевой связи, взвешенной центральности,удельного баланса трафика в вершинах социальной сети Scientificcollaboration.

3. Построениерепрезентативной выборки, отражающей свойства исследуемой сети.

4. Построение микро-моделираспространения вредоносного контента для социальной сети Scientificcollaboration. Моделированиеи анализ эпидемических процессов в репрезентативной выборке социальной сети Scientificcollaboration, построенных с помощьюавтоматизированного ПО, разработанного партнером по комплексной работе.

5. Разработка рекомендации по управлению эпидемическими процессами для рассматриваемых типов контента в социальной сети Scientificcollaboration.

Результаты, выносимые на защиту. После выполнения проделанной работы на защиту будут вынесены следующие пункты:

1. Структурно-функциональные особенности и звездная матрица для социальной сети Scientificcollaboration, полученная на основе собранной статистики в виде трехместного предиката и отражающая взаимосвязи между узлами сети;

2. Матрица репрезентативной выборки взвешенной инциденции и микро-модель распространения вредоносного контента, циркулирующего в сети Scientificcollaboration,на основе которыхс помощью специально разработанного программного обеспечения было проведено моделированиеэпидемических процессов распространения вредоносного контента;

3. Результаты моделирования:графики трафиков циркулирующих в социальной сети контентов при моделировании эпидемического процесса, графики противоборства двух типов контентов при моделировании процесса диффузии, риск, шанс.

4. Рекомендации по управлению эпидемическими процессами для рассматриваемых типов контента в социальной сети Scientificcollaboration.

Новизна результатов:

1. Впервые проведен анализ существующего контента в социальной сети Scientificcollaboration, а также построена репрезентативная выборка социальной

сети, удобная для дальнейшего анализа социальной сети Scientificcollaboration;

2. Впервые с использованием специально разработанного программного обеспечения, были получены графики циркулирующих трафиков в социальной сети при диффузии одного и двух контентов;

3. Впервые для социальной сетиScientificcollaborationбыли разработаны рекомендации по защите от деструктивного контента для различных типов субъектов, на основе анализа моделирования эпидемических процессов.

Теоретическая значимость работы заключается в:

1. Нахождении и доказательстве репрезентативной выборки генеральной совокупности социальной сети Scientificcollaboration;

2. Построении наглядных графиков циркулирующего в социальной сети трафика различных типов контентов;

3. Анализ проведенного моделирования и выработка рекомендаций на основе полученных результатов моделирования.

Практическая ценность работы заключается в том, что:

1. На основе структурно-функциональных особенностей сетиScientificcollaborationи распространяемого в нейконтента можно выявить характерные признаки деструктивного воздействия вредоносной информации;

2. Анализ звездной матрицы, матриц взвешенной центральности и удельного баланса позволяет определить, как связаны узлы между собой в случае многослойного представления сети, а также какие из них являются наиболее уязвимыми;

3. Моделирование процесса распространения вредоносного контента позволяет определить пути и методы осуществления негативного воздействия, оценить возможный ущерб от реализации угрозы, а также рассчитать параметры риска.

Методы исследования. В исследовании предполагается использовать методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы аналитического моделирования, методы теории рисков.

СПИСОК ЛИТЕРАТУРЫ

1 Виды социальных сетей: классификация и представители [Электронный ресурс]: Режим доступа: WorldWideWeb. – URL :http://darksiteofmarketing.com/stati/vidy-socialnyh-setei-klassifikacija-i-redstaviteli.html.

2 Borodin A., Finding authorities and hubs from link structures on the World Wide Web / A. Borodin, Roberts, P. Tsaparas / Proceedillgs of the 10th International World Wide Web Conference. – 2001. – P. 415-429.

3 Barabási, A. L., Jeong, H., Néda, Z., Ravasz, E., Schubert, A., &Vicsek, T. (2002). Evolution of the social network of scientific collaborations. Physica A: Statistical mechanics and its applications, 311(3), 590-614.

4 Scientific collaboration– Электрон. дан. – Режимдоступа:http://scipeople.ru.

5 Scientific collaboration– Электрон. дан. – Режимдоступа:http://link.springer.com/article/10.1007/s11192-007-1771-3.

6 Newman, M. E. J. the structure of scientific collaboration networks [Text]/ M. E. J. Newman// Proc. Natl. Acad. Sci. USA 98. -2001. – P. 404–409.

