DOI: https://doi.org/10.15688/jvolsu10.2017.2.3

УДК 004.738.52
ББК 22/18

ТЕХНОЛОГИИ НЕДОПУЩЕНИЯ РАСПРОСТРАНЕНИЯ УГРОЗЫ ИНФОРМАЦИИ, ПРИВОДЯЩЕЙ К НЕГАТИВНЫМ ПОСЛЕДСТВИЯМ

Елена Александровна Максимова

Кандидат технических наук, доцент,
заведующая кафедрой информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Елена Александровна Евдокимова

Студентка института приоритетных технологий,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Анализ проблем информационной безопасности выявил наличие проблемы запрещенного контента. Один из способов ее решения – создание моделей и алгоритмов предотвращения распространения угрозы информации, приводящей к негативным последствиям (ИПНП). В настоящее время разрабатывается и апробируется большое количество технологий, тем не менее эффективной защиты пользователей от угроз распространения ИПНП, в частности, в социальных сетях не существует.

Ключевые слова: информация, негативные последствия, технология, модель, социальная сеть, запрещенный контент, информационная безопасность, Интернет.

В доктрину информационной безопасности Российской Федерации, утвержденную 5 декабря 2016 г. Указом Президента РФ № 646 [2], включены следующие положения:

1) национальные интересы в информационной сфере;

2) основные информационные угрозы и состояние информационной безопасности;

3) стратегические цели и основные направления обеспечения информационной безопасности;

4) организационные основы обеспечения информационной безопасности.

Доктрина обозначает наиболее яркие проблемы и угрозы в сфере информационной безопасности, в том числе связанные с распространением информации, приводящей к негативным последствиям (далее – ИПНП), через СМИ и интернет-сети. Последнее в свою очередь имеет глобальный масштаб, что обосновывается количеством потенциальных пользователей, временем использования и функциональными возможностями интернет-ресурсов.

Так, Фондом «Общественное мнение» был подготовлен и проведен специальный оп-

рос, главной задачей которого было определить, какой промежуток времени проводят российские пользователи в Интернете, с какой целью, насколько он значим для их повседневной жизни. Как оказалось, 87 % опрошенных считают, что Интернет принес больше положительных моментов, чем отрицательных. Только 3 % категорично заявили, что использование Интернета принесло больше плохого, а 10 % затруднились ответить на поставленный вопрос. В качестве плюсов 60 % респондентов отметили обширное количество полезной, а также общедоступной информации, 31 % – «широкие возможности общения между людьми», 8 % – «быстрый доступ к информации», еще 8 % рассматривают Интернет как развлечение и как одну из форм досуга. С помощью Интернета 7 % черпают новые возможности для работы и учебы, 6 % «расширяют кругозор», 4 % используют его для оплаты счетов и совершения дистанционных покупок. Большинство пользователей считают, что если их лишить возможности пользоваться Интернетом, то их жизнь изменится. Так считают 53 % россиян, этот ответ наиболее распространенный во всех возрастных группах. При опросе в возрастной категории старше 50 лет к такому ответу склоняются 47 % опрошенных, в возрасте от 18 до 24 лет – 61 % [4].

По данным Mediascope, ежемесячная российская аудитория Интернета в октябре 2016 – марте 2017 г. достигла 87 млн человек в возрасте 12–64 лет, что составило 71 % от всего населения страны [3]. При этом, согласно данным 1-Росстат от 10 марта 2017 г. «Об оценке численности постоянного населения на 1 января 2017 г. и в среднем за 2016 г.», общая численность населения России на 1 января 2017 г. составляет 146 804 372 человека, в том числе в возрасте 10–14 лет – 7,3 млн человек, 15–19 лет – 6,7 млн человек. Это те категории, которые в условиях социально-экономического кризиса и политической неопределенности, а также в силу возрастных психологических и физических особенностей, являются наиболее уязвимыми.

За год российская интернет-аудитория увеличилась на 2 %. При этом 66 млн человек, или 54 % населения РФ, пользуются интернетом хотя бы 1 раз в месяц через мобильные устройства, а 20 млн человек – 16 % населения страны – только с мобильных устройств.

