УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Сборник научных трудов

Под редакцией член-корреспондента РАН
В.И. Борисова

Выпуск 1 (15), 2017

Воронеж
Издательство «Научная книга»
2017

УДК 004.42
ББК
У

Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. Вып. 1 (15), 2017. – Воронеж: Издательство «Научная книга». 2017. – 109 с.

ISBN

Статьи посвящены широкому кругу вопросов, связанных с исследованиями в области обеспечения безопасности пользователей сети Интернет, посредством оценки и регулирования их рисков.

Издание предназначено для специалистов и студентов в области обеспечения информационной безопасности.

Статьи сборника издаются в авторской редакции.

УДК 004.42
ББК
У

СОДЕЖАНИЕ

МЕЖРЕГИОНАЛЬНЫЙ ФОРУМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

МАТЕРИАЛЫ

Научно-практической конференции «Безопасный Интернет»

УДК 004.056.5

НАУЧНО-МЕТОДИЧЕСКИЕ ОСНОВЫ КОММЕРЦИАЛИЗАЦИИ ПРОГРАММНОГО ПРОДУКТА «NETEPIDEMIC»

А.Г. Остапенко, Е.А. Шварцкопф, Г.А. Остапенко, Л.В. Паринова

Разрабатываемый в настоящее время программный комплекс «Netepidemic» ориентирован на моделирование информационных эпидемий во взвешенных гетерогенных сетях [1-6]. Его алгоритмы позволяют формализовать процессы распространения деструктивного контента в сетевых структурах на основе матрицы взвешенной центральности элементов [7] и матрицы послойной внутрисетевой связности [8-12], а также микромодели вершины (агента) сети [13], учитывающей специфику восприятия агентом предлагаемого его вниманию контента. Субъективизм последней процедуры затрудняет коммерциализацию продукта.

Поэтому в настоящей работе предпринята попытка дальнейшей формализации этой процедуры в целях удобства пользования предлагаемым продуктом. Суть заключается в том, что практический интерес представляет процесс распространения в сетях не столько деструктивного контента, рассматриваемого в задачах обеспечения информационной безопасности [14-17], сколько контента вообще. Для широкого пользователя это его аудио и видео информационные блоки, популярность которых он хотел бы завоевать в соцсетях. В большинстве

гражданских случаев это не деструктив, а инструмент самореализации [18-20] в социальной и профессиональной среде. Именно здесь видится возможность самого широкого применения предлагаемого комплекса программ, ибо мощность множества таких пользователей насчитывает десятки миллионов человек.

На старте процесса, по большому счету, пользователю прежде всего необходимо определиться с соцсетью или классом соцсетей, отвечающим его интересам. Классификация таковых известна [4], и текущие статистические данные по топологии и «силе связей» в таких сетях открыто публикуются [21-26]. Именно эти данные служат основой для построения вышеупомянутых матриц, используемых в дискретных моделях процесса распространения контента в сетях [1,3,5-12, 17]. Определившись с сетью и получив ее данные, с помощью «Netepidemic» пользователь получит автоматизированную макромодель процесса. Далее, опираясь на матрицу взвешенной центральности и исходя из собственных возможностей доступа, он должен выбрать вершины сети, к которым будет доставляться контент.

Остается открытым вопрос о построении микромодели восприятия контента агентом. Детерминированный подход здесь неуместен, и необходимо применять вероятностный анализ, который для пользователя должен определить степень восприимчивости его контента агентами сети. Очевидно, она будет разниться в зависимости от слоя внутрисетевого взаимодействия. В этой связи для инженерного расчета уместно предложить следующую оценку вероятности восприятия

$$P_{BC}(x_i) = K_{KT}P(k), \qquad (1)$$

где K_{KT} – коэффициент восприимчивости (заразности) распространяемого контента;

P(k) – значение закона распределения степени вершин для *k*-го слоя (степень вершин равна *k*) сети, к которому принадлежит вершина (агент) x_i (номер ее имеется в текущей статистике).

Для социальных сетей, имеющих безмасштабный характер, *P(k)* представляет собой степенное распределение, достаточно хорошо изученное в научной литературе [27,28]. Фактически *P(k)* отвечает на вопрос о степени уникальности (элитарности) в сети вершин ее *k* –го слоя, которая напрямую связана с восприимчивостью этими вершинами информации, поступающей извне. Чем меньше агентов с данным качеством связности, тем более избирательно (с большей фильтрацией) они относятся к внешнему контенту. Это выражает степенное убывание *P(k)* с ростом степени вершин *k*.

Относительно определения коэффициента K_{KT} пользователю следует предложить экспериментальный путь. Сгенерированный контент уместно апробировать на окружении методом опроса заинтересованности в этом контенте, пронормировав результаты и сведя этот коэффициент в интервал значений от нуля до единицы. Данный коэффициент отражает специфику контента.

Задав, таким образом, вероятность восприятия (1) для каждого слоя, можно приступать к моделированию процесса распространения контента в сети.

Пользуясь предлагаемым инструментарием, пользователь может оперативно ориентировочно спрогнозировать ожидаемую восприимчивость сети к распространяемому в ней контенту, что позволяет надеяться на широкую популярность настоящего программного комплекса и успешную его коммерциализацию.

При подготовке к моделированию процесса распространения контента для пользователя важно представлять схему и механизм первичного «вброса» в сеть своего продукта. Простейшая схема такого

вброса представлена на рис. 1. Механизм подобной «инъекции» можно описать следующим образом.

Пользователь, рассматривая свой аккаунт как плацдарм для распространения сгенерированного контента, использует все имеющиеся в его распоряжении возможности для популяризации своего продукта. Это, прежде всего, новостная лента сети, привлекающая внимание её пользователей к данному контенту. Наконец, с той же целью пользователь может организовать ссылки на свой аккаунт в других сетях, расширяя круг возможных интересантов. Все это повышает вероятность успешного вброса контента в сетевое пространство. Разумеется, это надо учесть в стартовой микромодели (1). Подобный механизм (рис.1) применим и при описании вброса через блоги.

Таким образом, важнейшим может являться модель доставки контента, для которой используются новостные ленты, тематические сообщества и др. Формализация этих процедур на вероятностной основе представляется необходимой, имея в виду, что факт выбора обычно констатирует «лайк» и т.п. Пошаговое моделирование ветвящегося процесса «путешествия» контента по соцсети должен реализовать предлагаемый инструментарий, где необходимо учитывать вероятностные характеристики доставки и восприятия распространяемого контента. Причем, они имеют свою специфику для всякой рассматриваемой социальной информационной сети. Это должен учитывать программный комплекс «Netepidemic», особенно в плане коммерциализации предлагаемого продукта.

Условно данный проект можно назвать «калькулятор успеха». Он нацелен на прогнозное моделирование процессов распространения контента в социальных сетях, а удачный прогноз это уже половина успеха. Оценивая шансы обладания (восприятия) сгенерированного контента сетевой структурой, пользователь соцсети измеряет возможности своего

интеллектуального продукта. Амбиции автора могут успешно реализоваться в данном случае через мощный инструментарий электронного общения. При этом затратная часть в основном сконцентрирована в области генерации качественного контента, а главной целью современного пользователя (в широком смысле) является самореализация через завоевание популярности в сети. Он готов многократно совершать попытки по достижению данной цели и «калькулятор успеха» может оказаться удобным подспорьем в сокращении количества подобных попыток.

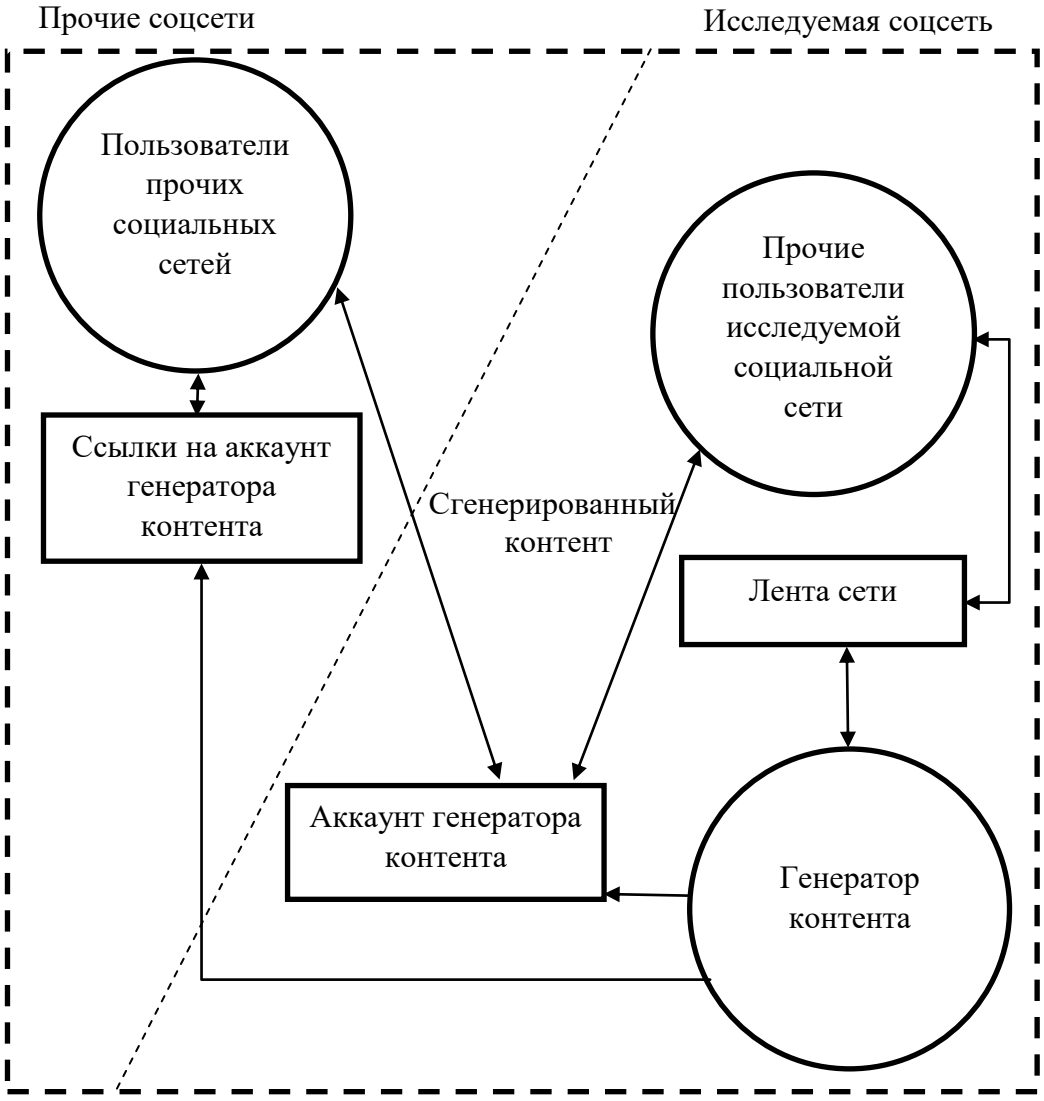

Рис. 1. Простейшая схема вброса в социальные сети контента, сгенерированного пользователем

Программный комплекс «Netepidemic» создавался для моделирования процессов сетевого распространения деструктивного контента, т.е. оценки эпистойкости сети в контексте обеспечения её безопасности. Однако, как это видно из вышеизложенного, просматривается его «двойное назначение». Он может быть достаточно универсальным, ибо применим как к контенту со знаком «минус» (деструктивному), так и контенту со знаком «плюс» (позитивному). Здесь всё зависит от намерений пользователя, генерирующего контент. И чем искуснее создан этот продукт, тем больше пользы или вреда (ущерба) он принесет сети и её социуму. Таким образом, интеллектуальный потенциал пользователя (в отсутствии жесткого контроля сети) играет здесь важнейшую роль, что во многом и определяет растущую популярность социальных сетей современности.

Создание популярного прикладного программного обеспечения (скажем, мобильного приложения) должно учитывать технические возможности широкого пользователя. В этом контексте не представляется реальным исследование крупномасштабных социальных сетей с помощью известных продуктов Signal/Collect, GraphLab, PBGL, KDT, ScaleGraph,Giraph, GraphX, которые для анализа многоразмерных сетей применяют суперкомпьютеры. «Проклятие размерности», довлеющее над такого рода задачами, должно быть снято. Только тогда можно будет говорить о возможности бытового применения предлагаемого программного обеспечения (скажем, на уровне смартфона). Такая возможность появляется в результате преобразования исходной сети в её репрезентативную выборку с сохранением сетевых свойств. Критерием подобия в этом случае можно выбрать закон распределения степеней вершин (для соцсетей он степенной), задав допустимые его отклонения при преобразовании сети от миллионов до сотен пользователей (очевидно, весомых).

В результате открывается перспектива осуществления инженерного (в первом приближении) и оперативного расчета параметров распространения в сети контента, сгенерированного пользователем. Условно такой инструментарий можно назвать «калькулятором сетевого успеха», с помощью которого представляется возможным оценить шансы успешного продвижения контента в пространстве интересующей социальной сети.

В качестве информационного обеспечения уместно использовать статистические данные топологии соцсетей (ресурс), где «сила» связи её элементов выражена трехместным предикатом (номер вершины-истока, номер вершины-стока, вес дуги, их связывающей). Очевидно, объединение таких предикатов и образует сеть, которую надо разрядить, исключив малозначимые вершины и оставив вершины в репрезентативном количестве и качестве.