7 Newman, M. E. (2004). Coauthorship networks and patterns of scientific collaboration. Proceedings of the National Academy of Sciences, 101(suppl 1): 5200-5205.

8 Social Network Analysis John Scott 19 ноября 2012 г. SAGE– Электрон. дан. – Режимдоступа: http://www.pnas.org/content/98/2/404.full.

9 Чураков А. Н. Анализ социальных сетей // СоцИс. – 2001. – №1. – С. 109–121.

10 Abassi A. Betweenness centrality as a driver of preferential attachment in the evolution of research collaboration networks / A. Abassi, L. Hossain, L. Leydesdorff // Journal of Informetrics. – 2012. – № 6. – P. 403–412.

11 Dorogovtsev S.N., Evolution of Networks: From Biological Networks to the Internet and WWW / S.N. Dorogovtsev, J.F.F. Mendes; - Oxford, USA: Oxford University Press, 2003. — 280 p.

12 Жуликов С. Е., Жуликова О. В. Современные подходы к анализу социальных сетей // Гаудеамус: психолого-педагогический журнал. – 2012. – №2 (20). – С. 200–202.

13 Jennifer Golbeck. Introduction to Social Media Investigation: A Hands-on Approach. Waltham: ElsevierInc., 2015.

14 Alan E. Mislove. Online Social Networks: Measurement, Analysis, and Applications to Distributed Information Systems. Houston, Texas: RICE University, 2009

15 PanagiotisKarampelas. Techniques and Tools for Designing an Online Social Network Platform. NewHampshire: HellenicAmericanUniversity, 2013.

16 Valerio Arnaboldi, Andrea Passarella, Marco Conti, Robin I.M. Dunbar. Online Social Networks: Human Cognitive Constraints in Facebook and Twitter Personal Graphs. Waltham: ElsevierInc., 2015.

17 Barbara Carminati, Elena Ferrari, Marco Viviani. Security and Trust in Online Social Networks. Morgan&Claypool, 2014.

18 Евин, И. А. Введение в теорию сложных сетей [Текст] / Компьютерные исследования и моделирование. —2010. — Т.2, No2. — С. 121–141.

19 Статистический сайт компании Alexa. – Электрон.дан. – Режим доступа: http://www.alexa.com/siteinfo/Scientific collaboration.

20 Анализ сайта Scientificcollaboration – Электрон.дан. – Режим доступа: http://www.liveinternet.ru/stat/scipeople.ru/index.html.

21 Мирзануров Д.Х. Методика защиты от нежелательной информации, распространяемой в системах SocialNetwork / Д.Х. Мирзануров // Символ науки. 2015. № 5. С.48 – 51.

22 Монахов Ю.М., Аналитическая модель дезинформированного узла социальной сети / Ю.М. Монахов, М.А. Медведникова; ИММОД-2011. - Санкт-Петербург, 2011. – Т. II. – 400 с., - С. 178- 180.

23 Tsvetovat M., Social Network Analysis for Startups: Finding Connections on the Social Web. — O'Reilly, 2011. — P. 45. — 192 c.

24 Катасѐв А.С. Методика анализа защищенности аккаунтов социальных сетей от вредоносного контента / А.С.Катасѐв, А.П.Кирпичников, Р.И.Рамазанова // Вестник Казанского технологического университета. 2015.Т 18.№ 18. С. 195 – 198.

25 Ермилов, Е.В. Функции ущерба риска при описании отказов информационных систем критически важных объектов [Текст] / Е.В. Ермилов, Г.А. Остапенко, А.О. Калашников // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 247-248.

26 Калашников, А.О. Атаки на информационно–технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков[Текст]: монография / А.О. Калашников, Е.В. Ермилов, О.Н. Чопоров, К.А. Разинкин, Н.И. Баранников; под ред. чл.–корр. РАН Д.А. Новикова. – Воронеж: Научная книга, 2013. –160 с.

27 Леонов, Н. И. Основы конфликтологии: Учеб.пособие [Текст] / Н.И. Леонов, — Ижевск, 2000. —122 с.

28 PanagiotisKarampelas. Techniques and Tools for Designing an Online Social Network Platform. NewHampshire: HellenicAmericanUniversity, 2015.