Российский филиал исследовательского концерна GfK Group (Gesellschaft fur Konsumforschung Group) 26 января 2017 г. опубликовал отчет «Тенденции развития Интернет-аудитории в России». Суммарный объем выборки Омнибуса GfK за 2016 г. составил 12 622 респондента.

Аудитория интернет-пользователей в России в возрасте от 16 лет и старше осталась на уровне 2015 г. – 70,4 %, что составляет порядка 84 млн человек.

Распространение Интернета среди молодых россиян (16–29 лет) достигло предельных значений еще в предыдущие годы и, по данным GfK, составляет 97 %.

13 апреля 2016 г. на форуме РИФ+КИБ 2016 Руслан Тагиев (TNS) сообщил, что в России 85 млн интернет-пользователей в возрасте 12+, что составляет 69 % населения. Директор РАЭК Сергей Плуготаренко в своем докладе отметил, что выходят в Сеть каждый день 66,5 млн россиян.

91–124 минуты в сутки, в среднем, проводят пользователи 12–64 лет в больших городах (от 700 тыс. человек) в мобильном интернете. В возрастной группе 12–24 года этот показатель составляет 124 минуты, в группе 35–64 года – 91 минуту. Большую часть этого времени пользователи моложе 35 лет проводят в социальных сетях. Эти и другие данные представил на форуме RIW-2016 директор по мультимедиа-исследованиям TNS Russia Михаил Райбман, сообщает сайт Adindex.ru.

В мире существует большое количество различных социальных сетей. Однако к наиболее популярным относят: в США – «Facebook», «MySpace», «Twitter» и «LinkedIn»; «Nexopia» – в Канаде, «Bebo» – в Великобритании, «Facebook», «dol2day» – в Германии. В России на сегодняшний день самыми популярными являются «ВКонтакте», «Одноклассники.ru» и «Мой Мир@mail.ru».

Современной проблемой таких систем является низкий уровень информационной безопасности, в том числе при предотвращении распространения ИПНП.

В России 1 сентября 2012 г. вступил в силу Федеральный закон от 29.12.2010 № 436-ФЗ

(ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию». В данном законе к запрещенной для распространения среди детей информации относится:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством (в ред. Федерального закона от 29.06.2015 № 179-ФЗ);

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи (в ред. Федерального закона от 29.06.2013 № 135-ФЗ);

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

8) сведения о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место жительства или место временного пребывания, место учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего (п. 8 введен Федеральным законом от 05.04.2013 № 50-ФЗ).

Для решения задачи, связанной с недопущением распространения угрозы ИПНП, в настоящее время разрабатываются и апробируются новые технологии, например, предложенные в трудах В.А. Герасименко, С.П. Расторгуева, П.Д. Зегжды, В.И. Завгороднего, А.А. Малюка, А.А. Грушо, В.В. Домарева, Р. Брэтта, К. Касперски, С. Норкатта, В. Столингса. Тем не менее эффективной защиты пользователей от угроз распространения ИПНП, в частности в социальных сетях, не существует.

Широкое распространение сегодня имеют технологии, основанные, например, на использовании моделей влияния, моделей просачивания и заражения (Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили, J. Leveille, D. Watts и S. Strogatz, R. Albert и A. Barabasi, J. Leskovec, M. Gjoka, S.N. Dorogovtsev, M.E.J. Newman и R.M. Ziff, J.O. Kephart и S.R. White и др.). Как правило, в них не учитываются топологические особенности сети. Взаимодействие между элементами крупномасштабных сетей при этом может дать погрешность прогнозирования угроз распространения ИПНП.

Наиболее распространенной является технология, основанная на комплексном подходе. Здесь среди множества функций защиты выделяется функция предупреждения проявления ИПНП. Она реализуется средствами прогнозирования угрозы распространения и рассылкой сообщений с предупреждениями о последствиях действий с запрещенным контентом.

Можно также определить следующие функции защиты от ИПНП в социальных сетях (см. таблицу). Выделенные функции реализуются на различных этапах работы с ИПНП.

Интересна технология, в рамках которой рассматривается только обмен сообщениями между пользователями. Концептуальная математическая модель информационного взаимодействия при этом представляется графом, узлами которого являются пользователи, а ребрами – связи между ними. Наиболее эффективное прогнозирование распространения угрозы ИПНП здесь осуществляется с помощью моделирования данного процесса (моделирование угрозы распространения ИПНП).