Отдельно следует рассмотреть вопрос о сервисных возможностях калькулятора, которые должны быть достаточно развиты. Пользователю было бы удобно получать выходную информацию, скажем в виде, представленном на рис.2, где p- задаваемая пользователем вероятность восприятия сгенерированного им контента. Так он будет видеть направление совершенствования своего контента в плане достижения сетевого успеха.

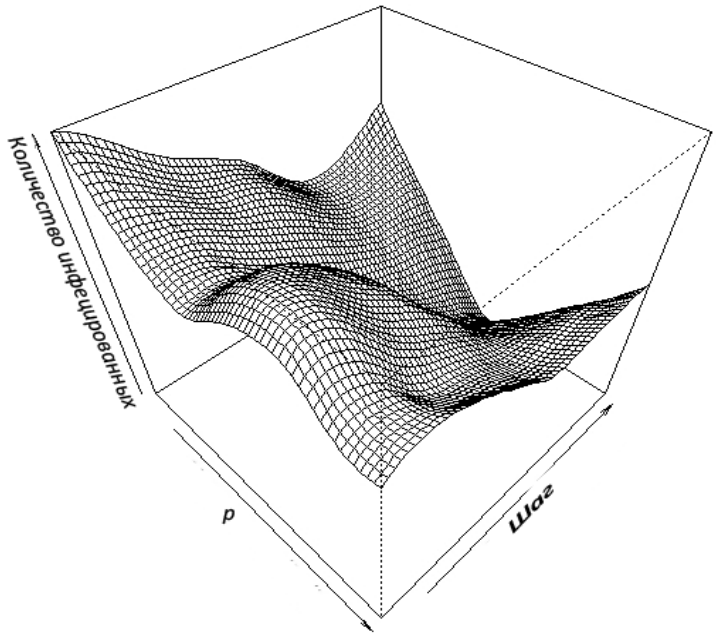

Рис. 2. Поверхность эпидемического процесса

В целом продукт следует рассматривать как результат реализации программы импортозамещения в контексте ограничений, вводимых на использование зарубежного программного обеспечения Постановлением Правительства Российской Федерации от 16.11.2015 №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». Учитывая тенденции импортозамещения и поддержки отечественного производителя, для современного российского рынка рассматриваемый продукт будет востребован также специалистами служб информационной безопасности, обеспечивающих мониторинг корпоративных и социальных сетей на предмет распространения деструктивной информации в защищенном пространстве.

Предлагаемый продукт имеет ярко выраженное и двойное применение – две задачи:

1. Анализ процессов распространения вредоносного контента в сети (вероятностная оценка риска);

2. Моделирование сетевого восприятия иных контентов (вероятностная оценка шанса).

Наиболее широкое применение предлагаемого продукта видится для решения второй задачи и именно в социальных сетях. Здесь имеет место:

- безмерное количество (миллионы и миллиарды) возможных потребителей продукта в лице пользователей соцсетей;
- устойчивая мотивация этих пользователей к обретению сетевого успеха в результате широкого и эффективного восприятия самостоятельно сгенерированного (авторского) контента, распространяемого в интересующей сети.

Каждый пользователь социальной сети хочет достичь популярности в ней, и он настойчиво ищет средства для достижения этой цели.

Причем здесь мало только предложить сети занимательный контент. Важно также знать, как он продвигается в сетевой инфраструктуре. А для этого необходим соответствующий инструментарий моделирования, учитывающий механизмы информационного обмена в ней.

Если предложить пользователю соцсети такой инструментарий со следующими потребительскими качествами:

- низкая цена (до 10$);
- возможность оперативного анализа в смартфоне (на основе ПО мобильного приложения);
- применимость ПО для исследования всевозможных действующих соцсетей;
- перспектива развития ПО в соответствии с прогрессом в области сетевых технологий;

- горизонт обновления инструментария с учетом совершенствования методологии генерирования распространяемого контента,

то десятки миллионов потребителей принесут инвестору миллиардную выручку периодическим обновлением продукта (систематическим пополнением выручки) в соответствии с новшествами научно-технического прогресса.

Это будет долгоиграющий проект, питающийся достижениями революционно развивающихся сфер информационно-кибернетической и информационно-психологической безопасности. Дельный инвестор, имеющий чутьё к экономической и, главное, имиджевой перспективе, очевидно, получит прибыль, ибо издержки продукта будут на порядки ниже его выручки, а перспектива его развития – необозримо широка (пока не включились конкуренты).

Привлекая для реализации проекта интеллектуально продвинутый научно-технический коллектив с достойным творческим потенциалом и ярко выраженной мотивацией профессионального и имиджевого роста, инвестор (на этом праве капитала и интеллекта) гарантировано получит коммерческий успех. Причем сроки разработки и внедрения продукта могут быть весьма скромными.

Участие в проектировании аспирантско-студенческой молодежи (аспирантско-студенческое инновационное бюро кафедры систем информационной безопасности ВГТУ), повально и самоотверженно увлеченной соцсетями, не только удешевит проектные работы, но и будет (своими восторженными информационными откликами) широко анонсировать их результаты, что несомненно позитивно скажется на популярности раздаваемого продукта.

Если прибавить к этому еще и звучное название будущего инструментария (например, «Калькулятор сетевого успеха»), то рекламная компания может быть достаточно продуктивной.

При этом, продвижение настоящего продукта в соцсетях станет многократно успешным с использованием наработок в борьбе с деструктивным контентом (секреты его распространения исследуются нашими параллельно в контексте «двойного применения», упомянутого выше).

Кстати говоря, в этом заключается особая специфика реализуемого проекта. Он будет несомненно осуществлен (не только благодаря, сколько вопреки) в России или за пределами.

Идея проекта и, особенно, реальная возможность его воплощения неслучайно возникли в научном коллективе, степень компетенции которого превышает мировую, прежде всего, в конкретной области сетевого риск/шанс анализа. В этом контексте привлечение универсальных программистов (особенно в долгосрочной перспективе) бесперспективно. Перманентное совершенствование (а проект, как уже отмечалось, явно долгоиграющий) возможно только с творчески растущими (параллельно с реализацией проекта) специалистами в дуальной реальности информационных рисков и шансов, включая адекватное управление ими.

Нужен прозорливый инвестор-патриот, для которого импортозамещение является сегодня не временной компанией, а стратегической дорогой к международному коммерческому успеху в важнейшем глобальном пространстве соцсетей, которое уже сейчас свергает правителей и перелицовывает целые государства.

Широкому потребителю достаточно сказать только одно: «Хочешь быть успешным - будь им, прежде всего, в популярных социальных сетях с использованием инструментария сетевого успеха».

Государство, лишающее себя и своих граждан такой возможности, обречено во многом проиграть «информационную войну». В этом заключается ещё и значение предлагаемого проекта. Он открывает очевидные перспективы позитивной коррекции общественного мнения через соцсети, однако это является предметом отдельного исследования (для другого заказчика). И этот поиск по силам авторскому коллективу настоящего проекта, плодотворно работающему над перестройкой теории сетей и сетевого противоборства. Именно фундаментальный подход в этой области делает самые практически значимые результаты на стыке методологических противоречий в оценке и регулировании рисков (первая задача) и шансов (вторая задача) распространения наполнителя в информационных (и не только информационных) сетях.

Литература

1. Остапенко, А.Г. Дискретные риск-модели развития информационных эпидемий в неоднородных информационно-телекоммуникационных сетях: многослойный риск-анализ / А.Г. Остапенко, Н.М. Радько, В.В. Исламгулова, Р.К. Бабаджанов, О.А. Остапенко // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – № 3. – С. 346-353.

2. Остапенко, Г.А. Информационные риски в социальных сетях / Г.А. Остапенко, Л.В. Паринова, В.И. Белоножкин, И.Л. Батаронов, К.В. Симонов. – Под ред. член-корр. РАН Д.А. Новикова. – 2013. – 161с.

3. Shvartskopf, E.A. Modeling of layering growth virus epidemic and spread of harmful content on Poisson networks / A.V Zaryaev, L. V. Parinova, and L. G. Popova // RES J PHARM BIOL CHEM SCI. - 2016. - Vol. 7. P. 2321-2331.

4. Гузев, Ю.Н. Топологическое многообразие сетей: структурно-функциональная классификация / Ю.Н. Гузев, Г.А. Остапенко, Е.Ю.

Чапурин // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – № 3. – С. 334-339.

5. Исламгулова, В.В. Дискретные риск-модели развития вирусных эпидемий в неоднородных информационно-телекоммуникационных сетях: разновидности эпидемических моделей и сетей / В.В. Исламгулова, Р.К. Бабаджанов, Н.М. Радько // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. - №4. – С. 476-479.

6. Новиков, Д.А. Информационные риски и эпистойкость безмасштабных сетей / Д.А. Новиков, А.Г. Остапенко, А.О. Калашников, О.А. Остапенко, Д.Г. Плотников, Е.С. Соколова, М.Ю. Уразов // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – №1. – С. 5-18.

7. Остапенко, Г.А. Основы топологического моделирования сетей: вершины, дуги и наполнитель / Г.А. Остапенко, Ю.Н. Гузев, Е.Ю. Чапурин // Информация и безопасность. – 2015. – Т. 18. – Вып.3 . – С. 322-329.

8. Исламгулова, В.В. Дискретные риск-модели развития вирусных эпидемий в неоднородных информационно-телекоммуникационных сетях: топологическое многообразие сетей в контексте их эпистойкости / В.В. Исламгулова, Р.К. Бабаджанов, Н.М. Радько // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – №4. – С. 480-483.

9. Остапенко, О.А. Дискретные риск-модели развития вирусных эпидемий в неоднородных информационно-телекоммуникационных сетях: микро-фрактал дискретной модели заражения / О.А. Остапенко, Н.М. Радько, В.В. Исламгулова, Р.К. Бабаджанов // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – № 4. – С. 472-475.

10. Соколова, Е.С. Риск-Анализ информационных эпидемий в социальных сетях с различным влиянием пользователей / Е.С. Соколова,

Ю.Н. Гузев, И.Л. Батаронов, В.И. Белоножкин // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – № 4. – С. 516-519.

11. Соколова, Е.С. Риск-Анализ информационных эпидемий в социальных сетях с различным влиянием пользователей / Е.С. Соколова, Ю.Н. Гузев, И.Л. Батаронов, В.И. Белоножкин // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – № 4. – С. 516-519.

12. Шварцкопф, Е.А. Моделирование эпидемического процесса заражения пользователей безмасштабной сети с учетом её топологии / Е.А. Шварцкопф, Ю.Н. Гузев, И.Л. Батаронов, В.И. Белоножкин, К.А. Разинкин // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. – № 4. – С. 520-523.

13. Исламгулова, В.В. Дискретные риск-модели развития вирусных эпидемий в неоднородных информационно-телекоммуникационных сетях: разновидности эпидемических моделей и сетей / В.В. Исламгулова, Р.К. Бабаджанов, Н.М. Радько // Информация и безопасность: Регион.науч.-техн. журнал. – Воронеж. 2015. - №4. – С. 476-479.

14. Губанов, Д.А. Модели информационного влияния и информационного управления в социальных сетях / Д.А Губанов, Д.А. Новиков, А.Г. Чхартишвили // Проблемы управления. – 2009. – №5. – С. 28-35.

15. Губанов, Д.А. Модели информационного влияния и информационного управления в социальных сетях / Д.А Губанов, Д.А. Новиков, А.Г. Чхартишвили // Проблемы управления. – 2009. – №5. – С. 28-35.

16. Губанов, Д.А. Модели распределенного контроля в социальных сетях / Д. А. Губанов, Д. А Новиков // Системы управления и информационные технологии. – 2009. – №37. – С. 124-129.

17. Губанов, Д.А. Социальные сети: модели информационного влияния, управления и противоборства: под ред. чл.-корр. РАН Д.А. Новикова / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили. – М.: ФИЗМАТ. – 2010. – 228 с.

18. Гузев, Ю.Н. Критерии оценки сетевого конфликта с учетом метрик взвешенных сетей / Ю.Н. Гузев, А.Л. Линец, Е.Ю. Чапурин // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова. – 2015. – Вып. 3 – С. 5-14.

19. Давыденко, В.А. Моделирование социальных сетей / В.А. Давыденко, Г.Ф. Ромашкина, С.Н. Чуканов // Журнал: Вестник Тюменского государственного университета – 2005. – № 1. – 12 с.

20. Brauer, F. Mathematical Models in Population Biology and Epidemiology / F. Brauer, C. Castillo-Chavez // Springer Science+Business Media, LLC – 2012. – P. 443-457.

21. Kumpula, J. M. Emergence of communities in weighted networks / J. M. Kumpula, J. P. Onnela, J. Saramaki, K. Kaski, J. Kertesz // Physical Review Letters. – Vol. 99. – 2007. – 5 p.

22. Зыков, А.А. Теория конечных графов / А.А. Зыков. – Новосибирск: Наука, 1969. – 543 с.

23. Barrat, A. The architecture of complex weighted networks / A. Barrat, M. Barthelemy, R. Pastor-Satorras, and A. Vespignani // Proc. Natl. Acad. Sci. – 2004. –P. 4-6.

24. Albert, R. Statistical mechanics of complex networks: Review of Modern Physics / R. Albert, A. L. Barabasi // Reviews of modern physics. – 2002. – Vol. 74. – 51 p.

25. Бусленко, Н.П. Моделирование сложных систем / Н.П. Бусленко. // М.: Наука, 1978. – С. 42-52.