29 Акулич М.М. Интернет – троллинг: понятие, содержание и формы/ М.М.Акулич // Вестник ТюмГУ . 2012. №8. С.47 – 54.

30 Черкасенко О.С. Феномен кибербуллинга в подростковом возрасте / О.С. Черкасенко // Личность, семья и общество: вопросы педагогики и психологии. 2015. № 6. С.15 – 20.

31 Внебрачных Р. А. Троллинг как форма социальной агрессии в виртуальных сообществах/ Р.А.Внебрачных // Вестник УдмГУ. 2012. №3 – 1.С.48 – 51.

32 Сайт статистики взвешенной матрицы. – Электрон.дан. – Режим доступа: http://opsahl.co.uk/tnet/datasets/Newman-Cond_mat_95-99-co_occurrence.txt.

33 Сайт статистики взвешенной матрицы. – Электрон.дан. – Режим доступа: http://opsahl.co.uk/tnet/datasets/Newman-Cond_mat_95-99-Author_names.txt.

34 Средство визуализации данных. - Электрон. Дан. – Режим доступа: https://gephi.org.

35 Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д.А. Новикова. –М.: Издательство физико-математической литературы, 2010. – 116с.

36 Гмурман В.Е., Теория вероятностей и математическая статистика. Учебное пособие. Высшее образование. – Москва, 2006 – С. 243.

37 George Casella, Roger L. Berger. Hypothesis Testing // Statistical Inference. — Second Edition. — Pacific Grove, CA: Duxbury, 2002. — С. 397. — 660 с.

38 Паринова, Л.В. К вопросу об оценке рисков атакуемых распределенных информационных систем: развитие математического обеспечения [Текст]/ Л.В. Паринова, Н.М. Радько, А.Г. Остапенко, В.Л. Каркоцкий, Д.Г. Плотников, А.Н. Шершень // Информация и безопасность. – 2012. – Т. 15. – № 4. – С. 585-586.

39 Радько, Н.М. Вирусные эпидемии в информационно-телекоммуникационных сетях: дискретные риск-модели [Текст]/ Н.М. Радько, О.А. Остапенко, Е.Н. Пономаренко, В.В. Исламгулова, А.О. Калашников, Р.К. Бабаджанов, Н.Н. Корнеева / Под ред. Член-корр. Д.А. Новикова. – Воронеж: Издательство «Научная книга». 2015. – 160 с.

40 Assessment of the system 's EPI -resistance under conditions of information epidemic expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, D.V. Gusev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (3). – P. 1781-1784.

41 Peak risk assessing the process of information epidemics expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251-255.

42 Discreet risk-models of the process of the development of virus epidemics in non-uniform networks / V.V. Islamgulova, A.G. Ostapenko,,N.M. Radko, R.K. Babadzhanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – P. 306-315.

43 Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M.

Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.

44 Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Jour-nal. – 2013. – 25 (3). – P. 410-415.

45 Optimization of expert methods used to analyze information security risk in modern wireless networks / S.A. Ermakov, A.S. Zavorykin, N.S. Kolenbet, A.G. Ostapenko, A.O Kalashnikov // Life Science Journal. – 2014. – № 11(10s). – P. 511-514.

46 Assessment of the system 's EPI -resistance under conditions of information epidemic expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, D.V. Gusev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (3). – P. 1781-1784.

47 Peak risk assessing the process of information epidemics expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251-255.

48 Discreet risk-models of the process of the development of virus epidemics in non-uniform networks / V.V. Islamgulova, A.G. Ostapenko,,N.M. Radko, R.K. Babadzhanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – P. 306-315.

49 Катасѐв А.С. Модели распространения вредоносного контента в социальных сетях / А.С. Катасѐв, Р.И. Рамазанова // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: VII Межрегиональная научно – практическая конференция. – Брянск: БГТУ, 2015. – С. 87 – 89.

50 M. E. J. Newman Newman, M. E. (2004). Coauthorship networks and patterns of scientific collaboration. Proceedings of the National Academy of Sciences. USA 98. -2001. – P. 312 – 318.

51 Fabian Hadiji, Christian Bauckhage, KristianKersting (2015). Maximum Entropy Models of Shortest Path and Outbreak Distributions in Networks // Diffusion of Innovations in Social Networks. – P. 54-63.