При рассмотрении вопросов, касающихся моделирования процессов, протекающих в социальных сетях, основным подходом является применение моделей влияния, информа-

Функции защиты от информации, приводящей к негативным последствиям, в социальных сетях

Наименование функции защиты	Описание
Предупреждение условий возникновения ИПНП	Реализуется с помощью нормативно-правовых актов. Не может полностью исключить угрозу распространения ИПНП в социальных сетях из-за проблемы соблюдения законов и технических сложностей в интернет-пространстве
Предупреждение непосредственного проявления ИПНП	Препятствует распространению ИПНП в социальной сети
Обнаружение проявившейся ИПНП	Связана с мониторингом сети на предмет ИПНП на страницах пользователей, с проблемами контекстного поиска, а также с необходимостью контроля над всей системой
Предупреждение воздействия на абонентов проявившейся ИПНП	Реализуется с помощью автоматической рассылки сообщений с предупреждением об ответственности за распространение ИПНП, вплоть до блокировки пользователя. Блокировка может осуществляться как легитимными, так и нелегитимными средствами. В первом случае – предупреждаются пользователи, на страницах которых найдена ИПНП, во втором – рассылаются предупреждения потенциальным получателям ИПНП
Обнаружение воздействия ИПНП на пользователей	Связана непосредственно с фиксацией процесса распространения ИПНП, может быть реализована через контекстный анализ сообщений
Локализация, ограничение воздействия ИПНП на пользователей	Реализуется через блокировку пользователей, распространяющих ИПНП; для ее эффективной реализации необходим контроль над системой
Ликвидация последствий обнаруженного воздействия ИПНП на пользователей	Связана с удалением ИПНП из системы; для реализации также необходим контроль над системой

ционного управления и противоборства [1]. В данной работе рассматриваются модели влияния, так как они наиболее адаптивны к решаемым задачам. В качестве моделей влияния выступают:

1) пороговые модели – любые модели, в которых есть пороговое значение или набор пороговых значений, используемых при изменении состояний. Классические модели с порогами были разработаны Schelling, Axelrod и Granovetter для моделирования коллективного поведения [5];

2) модели независимых каскадов (Independent Cascade Model). Принадлежат к категории моделей так называемых «систем взаимодействующих частиц»;

3) модели просачивания и заражения – популярный способ изучения распространения информации и инноваций в социальных системах (эпидемиологические модели);

4) модель Изинга – математическая модель, описывающая возникновение намагничивания материала. Предполагается, что конформность или независимость в большой социальной группе может моделироваться с помощью влияния ближайших соседей. Аналогом температуры является готовность группы мыслить творчески, готовность принять новые идеи. Внешним полем для социальной группы является влияние «авторитета» или управление;

5) модели взаимной информированности [1]. Есть агент, входящий в некоторую социальную сеть. Агент информирован о текущей ситуационной обстановке (действиях и представлениях других агентов, параметрах среды – так называемом состоянии природы (state of nature) и т. п.). Ситуационная обстановка влияет на имеющийся у агента набор ценностей, установок и представлений. Предрасположенность к тем или иным представлениям и ситуационная обстановка (например, действия других агентов) приводят к формированию новых или модификации старых представлений. В соответствии с этим агент принимает решение и выполняет действие. Результаты действий приводят к изменению как самой ситуационной обстановки, так и внутренних ценностей, установок и представлений;

6) модели согласованных коллективных действий. Ключевое значение здесь имеют социальные связи. С одной стороны, социальные связи могут обеспечить эффективный локальный социальный контроль для стимулирования участия в коллективном действии.

С другой стороны, эти связи обеспечивают агента информацией о намерениях и действиях других агентов в сети и формируют его (неполные) представления, на основе которых агент принимает свои решения. И, наконец, в пределах социальных связей агенты могут прикладывать совместные усилия по созданию локального общественного блага и совместно пользоваться им.