26. Albert, L. Linked: The New Science of Networks / L. Albert, S. Barab //Albert-Laszlo Barabasi – 2002. – P. 41-55.

27. Алексеев В.Е. Графы. Модели вычислений. Структуры данных / В.Е. Алексеев, В.А. Таланов // Издательство Нижегородского госуниверситета. – 2004. – С. 10-12.

28. Зыков, А.А. Теория конечных графов / А.А. Зыков. – Новосибирск: Наука, 1969. – 543 с.

Воронежский научно-образовательный центр управления информационными рисками

УДК 004.506

СЕТЬ СОЦИАЛЬНЫХ ЗАКЛАДОК BIBSONOMY: СТРУКТУРНО – ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ АНАЛИЗА ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ КОНТЕНТА

Е.С. Соколова, В.В. Колмаков, А.В. Паринов, Е.А. Москалева, Н.Н. Толстых, С.С. Куликов

Социальная сеть закладок - это сеть, которая построена по принципам связи людей, интересующихся схожей информацией в одной и той же области. Ключевым здесь является публикация статей, заметок. Социальная сеть Bibsonomy – научно публицистическая социальная сеть, основанная на сборе научных статей[1].

Анализ социальной сети предусматривает выявление признаков для составления классификации, в которой ресурсы можно разделить по принадлежности коллективного или персонального пользования. В коллективных ресурсах контент размещается или потребляется группой пользователей. В персональных ресурсах он размещается каждым субъектом сети отдельно и для каждого пользователя индивидуально. Соответствующая классификация изображена на рисунке 1.

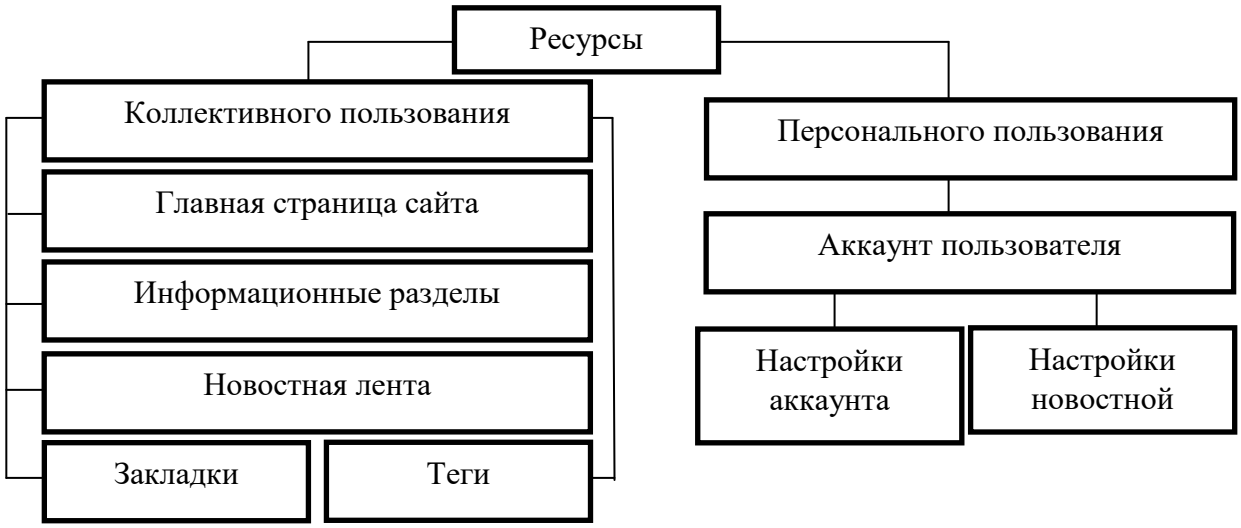

Рис.1. Классификация ресурсов социальной сети Bibsonomy

Ресурсы данной социальной сети состоят из 2 больших подгрупп – коллективного и персонального пользования [2].

Ресурсы коллективного пользования делятся на:

-главная страница сайта;

-информационные разделы;

-новостная лента;

-закладки;

-теги.

Ресурсы персонального пользования представлены аккаунтом пользователя, который, в свою очередь, делится на настройки аккаунта и настройки новостной ленты. Контент – это информационно значимое наполнение ресурса социальной сети[3].

Представим классификацию контента на рисунке 2, которая осуществлена по признаку различной типизации файлов, являющейся специфической для рассматриваемой социальной сети [4].

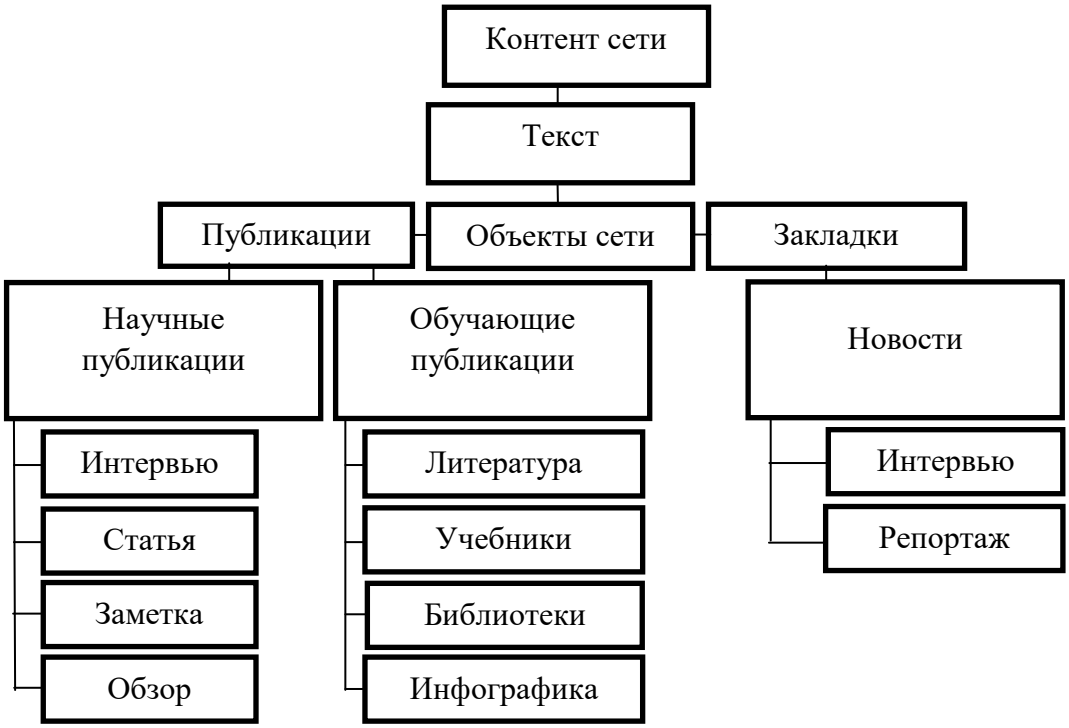

Рис. 2. Классификация контента, циркулирующего в социальной сети

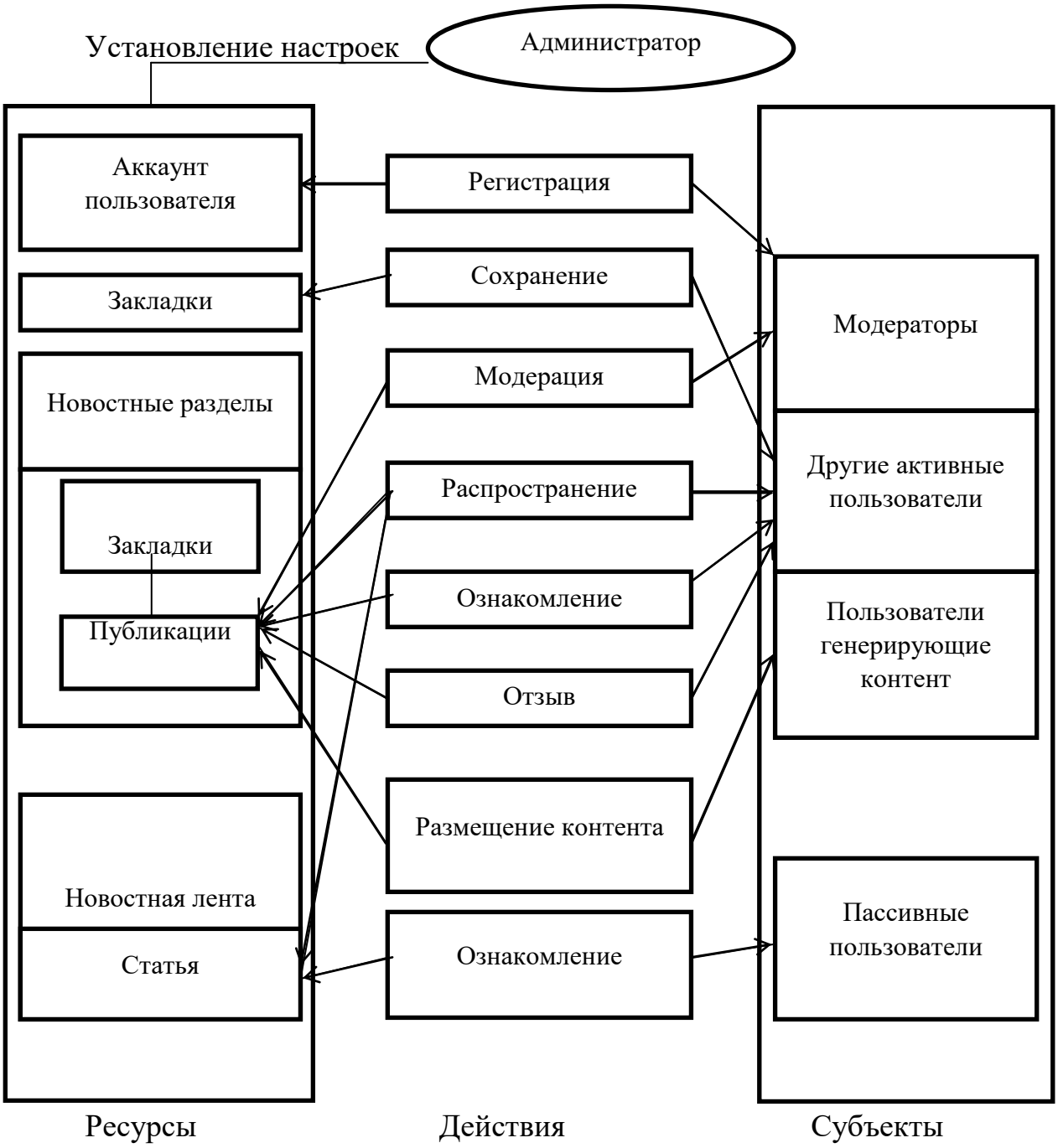

Рис. 3. Структурно – функциональная схема сети

Контент, циркулирующий в социальной сети представляет собой статьи, публикации, заметки. Необходимым элементом для анализа социальной сети Bibsonomy является нахождение взвешенных метрик. Статистические данные социальной сети Bibsonomy показаны в (таблице 1). Данные представляют в виде трехместного предиката, в котором на

первом месте располагается узел сети, из которого исходит ребро, подтверждающее связь между пользователями сети. На втором месте – узел, в который входит это же самое ребро, а на третьем – вес ребра, отражающий силу связи между вершинами [5].

Таблица 1 – Фрагмент трехместного предиката социальной сети Bibsonomy.

Идентификатор истока вершины	Идентификатор стока вершины	Вес дуги
1	2	1
1	3	5
1	4	5
1	5	1
1	6	1
7	8	2
7	10	1

Формат данных в этом предикате соответствует следующей формуле (1):

$$\Gamma(x_i, x_j, a_{ij}) \Leftrightarrow \Gamma(i, j, \delta(a_{ij})), \quad (1)$$

где i и j – номера вершин x_i и x_j в сети;

$\delta(a_{ij})$ - вес дуги a_{ij}, связывающей x_i и x_j, и направленной от i к j;

В данном случае весом дуги $\delta(a_{ij})$ является динамический ресурс, то есть передача контента определенного объема V и его ценности C в сети в единицу времени по формуле (2):

$$\delta(a_{ij}) = \frac{\partial[CV]}{\partial t} = \langle C \rangle V', \quad (2)$$

где $\langle C \rangle$ – усредненная ценность наполнителя (контента);

V' – интенсивность обмена контентом [6].

В социальной сети закладок Bibsonomy весом дуги будет являться количество совместных написанных статей.

Суть алгоритма преобразования исходных данных социальной сети Bibsonomy заключается в построении трехместного предиката сначала в виде звездной матрицы и затем в виде матрицы взвешенной центральности. На основе предложенного алгоритма преобразования исходных данных сети построим звездную матрицу социальной сети Bibsonomy (таблица 2).

Таблица 2 – Звездная матрица социальной сети Bibsonomy

Номер вершины	1	2	3	4	5	-	11	12	13	14	15	-	21	22	23	18890
1	-	3	8	2	8	-	7	0	0	0	0	-	4	5	8	0
2	0	-	1	5	0	-	0	7	5	3	1	-	4	0	0	6
3	0	0	-	0	0	-	0	4	2	0	0	-	3	5	3	2
4	0	0	0	-	0	-	0	5	0	0	0	-	0	0	3	0
5	0	0	0	0	-	-	0	0	7	0	4	-	0	0	0	0
-	-	-	-	-	-	-	0	1	3	5	0	-	2	0	0	0
11	0	0	0	0	0	0	-	0	3	0	11	-	0	0	7	0
12	0	0	0	0	0	0	0	-	0	0	0	-	0	1	0	0
13	0	0	0	0	0	0	0	0	-	3	0	-	5	0	0	0
14	0	0	0	0	0	0	0	0	0	-	0	-	0	7	2	0
15	0	0	0	0	0	0	0	0	0	0	-	-	0	0	9	0
-	-	-	-	-	-	-	-	-	-	-	-	-	5	0	6	5
21	0	0	0	0	0	0	0	0	0	0	0	0	-	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	-	1	3
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-	1
18890	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-

На втором шаге данного алгоритма определим количество исходящих дуг (степень исхода) для каждого узла социальной сети. Данная матрица будет необходима для последующих процедур моделирования процессов диффузии контента в социальной сети (таблица 3).

Таблица 3 – Диагональная матрица степеней вершин сети

Номер вершины	1	2	…	10	11	…	20	21
1	6	-	…	-	-	…	-	-
2	-	10	…	-	-	…	-	-
…	…	…	…	-	-	…	-	-
10	-	-	-	214	-	…	-	-
11	-	-	-	-	18	…	-	-
…	…	…	…	…	…	…	-	-
20	-	-	-	-	-	-	53	-
21	-	-	-	-	-	-	-	73

На третьем шаге алгоритма предлагается построить квадратную матрицу взвешенной центральности элементов сети по формуле (3) . Для этого необходимо определить удельный вес ее вершин и дуг с помощью нормировки их весов по суммарному трафику сети по следующей формуле:

$$\delta(\bar{a}_{ij}) = \delta(a_{ij}) / \sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}), \quad (3)$$

где $\delta(a_{ij})$ – вес трафика в дуге a_{ij}. Данная формула будет характеризовать степень взвешенной (по трафику) центральности дуги. Однако следует заметить, что суммарный трафик сети не разделяет входящие и исходящие дуги. Поэтому для определения взвешенной

центральности вершины x_s можно использовать сумму которую далее следует пронормировать в формуле (4) по суммарному трафику сети:

$$\sum_i \delta(a_{si}) + \sum_j \delta(a_{js}). \quad (4)$$

В результате получим нормированную величину, которая будет характеризовать удельный вес трафика, проходящего через вершину x_s, по отношению ко всему трафику сети по формуле (5):

$$\delta(\bar{x}_s) = \left[\sum_i \delta(a_{si}) + \sum_j \delta(a_{js})\right] / \sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}), \quad (5)$$

где $\delta(a_{si})$ – вес трафика в исходящей и узла a_{si} дуге;

$\delta(a_{si})$ – вес трафика во входящей в узел a_{js} дуге

В итоге, следуя формуле (5), получим матрицу взвешенной центральности элементов исходной сети следующего вида (таблица 4).

Таблица 4 - Матрица взвешенной центральности социальной сети Bibsonomy

Номер вершины	1	2	3	4	5	…	18890
1	0.032922	-	-	-	-	…	-
2	-	0.036594	-	-	-	…	-
3	-	-	0.033576	-	-	…	-
4	-	-	-	0.025980	-	…	-
5	-	-	-	-	0.231136	…	-
…	…	…	…	…	…	…	-
18890	-	-	-	-	-	-	0.00452

Последний этап заключается в нахождении и построении диагональной матрицы удельного баланса трафика в вершинах социальной

сети Bibsonomy [7-8]. На данном этапе будет учитываться не сумма, а разность исходящего и входящего для вершины трафиков в формуле (6) :

$$\delta(\bar{B}_s) = \left[\sum_i \delta(a_{si}) - \sum_j \delta(a_{js})\right] / \sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}), \quad (6)$$

где: $\delta(a_{si})$ – вес трафика в исходящей и узла a_{si} дуге;

$\delta(a_{si})$ – вес трафика во входящей в узел a_{js} дуге.

В результате данных вычислений получим диагональную матрицу удельного баланса трафика в вершинах сети (таблица 5).

Полученная удельная величина характеризует роль вершины (субъекта) сети:

- при $\bar{B}_s > 0$ – это генератор контента;

- при $\bar{B}_s < 0$ – это аккумулятор контента.

Чем больше модуль $\bar{B}_s$, тем в большей степени проявляется его ролевая функция.

Таблица 5 - Матрица удельного баланса трафика в вершинах социальной сети Bibsonomy

Номер вершины	1	2	3	4	5	…	18890
1	0.00095	-	-	-	-	…	-
2	-	-0.0004	-	-	-	…	-
3	-	-	-0.00015	-	-	…	-
4	-	-	-	-0.00004	-	…	-
5	-	-	-	-	-0.00014	…	-
…	…	…	…	…	…	…	
18890	-	-	-	-	-		0.00000012

Далее следует преобразовать всю сеть в некоторую выборку сети, которая в полной мере описывает и отражает все основные её свойства. Данный подход заключается в отборе вершин по их степени, то есть

количеству инцидентным им дуг. Однако он не учитывает тот факт, что каждая дуга имеет свой вес. Таким образом, отсутствует взвешенная оценка с точки зрения трафика. Суть алгоритма в том, что требуется из полученных квадратных матриц взвешенности, получить усеченное количество узлов, способных с сохранением подобия описать исходную сетевую структуру. Поэтому в предложенном алгоритме уместно использование квадратной матрицы взвешенной центральности элементов сети, а точнее – ее диагонали, где определена степень взвешенной центральности каждой вершин.

Таблица 6 – Степени взвешенной центральности вершин

Номер узла	Степень	Номер узла	Степень
1	0,00007672	22	0,00000491
2	0,00011416	23	0,00002578
3	0,00002271	24	0,00000798
4	0,00009391	25	0,00000982
…	…	…	…
20	0,00006261	18890	0,00000307
21	0,00000184	18891	0,00000184

На втором этапе данного алгоритма необходимо проранжировать степени узлов матрицы по убыванию (таблица 7).

Таблица 7 – Проранжированные степени взвешенной центральности вершин

Номер узла ранжирован-ной выборки	Номер узла усечённой выборки	Степень	Номер узла ранжирован-ной выборки	Номер узла усечённой выборки	Степень
1	3780	0,03105	8	12445	0,01028
2	6574	0,02988	9	7324	0,01009
3	8965	0,02822	10	9753	0,00850
4	9900	0,02413	11	14769	0,00803
5	10235	0,02245	12	12747	0,00749
6	11850	0,01842	…	…	…
7	3406	0,01537	340	4290	0,00001

На следующем этапе просуммируем полученные значения до получения необходимого результата (точности модели), т.е. до значения 0.95. Так как для нас допустима 5% потеря трафика, полученная сумма должна быть не меньше 0,95. Этим критерием и ограничится репрезентативная (с точки зрения трафика) выборка:

$$\delta(\bar{x}_s) = 0{,}03292253521127 + 0{,}03659456740443 + 0{,}03357645875252 + \cdots +$$
$$0{,}0004527162 + 0{,}00042756539235 + \cdots + 0{,}001365 = 0{,}9515.$$

При данном суммировании получили выборку из 340 элементов.

Далее, обнулив столбцы и строки, на пересечении которых стояла исключенная вершина, построим матрицу (таблица 8).

Таблица 8 – Усеченная матрица социальной сети bibsonomy

Номер вершины	3780	6574	8965	9900	11650	12445	13850	…	18891
3780	-	0	0	0	0	0	2	…	0
6574	0	-	13	0	34	1135	0	…	46
8965	0	0	-	0	0	0	0	…	0
9900	0	0	0	-	0	0	25	…	0
11650	0	0	0	0	-	0	0	…	0
12445	0	0	0	0	0	-	0	…	3
13850	0	0	8	0	0	0	-	…	0
…	…	…	…	…	…	…	…	…	0
18891	0	0	0	0	0	0	0	…	-

Для сравнения рассмотрим генеральную совокупность взвешенной мощности социальной сети и взвешенную мощность сети на конечном этапе и определим коэффициент среднеквадратичного отклонения. Выборка должна обладать репрезентативностью, распространяющую полученные выводы на генеральную совокупность.

Определение репрезентативности состоит из расчета средних показателей генеральной совокупности и распределения выборочных значений[9].

Рассчитаем среднеквадратическое отклонение для элементов генеральной совокупности и выборки по формуле (7):

$$D_x = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2, \quad (7)$$

где D_x – дисперсия, x_i-i-й элемент выборки, $\bar{x}$-среднее арифметическое выборки, N – объем выборки. Исходя из формулы (7) расчета дисперсии генеральной совокупности и репрезентативной выборки, найдем СКО:

$$S = \sqrt{\frac{\sum_{i=1}^{n}(X_i - \bar{X})^2}{n}} = \sqrt{D_x}, \quad (8)$$

где $S_{ГС} = 0{,}00136642$, $S_{РВ}$=0,00129984 – СКО генеральной совокупности и репрезентативной выборки. Вычислим коэффициент среднеквадратичного отклонения по формуле (9):

$$\alpha = \frac{S_{ГС} - S_{РВ}}{S_{ГС}}. \quad (9)$$

В результате (9) получим, что коэффициент среднеквадратичного отклонения α = 13,230 . Из этого можно сделать вывод, что выборки подобны. Покажем это соотношение на графике (рисунок 4).

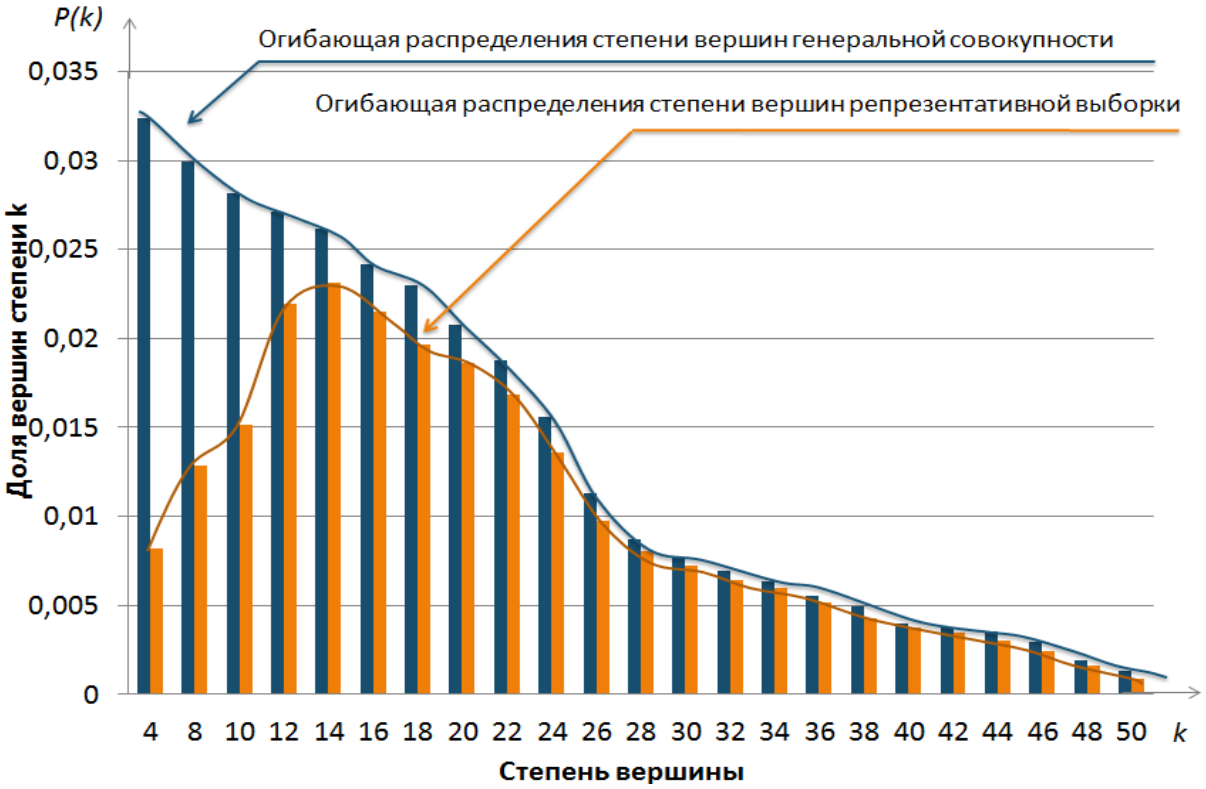

Рис. 4. Гистограмма распределения степеней вершин

Таким образом, для построения структурно-функциональной модели распространения контента в социальной сети были: рассмотрены ресурсы социальной сети, проведена классификация контента сети, выявлены субъекты социальной сети, классифицированы действия субъектов социальной сети. Также были построены матрицы и получена визуальная модель усеченной социальной сети, просчитано среднеквадратичное отклонение генеральной совокупности и репрезентативной выборки.

На основе полученной статистики построим усеченный граф исследуемого участка социальной сети Bibsonomy при помощи

программного обеспечения Gephi [10]. Полученные результаты представлены рисунком 5.