Анализ проблем информационной безопасности выявил наличие проблемы запрещенного контента. Один из способов ее решения – создание моделей и алгоритмов предотвращения распространения угрозы ИПНП. Однако в силу специфики организационной структуры менеджмента информационной безопасности в качестве основной (зачастую единственной) технологии работы в данном направлении на практике является технология, основанная на комплексном подходе. При этом работа идет с ограниченным количеством функций защиты, что приводит к неразрешимости обозначенной проблемы и невозможности обеспечения безопасности информационного пространства в целом.

СПИСОК 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. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 года. – Электрон. текстовые дан. – Режим доступа: http://www.scrf.gov.ru/documents/6/5.html (дата обращения: 17.01.2017). – Загл. с экрана.

3. Развитие Интернета и его значение. – Электрон. текстовые дан. – Режим доступа: http://www. bizhit.ru/ (дата обращения: 21.06.2017). – Загл. с экрана.

4. Сколько времени россияне проводят в сети и какие сайты посещают? – Электрон. текстовые дан. – Режим доступа: http://wiseanswers.ru/skolko-vremeni-rossiyane-provodyat-v-seti-i-kakie-sajty-poseshhayut/ (дата обращения: 20.06.2017). – Загл. с экрана.

5. On-Line Guide for Newcomers to Agent-Based Modeling in the Social Sciences Robert Axelrod and Leigh Tesfatsion. – Электрон. текстовые дан. – Режим доступа: http://www2.econ.iastate.edu/tesfatsi/abmread.htm/ (дата обращения: 21.06.2017). – Загл. с экрана.

REFERENCES

1. Gubanov D.A., Novikov D.A., Chkhartishvili A.G. *Sotsialnye seti: modeli informatsonnogo vliyaniya, upravleniya i protivoborstva* [Social Networks: Models of Informational Influence, Management and Confrontation]. Moscow, Fizmatlit Publ., 2010. 228 p.

2. *Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii ot 5 dekabrya 2016 g.* [The Doctrine of Information Security of the Russian Federation of December 5, 2016]. URL: http://www.scrf.gov.ru/documents/6/5.html. (accessed January 17, 2017).

3. *Razvitie Interneta i ego znachenie* [Development of the Internet and Its Meaning]. URL: http://www.bizhit.ru/. (accessed June 21, 2017).

4. *Skolko vremeni rossiyane provodyat v seti i kakie sayty poseshchayut?* [How Much Time do Russians spend on Internet and What Sites do They Surf?]. URL: http://wiseanswers.ru/skolko-vremeni-rossiyane-provodyat-v-seti-i-kakie-sajty-poseshhayut/. (accessed June 20, 2017).

5. *On-Line Guide for Newcomers to Agent-Based Modeling in the Social Sciences Robert Axelrod and Leigh Tesfatsion*. URL: http://www2.econ.iastate.edu/tesfatsi/abmread.htm/. (accessed June 21, 2017).

TECHNOLOGIES FOR PREVENTING THE DISSEMINATION OF INFORMATION LEADING TO NEGATIVE CONSEQUENCES

Elena Aleksandrovna Maksimova

Candidate of Technical Sciences, Associate Professor,
Head of the Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Elena Aleksandrovna Evdokimova

Student, Institute of Advanced Technologies,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Public Opinion Fund prepared and carried out special survey, which main task was to determine how much time Russian users had spent on the Internet, with what purpose, and how significant it had been for their daily lives. As it turned out, 87 % of respondents believe that the Internet has brought more positive things than negative. Only 3 % categorically stated that the use of the Internet has brought more bad, and 10 % did not answer the question. As the pros 60 % of respondents note a large number of useful and public information, 31 % – ample opportunities of communication between people, 8 % – quick access to information, another 8 % consider the Internet as entertainment and as a form of entertainment. Using the Internet, 7 % draw up new opportunities for work and study, 6 % – the "expanding horizons", 4 % use it for paying bills and making remote purchases. Most users believe that if you deprive them of the ability to use the Internet, their lives will change. 53 % of Russians think so, and the answer is common in all age groups.

Analysis of information security problems reveals the problem of prohibited content. One way to solve it is to create models and algorithms to prevent the dissemination of threat of information, which have negative consequences. Currently, a large number of technologies are being developed and tested. Nevertheless, the effective protection of users from the threats of the dissemination of information, which have negative consequences, in particular, in social networks, does not exist.

Key words: information, negative consequences, technology, model, social network, prohibited content, information security, the Internet.