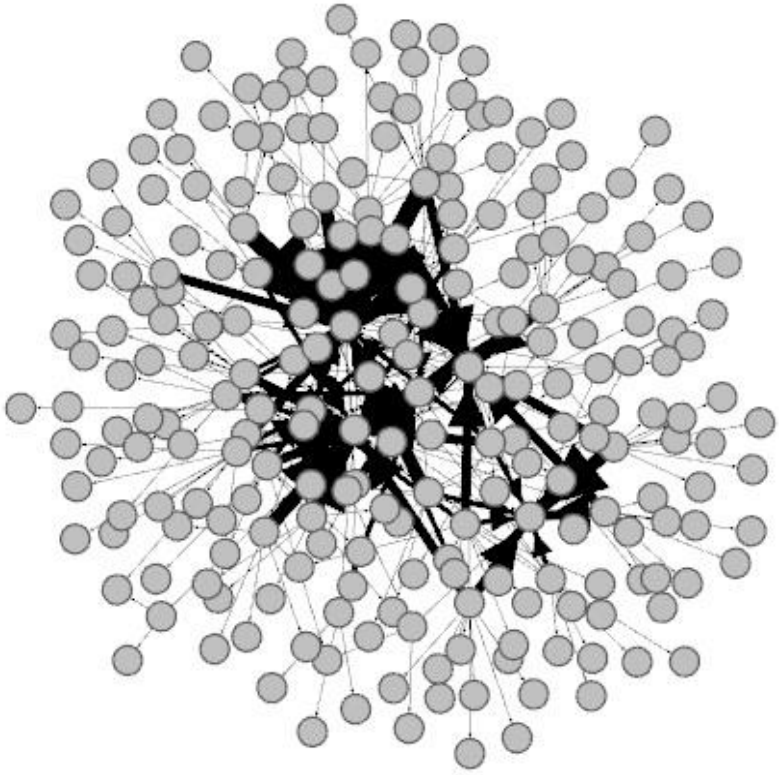

Рис.5. Выборка социальной сети Bibsonomy

Стоит отметить, что у данной социальной сети явная кластерность не прослеживается. Это напрямую зависит от возможностей авторизованных пользователей – любой авторизованный пользователь может прочесть любую статью, прокомментировать ее и сохранить к себе в закладки. При этом в данной сети нет групп, в которые пользователи могут объединять для обсуждения интересующих их вопросов. В социальной сети все ресурсы и контент общедоступны. Последний этап алгоритма состоит в формировании итоговой матрицы в виде, удобном для последующего моделирования информационной диффузии. Данная матрица выглядит следующим образом:

- недиагональные элементы равны ±1, так как интересует лишь факт смежности вершин истоков (+1) и стоков (-1) [11-14]. В некоторой степени это возврат к формату матрицы смежности;

- диагональные элементы имеют вес *k*, равный сумме элементов (+1) столбца. Отсюда определяется ожидаемое количество вирусованных контентом элементов [9].

Таблица 9 – Модифицированная матрица смежности социальной сети Bibsonomy

Номер вершины	2	3	5	250	300	…	340
2	17	0	1	0	0	…	1
3	0	24	0	1	0	…	0
5	0	0	52	0	1	…	1
250	0	0	0	3490	1	…	1
300	0	0	0	0	34	…	0
…	…	…	…	…	…	…	1
340	0	0	0	0	0		84

Таким образом, проанализировав структурно-функциональную особенность распространения контента в социальной сети Bibsonomy, можно достичь главной цели исследования, которая состоит в оценке и регулировании рисков, возникающих в сети в случае распространения в ней деструктивного контента. Для этого в дальнейшем необходимо решить ряд задач [15]:

1. Используя построенную макро-модель сети Bibsonomy, промоделировать сетевой эпидемический процесс[16];

2. Управление рисками с учетом определенного вероятного ущерба информационной эпидемии по суммарному весу, метрик, матриц смежности, взвешенности и послойной внутрисетевой связанности [17-21].

Литература:

1. Бреер В.В., Стохастические модели социальных сетей / В.В. Бреер; Управление большими системами., № 27.. Типография МГУ, 2010 - С. 169-204.

2. Назарчук А.В., О сетевых исследованиях в социальных науках МГУ им. М. В. Ломоносова - М:. Типография МГУ, 2008. – 73 с.

3. 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

4. Bibsonomy // neural. Дата обновления: 23.08.2016. URL: http://www.neural.ru/dictionary/Bibsonomy%20Trust%20Metric (дата обращения: 23.10.2016).

5. Анализ сайта Bibsonomy.org a.pr-cy. // Дата обновления: 24.08.2016. URL: https://a.pr-cy.ru/ Bibsonomy.org/ (дата обращения: 17.09.2016).

6. Монахов Ю.М., Моделирование распространения нежелательной информации в социальных медиа / Ю.М. Монахов, К.Г. Абрамов; Вестник КГУ им. Н.А. Некрасова.- 2011. – Т.17, №3. - С. 15-18.

7. Абрамов К. Г., Моделирование распространения нежелательной информации в социальных медиа / К.Г. Абрамов, Ю.М. Монахов; Труды XXX Всероссийской научно-технической конференции. Проблемы эффективности и безопасности функционирования сложных технических и информационных систем / Серпуховский ВИ РВ. - 2011. – ч. IV. - С. 178-182.

8. Kalashnikov, A.O. Attacks to information and technological infrastructure of crucial objects: assessment and regulation of risks: Monograph / A.O. Kalashnikov, E. V. Yermilov, O. N. Choporov, K. A. Razinkin, N. I.

Barannikov; under the editorship of the Member correspondent of RAS D. A. Novikov. - Voronezh: Scientific Book publishing house. 2013. - 160 p.

9. Статистика социальной сети bibsonomy. - Электрон. Дан. – Режим доступа: http://konect.uni-koblenz.de/networks/bibsonomy. (дата обращения 4.09.2016)

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

11. 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 Journal. – 2013. – 25 (3). – P. 410-415.

12. 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.

13. 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.

14. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.

15. 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.

16. 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. – P. 142-151.

17. Sybil-Resilient Online Content Rating Dinh Nguyen Tran, Bonan Min, Jinyang Li, Lakshminarayanan Subramanian, Courant Institute of Mathematical Sciences, New York University.

18. Caldarelli G. Scale-Free Networks. Complex Webs in Nature and Technology / G. Caldarelli / Cambridge University Press, 2007. – P. 45-51.

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

20. N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev. Peak risk assessing the process of information epidemics expansion. Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251. A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik. Flood-attacks within the hypertext information transfer protocol: damage assessment and management. Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.

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

Региональный учебно-научный центр по проблемам информационной безопасности

Воронежский научно-образовательный центр управления информационными рисками

УДК 004.056

СОЦИАЛЬНАЯ СЕТЬ YOUTUBE: СТРУКТУРНО – ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ РАСПРОСТРАНЕНИЯ КОНТЕНТА

В.В. Роженко, Д.А. Савинов, О.В. Поздышева,
В.И. Белоножкин, В.Н. Деревянко, Д.О. Карпеев, К.А. Разинкин

YouTube — видео хостинг, предоставляющий пользователям услуги хранения, доставки, показа и монетизации видео [31]. Она конкурирует с телевидением.

Задача сети – обеспечить бесплатное и удобное распространение видео контента как внутри самой сети, так и за её пределами [31].

Социальная сеть – сообщество людей, связанных общими интересами, общим делом или имеющих другие причины для общения между собой [23]. В Интернете – это сложноустроенный программный сервис, который является инструментом для обмена между пользователями любыми данными, например, сообщениями, мультимедиа, рекомендациями, новостями и другим контентом [23].

Сетевые ресурсы социальной сети – это программное, техническое и организационное обеспечение информационной сети, предназначенное для решения прикладных задач [24].

Все сетевые ресурсы социальной сети YouTube делятся (рис. 1) на закрытые (аккаунт пользователя и данные аккаунта модератора) и открытые (новостная лента, форум, страницы канала и страница оформления жалоб и предложений).

Персональные ресурсы (закрытые) пользователя (личный профиль каждого зарегистрированного пользователя) являются

конфиденциальными. Допуск к таким данным имеет только непосредственный владелец профиля.

Ресурсы коллективного пользования (открытые) просмотреть и прочитать может и зарегистрированный, и незарегистрированный пользователь данной сети, однако размещать видеоконтент и оценивать его разрешено только после авторизации в YouTube [24].

Для наибольшей наглядности ресурсы социальной сети YouTube представим на рисунок 1.

Рис. 1. Классификация сетевых ресурсов социальной сети YouTube

Для данной социальной сети представление контента актуально в трех формах: видео, текстовом и гибридном (рис. 2).

Большую часть в сети занимает видеоконтент, т.е. более 95% всей циркулирующей информации. Оставшиеся 5% - доля текстовой и гибридной информации.

Видео контент включает в себя множество различных видов. Это видеозаписи информационного характера, развлекающие видео, летс-плеи, «живое» видео, скринкасты, рисованное видео и видео-презентации.

Текстовый контент включает в себя: комментарии, опросы, текстовую рекламу, подпись и обсуждения на форуме.

Под гибридным контентом будем понимать контент, полученный вследствие сочетания двух или более различных форм контента [29].

Рис. 2. Классификация содержания контента социальной сети YouTube

С учетом всей известной информации и статистики для субъектов (рис. 3) социальной сети YouTube проведем классификацию по двум критериям: активные и пассивные субъекты. В свою очередь пассивных пользователей можно разделить на пользователей прошедших регистрацию и гостей социальной сети YouTube.

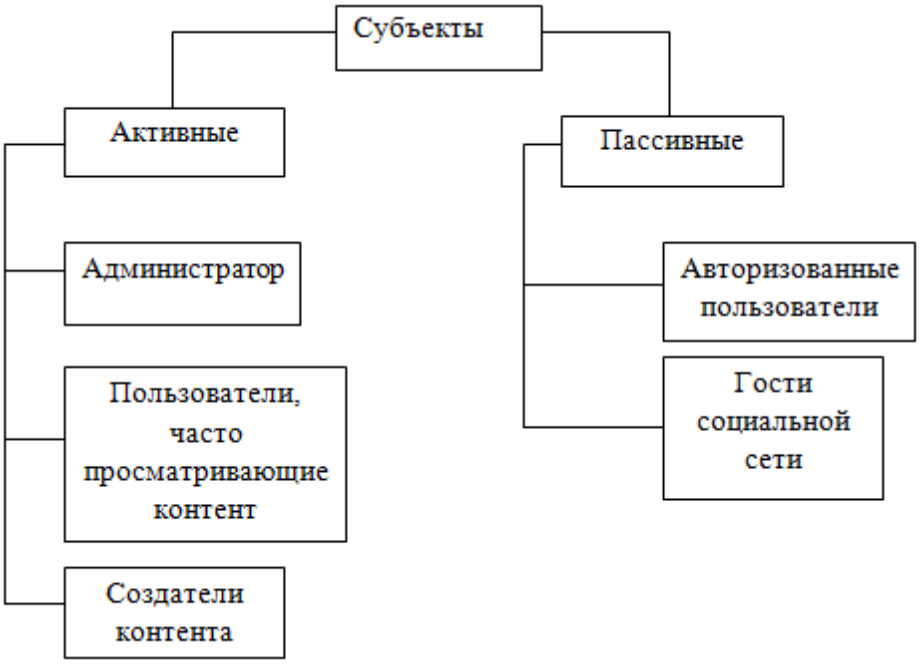

Рис. 3. Классификация объектов, создаваемых в ресурсах сети YouTube

Действия (рис. 4) в социальной сети YouTube могут быть двух типов: управленческие и пользовательские. К управленческим действиям относится модерация, настройка канала. Пользователь может подстроить канал так, как ему удобно. Так же пользователь, наделенный управленческими полномочиями, контролирует саму социальную сеть, отвечает на вопросы других пользователей и решает появившиеся проблемы [32].

Пользовательские действия делятся на доступные только авторизованным пользователям действия и доступные неавторизованным пользователям действия. В свою очередь авторизованные пользователи могут производить в сети YouTube такие действия как: загрузка и

публикация контента, сохранение контента, добавление, комментирование, оценивание, распространение. Так же авторизованный пользователь может отправить жалобу, если ему не понравится что-либо в данной сети.

Рис. 4. Классификация действий субъектов в социальной сети YouTube

Соответственно структурно-функциональная схема сети представлена на рисунке 5.

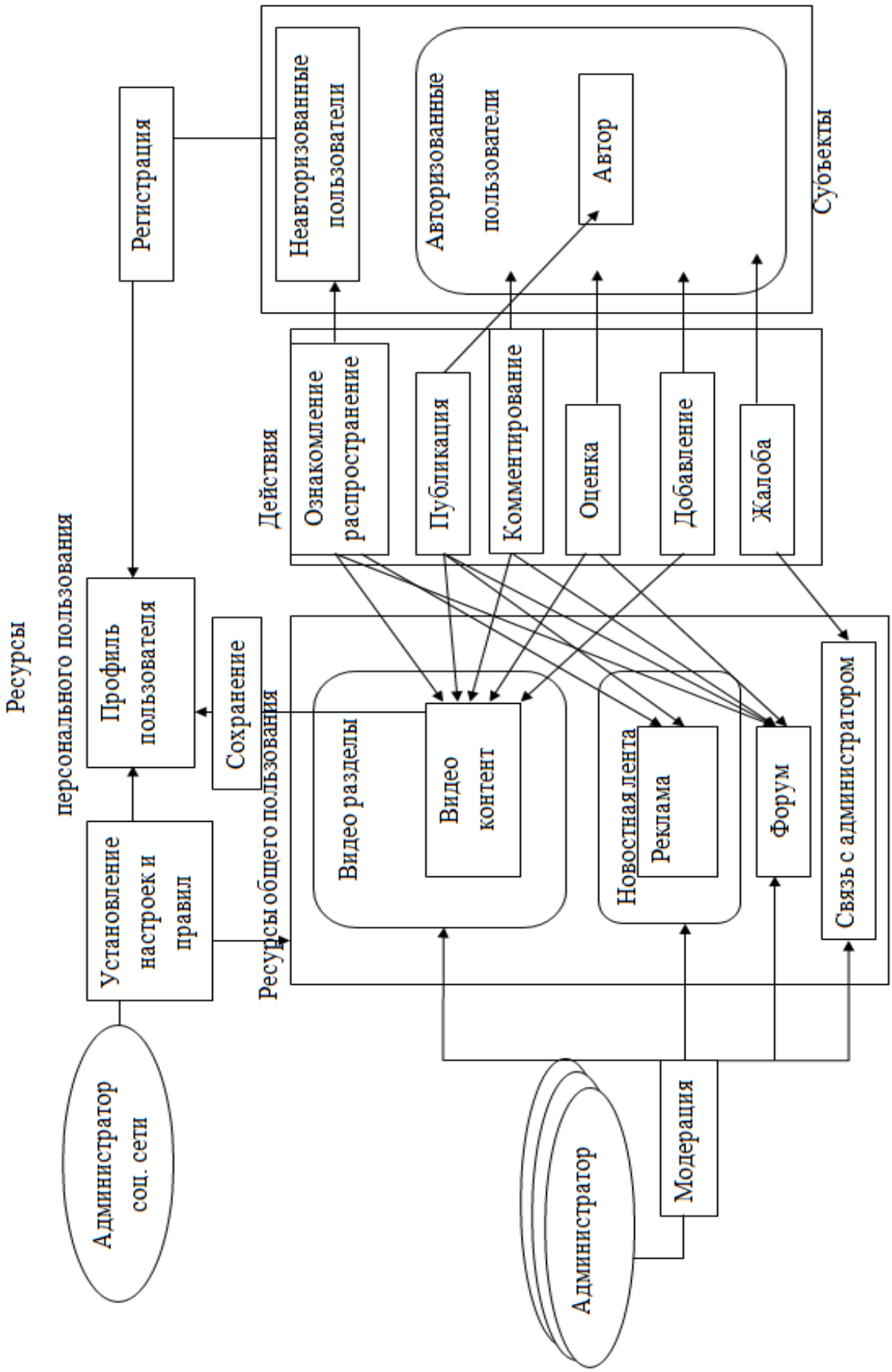

Рис. 5. Структурно-функциональная схема социальной сети YouTube

Для того чтобы перейти к представлению статистических данных в виде матрицы взвешенности рассмотрим понятие трехместного предиката на основе статистики сети YouTube. Трехместный предикат для социальной сети YouTube будет иметь вид *(x y z)*, *x* и *y* - смежные вершины, *z* - вес инцидентного ребра для вершин *x* и *y*.

Рассмотрим статистические данные социальной сети YouTube [35]. Данная сеть является ориентированной и состоит из 12492 вершин. Т.к. данный предикат состоит из 65188 строк, изобразим только некоторую его часть для наглядности в таблице 1, где вес вершины обозначает суммарное количество информации, прошедшей через определенную вершину.

Таблица 1 – Фрагмент трехместного предиката социальной сети YouTube

Идентификатор первой вершины	Идентификатор второй вершины	Вес вершины
1	0	4
2	5	0
14	1	2
16	25	15
35	13	2
41	3	3
46	4	8
50	6	9
55	11	3

Суть преобразования исходных данных социальной сети YouTube заключается в построении звездной матрицы и затем в виде матрицы взвешенной центральности [33].

На основе предложенного алгоритма преобразования исходных данных сети построим звездную матрицу социальной сети YouTube, элементы строки которой соответствуют дугам, входящим в данную вершину, а элементы столбца – дугам, исходящим из вершины (табл. 2):

Таблица 2 – Звездная матрица для социальной сети YouTube

№ узла / № узла	1	2	3	.	18	19	20	.	100	101	102	.	12492
1	-	5	4	.	0	0	0	.	2	0	0	.	0
2	1	-	0	.	0	3	0	.	0	5	0	.	0
3	0	0	-	.	0	0	0	.	0	3	0	.	0
⋮	.	.	.	-	.	.	.	.	.	.	.	.	.
18	0	0	0	.	-	0	0	.	0	0	2	.	0
19	0	3	0	.	0	-	0	.	0	4	0	.	0
20	0	0	0	.	0	0	-	.	0	0	1	.	0
⋮	.	.	.	.	.	.	.	-	.	.	.	.	.
100	0	0	0	.	0	0	0	.	-	0	0	.	0
101	0	0	0	.	0	0	0	.	0	-	2	.	0
102	0	0	0	.	0	0	0	.	0	2	-	.	1
⋮	.	.	.	.	.	.	.	.	.	.	.	-	
12492	0	0	0	.	0	0	0	.	0	0	0	.	-

На втором шаге определим количество исходящих дуг (степень исхода) для каждого узла социальной сети. Данная матрица будет необходима для последующих процедур моделирования процессов диффузии контента в социальной сети (табл. 3).

Таблица 3 – Диагональная матрица степени вершин сети YouTube

№ узла	1	2	3	4	5	6	-	12491	12492
1	3	0	0	0	0	0	-	0	0
2	0	2	0	0	0	0	-	0	0
3	0	0	4	0	0	0	-	0	0
4	0	0	0	6	0	0	-	0	0
5	0	0	0	0	1	0	-	0	0
6	0	0	0	0	0	15	-	0	0
-	-	-	-	-	-	-	-	-	-
12490	0	0	0	0	0	0	-	1	0
12491	0	0	0	0	0	0	-	5	0
12492	0	0	0	0	0	0	-	0	11

На третьем шаге построим квадратную матрицу взвешенной центральности элементов сети [33]. Для этого нужно нормировать веса узлов по сумме весов всех дуг сети, т.е. – по суммарному трафику сети (1),

$$\sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}). \quad (1)$$

Тогда нормированная величина, полученная с помощью выражения (1), будет показывать удельный вес трафика в дуге a_{ij} к сумме всего трафика сети

$$\delta(\bar{a}_{ij}) = \delta(a_{ij}) / \sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}). \quad (2)$$

Выражение (2) будет характеризовать степень ее взвешенной центральности (по трафику). Следует заметить, что суммарный трафик сети не разделяет входящие и исходящие дуги. Поэтому для определения взвешенной центральности вершины x_s можно использовать сумму, которую далее следует нормировать по сумме всего трафика сети

$$\sum_i \delta(a_{si}) + \sum_j \delta(a_{js}). \quad (3)$$

Из выражения (3) получим нормированную величину, которая будет характеризовать удельный вес трафика, проходящего через вершину x_s, по отношению ко всему трафику сети (4). Такова будет степень взвешенной центральности данной вершины

$$\delta(\bar{x}_s) = \left[\sum_i \delta(a_{si}) + \sum_j \delta(a_{js})\right] / \sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}). \quad (4)$$

Следуя формуле (3), можно получить квадратную матрицу взвешенной центральности элементов исходной сети. В таблице 4 продемонстрированы ключевые вершины.

Таблица 4 – Матрица взвешенной центральности для сети YouTube

№ узла / № узла	4879	283	3	2145	1345	573	945	12492
4879	0,0045	0	0	0	0	0	0	0
283	0	0,0028	0.0031	0	0	0		0
3	0	0.00023	0,0019	0	0	0	0	0
2145	0	0	0	0,000045	0	0	0	0
1345	0	0	0	0.00029	0,000045	0	0	0
573	0	0	0	0	0	0,000045	0	0
945	0	0	0	0	0	0.000348	0,000022	0
12492	0	0	0	0	0	0	0	0,000022

Следующий этап – построение диагональной матрицы удельного баланса трафика в вершинах сети (табл. 5). Здесь учитывается не сумма, а разность исходящего и входящего для вершины трафиков (5):

$$\delta(\bar{B}_s) = \left[\sum_i \delta(a_{si}) - \sum_j \delta(a_{js})\right] / \sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij}). \qquad (5)$$

Полученная удельная величина будет характеризовать, какую роль данная вершина (субъект) занимает в социальной сети.

Таблица 5 – Диагональная матрица удельного баланса трафика в вершинах сети YouTube

№ узла / № узла	1	2	3	.	4879	4880	4881	.	12491	12492
1	0,0026	0	0	.	0	0	0	.	0	0
2	0	0,0012	0	.	0	0	0	.	0	0
3	0	0	0,0019	.	0	0	0	.	0	0
.	.	.	.	-	.	.	.	.	.	.
4879	0	0	0	.	0,000045	0	0	.	0	0

Продолжение таблицы 5

4880	0	0	0	.	0	0,000045	0	.	0	0
4881	0	0	0	.	0	0	0,000045	.	0	0
.	.	.	.	.	.	.	.	.	.	.
12491	0	0	0	.	0	0	0	.	0,000022	0
12492	0	0	0		0	0	0	…	0	0,000022

Так как социальная сеть достаточно велика и включает в себя более десяти тысяч вершин, что затрудняет ее анализ, следует преобразовать всю сеть в некоторую её выборку, которая в полной мере отражает все основные свойства сети.

Данный подход заключается в отборе вершин по их наибольшей степени, то есть количеству инцидентным им дуг. Фактически требуется из полученных квадратных матриц взвешенности получить усеченное множество узлов, которые способны с сохранением подобия описать исходную сетевую структуру.

Поэтому в предложенном алгоритме уместно использование квадратной матрицы взвешенной центральности элементов сети, а точнее – ее диагонали, где определена степень взвешенной центральности каждой вершины.

Таблица 6 – Ранжированная матрица взвешенной центральности сети YouTube

№ узла / № узла	1	2	3	…	4879	4880	4881	…	12491	12492
1	0	0,0028	0	…	0	0	0	…	0	0
2	0,0031	0	0	…	0.003145	0	0	…	0.00214	0.003145
3	0,0028	0	0	…	0	0,000045	0	…	0	0
..	..	..	..	.	..	..	..	.	..	..
4879	0	0.00003	0	…	0	0	0	…	0,000045	0
4880	0	0	0	..	0	0	0	…	0	0
4881	0	0	0	…	0,000022	0	0	…	0	0
12491	0	0.000294	0	…	0	0	0	…	0	0
12492	0	0	0.000348	…	0	0	0	…	0	0

На следующем этапе просуммируем полученные значения до получения необходимого результата (точности модели), т.е. до значения 0.95. Полученная сумма должна быть не меньше 0.95 [27]. Этим критерием и ограничится репрезентативная (с точки зрения трафика) выборка (6):

$$\delta(\bar{B}_s) = 0.0913456 + 0.0710745 + \cdots + 0.0027543 + \cdots + 0.000101854 = 0.9519. \quad (6)$$

При данном суммировании имеем выборку из 385 элементов.

Далее обнулим столбцы и строки не входящие в данную выборку узлов матрицы (табл. 4).

Таблица 7 – Ранжированная усеченная матрица социальной сети YouTube

№ узла / № узла	1	2	.	150	.	300	301	.	385
1	0	0	.	0	.	0	0	.	0
2	0	$1845*10^{-7}$	.	0	.	0	0	.	0
.	.	.	.	.	.		.	.	.
150	$2965*10^{-7}$	0	.	0	.	0	$1032*10^{-7}$		0
.	.	.	.	.	.	.	.	.	.
300	0	$45102*10^{-7}$	.	0	.	0	0	.	0
301	0	0	.	0	.	0	0	.	0
.	.	.	.	.	.	.	.	.	.
385	0	0	.	0	.	0	0	.	0

Используя программное обеспечение «Gephi», можно представить исследуемую социальную сеть без узлов администрации в виде графа, в котором вершины являются пользователями, а взвешенные дуги обозначают весь контент, который проходит между пользователями YouTube [34]

У данной социальной сети (рис. 6) явная кластерноть не прослеживается. Это напрямую зависит от возможностей авторизованных пользователей – любой авторизованный пользователь может просмотреть любой видео ролик, прокомментировать его и сохранить к себе в закладки.

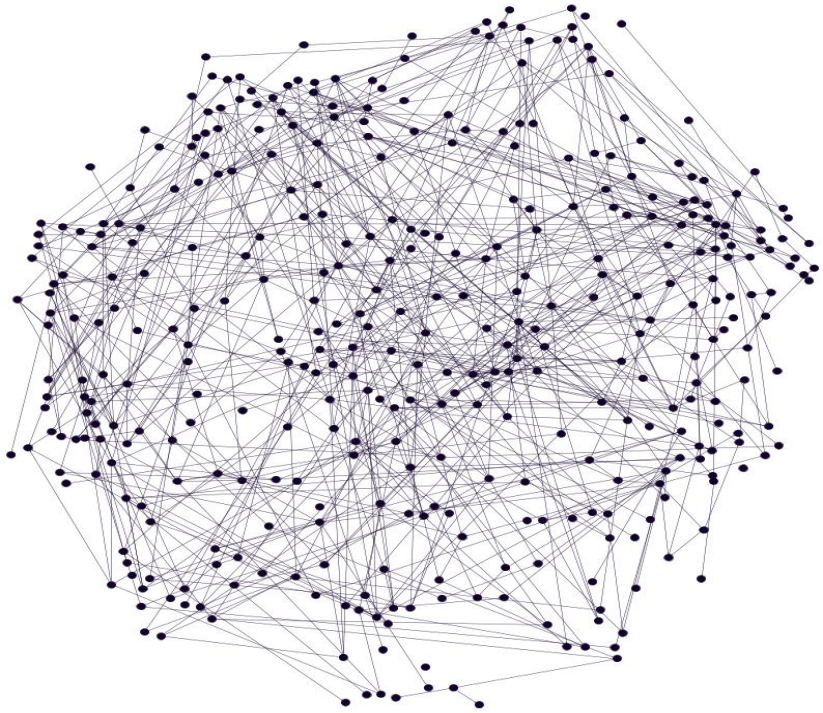

Рис. 6. Выборка социальной сети YouTube

Завершающий этап алгоритма состоит в формировании итоговой матрицы в виде, удобном для последующего моделирования информационной диффузии. Данная матрица представлена в таблице 8.

Таблица 8 – Модифицированная матрица смежности социальной сети YouTube

№ узла / № узла	1	2	.	150	.	300	301	.	385
1	0	0	.	0	.	0	0	.	0
2	0	8	.	0	.	0	0	.	0
.	.	.	.	.	.	.	.	.	.
150	0	0	.	14	.	0	0	.	0

Продолжение таблицы 8

.	.	.	.	.	.	.	.	.	.
300	0	0	.	0	.	17	0	.	0
301	0	0	.	0	.	0	9	.	0
.	.	.	.	.	.	.	.	.	.
385	0	0	.	0	.	0	0	.	15

Для того, чтобы с уверенностью можно было пользоваться усеченной моделью, необходимо доказать подобие основной сети ее выборке [27]. Одним из возможных способов доказать подобие основной сети и полученной репрезентативной выборки (на основе доказательства о принадлежности полученной выборки сети к степенному закону распределения) является критерий Пирсона

$$\chi^2_{набл} = \sum_{i=1}^{k} \frac{(n - np_i)^2}{np_i}, \quad (7)$$

где n – объем выборки;

p_i - вероятность попадания случайной величины X в заданный интервал.

Тогда следуя представленной формуле (7), рассчитаем значение χ^2. В данном случае χ^2 = 7.64. Теперь посчитаем $n = 18$ (выборка) – 1 (количество параметров в плотности степенного распределения) = 17 (число степеней свободы). Выберем уровень значимости $\alpha = 0{,}05$, тогда $p = 1 - \alpha = 0.95$ [27]. Табличное значение $\chi^2(27)$ равно 8.67. Получается, что табличное значение χ^2 больше вычисленного. Следовательно, гипотеза верна, что также доказывает рисунок 7.

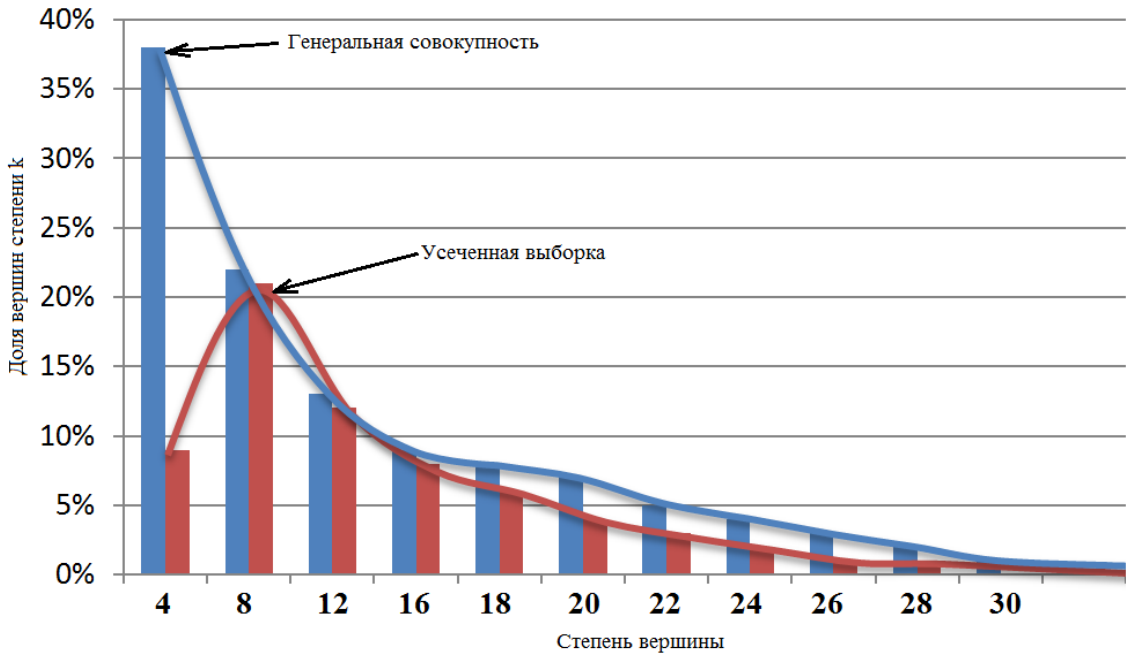

Рис. 7. Гистограмма распределения степеней вершин

Из рисунка 7 видно, что распределение генеральной совокупности и полученной репрезентативной выборки имеют схожую форму и имеют допустимое отклонение 11,81%, что и было получено в ходе проверки распределений [27].

Таким образом, используя алгоритм преобразования исходных данных сети, была найдена репрезентативная выборка, получена визуальная модель усеченной социальной сети YouTube и соответствующие матрицы, способные в полной мере охарактеризовать структурно-функциональные особенности распространения контента в социальной сети YouTube, что поможет достичь главной цели исследования, которая состоит в оценке и регулировании рисков, возникающих в сети в случае распространения в ней деструктивного контента [2-4, 10, 12, 18, 20].

Литература:

1. Antsupov, A. Ya. Conflictology: the textbook for higher education

institutions / A.Ya. Antsupov, A. I. Shilov. - 3rd prod., reslave, and additional - SPb.: St. Petersburg. – 2007. – 591 p.

2. 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.

3. 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 Journal. – 2013. -25 (3). – P. 410-415.

4. 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.

5. Antsupov, A. Ya. Conflictology: the textbook for higher education institutions / A.Ya. Antsupov, A. I. Shilov. – 3rd prod., reslave. and additional – SPb.: St. Petersburg. – 2007. – 591 p.

6. Bachilo, I. L. About the concept of legal support of informatization of Russia. Legislative problems of informatization of society/I.L. Bachilo, G. V. Belov / - M.: World. – 1992. – 400 p.

7. Bachilo, I. L. Information right. The textbook Under the editorship of the academician of RAS B. N. Topomina/I.L. Bachilo, V. N. Lopatin, M. A. Fedotov and other / SPb.: Legal center. – 2001. – 789 p.

8. Bachilo, I. L. Information right: fundamentals of practical informatics: Education guidance / I.L. Bachilo / - M: Edition of Mr. M.Yu.Tikhomirov. – 2001. – 352 p.

9. Byrd, K. War with many unknowns / K. Byrd//Computerra. - M. – 2009. - No 20. – 5 p.

10. 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.

11. Evolution and convergence of the patterns of international scientific collaboration Proc. Natl. Acad. Sci. USA. – 2016. 57 - 61c.

12. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.

13. Grinyaev, S. Russia in global information society: threats, risks and possible ways of their neutralization / S. Grinyaev, - - Электрон. дан. - Режим доступа: http://www.noravank.am/upload/pdf/419_ru.pdf.

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

15. Kalashnikov, A.O. Attacks to information and technological infrastructure of crucial objects: assessment and regulation of risks: Monograph / A.O. Kalashnikov, E. V. Yermilov, O. N. Choporov, K. A. Razinkin, N. I. Barannikov; under the editorship of the Member correspondent of RAS D. A. Novikov. - Voronezh: Scientific Book publishing house. – 2013. – 160 p.

16. Newman, M. E. Finding and evaluating community structure in networks / M. E. J. Newman, M. Girvan // Phys. Rev. E 69. – 2004 . – 123 p.

17. 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.-№ ll(10s). – P. 511 - 514.

18. Principles of scientific research team formation and evolution Proc. Natl. Acad. Sci. USA. – 2014. – 89 p.

19. 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.

20. Social Network Analysis John Scott 19 ноября 2013 г. SAGE -

Электрон. дан. - Режим доступа: http://www.pnas.Org/content/98/2/404.full

21. Social Networking Data Mining. – Электрон. Дан. – Режим доступа: http://ru-sndm.livejournal.com/1481.html

22. YouTube//Konect. Дата обновления 23.08.2016. – Электрон. Дан. – Режим доступа: http:/konect.unicoblenz.de/networks/YouTube (дата обращения 13.09.2016).

23. Анализ социальных сетей. Дата обновления 12.06.2016 URL: http://letopisi.org/index.php/. (Дата обращения 1.09.2016)

24. Анализ контента социальных медиа в эпоху больших данных. – Электрон. Дан. – Режим доступа: https://mebius.io/analysis/social-media-content-analysis.

25. Абрамов К.Г., Модели распространения вредоносных программ в топологических гетерогенных социальных сетях - Электрон. Дан. - К.Г. Абрамов, Ю.М. Монахов; Труды НТС. Комитет по информатизации, связи и телекоммуникациям Администрации Владимирской области. – 2010. – С.156-161.

26. Абрамов К.Г., Труды пятой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности "Имитационное моделирование. Теория и практика" / Абрамов К.Г., Монахов, Ю.М., Бодров И.Ю. // Теория и практика" ИММОД-2011. – Санкт-Петербург: ОАО 105 "Центр технологии и судостроения". – 2011. – С. 373-378.

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

28. Губанов Д.А., Социальные сети: модели информационного влияния, управления и противоборства / Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. // уч – С. 203-205.

29. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства /

Под ред. чл. РАН ДА. Новикова. -М: Издательство физико-математической литературы. – 2010. – 116 с.

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

31. Информация о социальной сети YouTube. - Электрон. Дан. - Режим доступа: https://ru.wikipedia.org/wiki/YouTube

32. Стрельников А. Н. Социальные сети: механизмы работы и пути развития. Электронные данные - Режим доступа: http://www.rae.ru/forum2011/153/1796

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

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

35. Статистика посещаемости основных социальных сетей по России за май 2015 года. – Электрон. Дан. – Режим доступа: http://www.fabians.ru/социальные-сети-посещаемость-май-2015.

36. Черняк, Л. Сервисы и теории социальных сетей Текст. / Л. Черняк / Открытые системы. СУБД. – 2008. - № 8. – С. 25-31.

Региональный учебно-научный центр по проблемам
информационной безопасности

Воронежский научно-образовательный центр управления
информационными рисками

УДК 004.056.57

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ СЕТЕВОГО ПРОТИВОБОРСТВА И КОНТРОЛЬ СОЦИАЛЬНЫХ СЕТЕЙ

Г.А. Остапенко, Е.С. Соколова, Н.Ю. Щербакова, Н.М. Тихомиров, Д.Г. Плотников

Для анализа состояния информационного пространства, пожалуй, особую ценность представляет «дробь Толстого», где Лев Николаевич проявил себя не только как литературный гений, но и в качестве глубокого аналитика. Напомним, что в ней человек оценивается как некоторая дробь, в числителе которой представлена объективная характеристика анализируемой личности, а в её знаменателе фигурирует показатель самомнения, т.е. то, что этот человек о себе думает. Отсюда отклонение дроби от единицы характеризует либо неуверенность, либо нахальство исследуемого индивидуума. При этом значительный разброс указывает на людей, склонных к предательству и авантюризму. Так что информационная «дробь Толстого» весьма полезна в обычном общении, хотя бы в плане ограничения контактов с неадекватными людьми.

Иное дело, когда общение происходит в виртуальном пространстве, например в социальной информационной сети. Здесь «дробь Толстого» следует модифицировать. Знаменатель указывает на то, как позиционирует себя пользователь в сети, а числитель характеризует его сетевой имидж. В этом случае, в виду анонимности, знаменатель весьма сомнителен и только глубокий контроль и анализ могут раскрыть его сущность. Отсюда мониторинг и прогнозирование процессов, протекающих в социальных сетях, сегодня становится важнейшей составляющей обеспечения сетевой безопасности личности, общества и государства. Рассмотрим более

подробно информационно психологические аспекты сетевого противоборства и контроля.

Сетевой терроризм. Одной из основных проблем общества является терроризм. Специфика современного терроризма видится в том, что:

– теракт сегодня выступает детонатором для информационной бомбы;

– она имеет ярко выраженный распределенный характер, то есть срабатывает информационно - психологические «заряды» в сознании каждого отдельно взятого члена социума, порождающие панический страх перед терроризмом;

– детонация этих зарядов в совокупности способна вызвать хаос в социальном пространстве и дезорганизацию его жизнедеятельности;

– масштабы взрыва зависят от размерности и разветвлённости информационной сети, в которую поступают сведения о теракте, то есть от мощности множества ее пользователей;

– наконец, интенсивность информационного взрыва определяет также степень критичности для социума объекта теракта (символы нации и её будущего, ядерные объекты и т.п.).

Отсюда следует необходимость антитеррористического контроля информационного пространства.

В нашей стране действует конституционный запрет на цензуру, что создает определенные проблемы. При этом у ИГИЛ есть целые подразделения занимающиеся пропагандой. Каждую неделю они выпускают новый ролик на русском языке и массированно выбрасывают его в Сеть – на сотни, а то и тысячи площадок, сайтов, форумов, социальной сети. За сутки двое удается удалять все эти ролики. Раньше они пытались поместить на максимальном количестве площадок один и тот же ролик. Теперь новые ролики выпускают один за другим в расчете на то, что хоть кто-то успеет их увидеть.

Сетевой суперфильтр. Китайский проект «Золотой щит» ближе к определению цензуры. Фильтрует информацию, поступающую в китайское интернет пространство извне. Обслуживают ее десятки тысяч высококвалифицированных специалистов, и китайское общество значительно защищено. Логично контролировать точки входа Интернета и в нашу страну. Интернет был создан Пентагоном. Позднее он превратился в гражданское средство связи. Однако, доменные имена и IP-адреса (это своего рода сетка, на которой держится Интернет, его инфраструктура) распределяет американская корпорация ICANN. Влияние США на эту организацию огромное.

Сетевой шпион. Смартфон – это вовсе не дружественный попутчик, наоборот, он постоянный и внимательный наблюдатель. Функции принудительного фотографирования, реализованная в приложении «Фонарик», получает из вашего телефона огромный объем информации, которой можно торговать, например копирование контактов, передача данных о вашем местоположении. Большие данные – это, по сути, уголь и нефть будущего. Подобная информация позволяет прогнозировать, как люди того или иного возраста, пола, проживающие на определенной территории, будут вести в некой ситуации. Информацию можно держать в смартфоне, компьютере, отдавая себе отчет в том, что они в любой момент могут быть отправлены в неизвестном направлении. Абсолютно личную информацию нужно записывать на бумаге, и тем более не помещать в Интернете. Здесь нужен самоконтроль (информационная гигиена).

Сетевой анализ. Международная группа ученых из университетов Абердина, Кембриджа, Сарагосы и Колумбии построила модель распространения и информации в соцсетях, сравнив этот процесс с вирусной инфекцией. Специалисты решили провести сравнение между сложными социальными явлениями и инфекционными заболеваниями.

Они использовали модели распространения эпидемий для построения математической модели распространения новых идей.

По словам руководителя исследования, доктора Франциско Перес-Рече, предложенные ранее математические модели обычно не учитывают, выражаясь научным языком, синергического эффекта связей между людьми и потому не могут дать объяснение феномену цепной реакции (синергеческий эффект – возрастание эффективности деятельности в результате соединения, интеграции, слияния отдельных частей в единую систему). По его мнению, математическая модель, разработанная им его группой, вполне подходит для практического использования. Например, ее можно применять как для решения различных социальных проблем, так и для продвижения коммерческих идей.

Калькулятор сетевого успеха и ущерба. Социальные сети – сегодня самый мощный вещатель (миллиарды активных и пассивных пользователей). Пользователь – субъект сети, объективно заинтересованный в достижении максимальной популярности в социуме и в получении самой полезной информации через сетевые сервисы. В этом состоит феномен лавинообразного роста количества соцсетей различного назначения и их пользователей, а также - ожесточенной конкурентной борьбы в этом информационном пространстве. Фактически речь идет о битве контентов за информационно-психологические предпочтения массы социально и экономически активных людей, охватывающей треть Человечества. Ставки весьма высоки и поэтому технологическая изощрённость конструирования и распространения контента в социальных сетях превышает всякие ожидания. И здесь краеугольным выступает вопрос об инструментарии – комплексе средств пошагового моделирования процесса диффузии контента в соцсетях, исходя из вероятностных параметров его восприятия. То есть остро необходим инструмент прогнозирования сетевого успеха контента, который желают

использовать как всякий активный пользователь, так и многочисленные исследователи социальных сетей. Ожидаемую востребованность такого комплекса (в том числе при исполнении его в виде мобильного приложения) трудно переоценить.

В плане импортозамещения весьма полезными оказались наработки нашей научной школы [1-14] в области дискретного моделирования информационных процессов. Дело в том, что традиционный инструментарий моделирования диффузии наполнителя в сетевых структурах, широко используемый для описания медико-биологических эпидемий, в силу своего аналогового характера практически исчерпал свои возможности, оставив множество вопросов. Особенно ярко они проявились при моделировании эпидемических процессов социальных сетей, где дискретная природа состояний пользователей (заражен, латентен, иммунизирован и др.) очевидно требует разрешение следующих противоречий между:

– практической необходимостью учета часто применяемого репостинга деструктивного контента и невозможностью описания этого явления в аналоговых моделях;

– насущной потребностью моделирования атак сетей деструктивным контентом, распределенных как в пространстве сети (множество источников), так и во времени (асинхронный вброс), и принципиальной неготовностью традиционных инструментов для анализа этой ситуации;

– актуальной необходимостью смены (управления защитой) параметров (вероятностных и пр.) сети на определенном шаге моделирования и неспособностью аналоговых моделей это сделать;

– реальной потребностью учета весов (значимости) пользователей в эпидемическом процессе и ориентированностью традиционного моделирования на не взвешенные сети;

– объективной необходимостью моделирования процессов столкновения конкурирующих контентов в вершинах сети, соответствующих её пользователям, и принципиальной невозможностью описания аналоговыми моделями такой ситуации.

В этой связи возникает цель – создание инструментария (математического и программного обеспечения) дискретного моделирования процессов распространения контента в гетерогенных информационных сетях, разрешающего вышеперечисленные противоречия в интересах более адекватного прогнозирования развития данных процессов в условиях нарастающего сетевого противоборства.

Для достижения поставленной цели необходимо решение следующих задач:

1. Формирование информационного обеспечения, включая топологические особенности (инцидентность пользователей и силу их связей) анализируемой сети, величину межэлементного трафика, а также – вероятности переходов пользователей из одного состояния в другое при воздействии на них контентов различной тематики.

2. Создание моделей и методик инфицирования пользователей контентом, а также – диффузии контента в сети с учетом неоднородности её элементов, в том числе при столкновении конкурирующих контентов в вершинах сети.

3. Алгоритмизация и программная реализация разработанного математического обеспечения на перспективных платформах, включая создание мобильных приложений, ориентированных на широкую аудиторию виртуального пространства.

При этом надо понимать, что проектируемый инструментарий имеет двойное назначение, ибо будет позволять не только прогнозировать популярность (шанс) распространения конструктивного контента, но и

оценивать опасность (риски) возникновения эпидемии деструктивного контента.

На старте моделирования, по большому счету, пользователю, прежде всего, необходимо определиться с соцсетью или классом соцсетей, отвечающим его интересам. Классификация таковых известна, и текущие статистические данные по топологии и «силе связей» в таких сетях открыто публикуются. Именно эти данные служат основой для построения вышеупомянутых матриц, используемых в дискретных моделях процесса распространения контента в сетях. Пользователь также может самостоятельно определить (скажем, экспертным путем) и задать вероятностные параметры контента. Далее, опираясь на матрицу взвешенной центральности и исходя из собственных возможностей доступа, он должен выбрать вершины сети, к которым будет доставляться контент. Пользуясь предлагаемым инструментарием, пользователь может оперативно спрогнозировать ожидаемую восприимчивость сети к распространяемому им контенту, что позволяет надеяться на широкую популярность настоящего программного комплекса и успешную его коммерциализацию.

Условно данный проект можно назвать «калькулятор сетевого успеха». Он нацелен на прогнозное моделирование процессов распространения контента в социальных сетях, а удачный прогноз это уже половина успеха. Оценивая шансы восприятия сгенерированного контента сетевой структурой, пользователь соцсети измеряет возможности своего интеллектуального продукта. Амбиции автора могут успешно реализоваться в данном случае через сервисы соцсетей. При этом затратная часть в основном сконцентрирована в области генерации качественного контента, а главной целью современного пользователя (в широком смысле) является самореализация через завоевание популярности в сети. Он готов многократно совершать попытки по достижению данной

цели и «калькулятор сетевого успеха» может оказаться удобным подспорьем в сокращении количества подобных попыток.

Программный комплекс «Netepidemic» создавался для моделирования процессов сетевого распространения деструктивного контента, т.е. оценки эпистойкости сети в контексте обеспечения её безопасности. Однако, он применим как к контенту со знаком «минус» (деструктивному), так и для контента со знаком «плюс» (позитивному). Здесь всё зависит от намерений пользователя, генерирующего контент. И чем искуснее создан этот продукт, тем больше пользы или вреда (ущерба) он принесет сети и её социуму. Таким образом предлагаемый продукт имеет ярко выраженное двойное назначение:

1. Анализ процессов распространения вредоносного контента в сети (вероятностная оценка риска).

2. Моделирование сетевого восприятия позитивного контента (вероятностная оценка шанса).

Наиболее широкое применение предлагаемого продукта видится для решения второй задачи, а именно в социальных сетях, где имеет место:

– огромное количество (миллионы и миллиарды) возможных потребителей продукта в лице пользователей соцсетей;

– устойчивая мотивация этих пользователей к обретению сетевого успеха в результате широкого и эффективного восприятия самостоятельно сгенерированного (авторского) контента, распространяемого в интересующей сети.

Увы, пространство социальных сетей стало ареной ожесточенной политической борьбы за право управлять массовым сознанием и это еще раз подчеркивает актуальность, научную и практическую значимость ожидаемых результатов в плане оценки возникающих в данном случае рисков и шансов, информационного управления ими в интересах устойчивого развития Человечества.

Литература

1. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G. Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. – 2013. – 25 (3). – P. 404-409.

2. The usefulness and viability of systems: Assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. – 2013. – 25 (4). – P. 675-679.

3. 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.

4. 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 Journal. – 2013. – 25 (3). – P. 410-415.

5. Ensuring the security of critically important objects and trends in the development of information technology / A.O. Kalashnikov, Y.V. Yermilov, O.N. Choporov, K.A. Razinkin, N.I. Barannikov // World Applied Sciences Journal. – 2013. - № 25 (3). – P. 399-403.

6. 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.

7. Email-flooder attacks: The estimation and regulation of damage / V.V. Butuzov, A.G. Ostapenko, P.A. Parinov, G.A. Ostapenko // Life Science Journal. – 2014. – 11 (7s). – P. 213-218.

8. 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.

9. 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.

10. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.

11. 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. – Vol. 86. – No.2. – P. 306-315.

12. Algorithm of Generation of Scale-Free Network at Realization Virus Attacks on Model Chiang Lu. / E. S. Sokolova, N. I. Barannikov, I. L. Bataronov, V.I.Belonozhkin, Research Journal of Pharmaceutical, Biological and Chemical Sciences. – 2016. – Vol. 7. – No.4. – P. 2438-2447.

13. Modeling of layering growth virus epidemic and spread of harmful content on Poisson networks / E.A. Shvartskopf, A.V. Zaryaev, L.V. Parinova, L.G. Popova. / Research Journal of Pharmaceutical, Biological and Chemical Sciences. – 2016. – Vol. 7. – No.4. – P. 2321-2331.

14. Discrete risk models of the process of viral epidemics development in homogenous information and telecommunication networks / E.N. Ponomarenko, V.N. Kostrova, R.K. Babadzhanov, Y.N. Guzev, V.S. Zarubin // Journal of Theoretical and Applied Information Technology. – 2016. – Vol. 92. – No.2. – P. 235-252.

УДК 004.056.57

ПРОЕКТ «ИНДУСТРИЯ – 4.0» И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА

О.А. Остапенко, Д.А. Медведев, А.Е. Дешина, И.П. Нестеровский

Пожалуй, первой индустриальной революцией следует считать открытие технологии добывания огня и изобретение колеса. Далее в этот период совершены другие важнейшие для человечества открытия: порох, бумага и т.д. Назовем эту стадию развития «Индустрия -1.0».

Затем качественный скачок, обозначивший начало нового этапа «Индустрия-2.0», произошел с появлением двигателя внутреннего сгорания.

Стартом проекта «Индустрия-3.0», вероятно, следует считать эру массовой автоматизации производств и технологий, резко повысившей производительность труда, качество и количество производимых продуктов.

Сейчас экономической темой номер один, пожалуй, следует считать проект «Индустрия-4.0», заявленный на Давосе-2016 как единственно возможный вариант будущего. Презентация нового технологического уклада шло исключительно в режиме рекламного буклета с упором на потребительские эффекты («умный дом», «умный город», «интернет вещей»), производственные возможности (искусственный интеллект, роботизация, 3D-принтеры) и экономические выгоды (взрывной рост инвестиций) [1-6].

Результат проекта представляют как заманчивое будущее, где люди вместо рутинного труда будут заняты высокодуховным творчеством, производство роботизировано, а коммуникации осуществляются через

«информационное облако». Причем проект меняет базовую модель бизнеса с логики изготовления товара на логику оказания услуги. Иными словами, приобретая чайник, человек покупает не «железо», а функцию кипячения воды, как частичку глобальной информационной сети. Традиционную затратную логистику складов и транспортных поставок классического производства сменит логистика компьютерного файла. Вместе с моделью бизнеса меняется природа капитальных активов, где стоимостью (товаром на продажу) будет не холодильник, а мороз, который этот холодильник производит. Объектом защиты проекта станет информационная платформа, которую невозможно продать, а можно только сдать в аренду пользователям. Основной объём инвестиций пойдёт в создание программного обеспечения, где возникает масса проблем с безопасностью [1].

Идиллия выглядит примерно таким образом. «Пообщавшись» с будильником, котёл греет воду (столько, сколько надо, до той температуры, какой надо, и к тому моменту, когда надо), чтобы вы приняли душ. Кофеварка и тостер готовят завтрак к моменту выхода из душа. Машина сама себя прогреет и запишется в автосервис на ТО в зависимости от пробега, уведомив вас об этом смской на смартфон [1].

Способность вещей «общаться» между собой не является технологической революцией. Переворотом является создание единого общемирового протокола для «общения» вещей независимо от их происхождения и принадлежности.

Из социалистического прошлого уместно вспомнить, что обещания светлого будущего ещё никогда не исполнялись. Увы, промышленные революции никогда не приводили к всеобщему благоденствию, сопровождаясь резким обострением социальных противоречий и даже войнами. При этом смена технологического уклада всегда была одним из способов определения победителей и побеждённых в глобальной гонке

мировых держав. В отношении проекта «Индустрия-4.0» однозначно можно утверждать, что победителем будет тот, кто станет контролировать «большие данные».

В проекте «Индустрия-4.0» все потребности человека будут удовлетворены роботами, но возникает проблема: по каким принципам будет ранжироваться социум и строиться социальная пирамида?

В рекламе «Индустрия-4.0» представляется как способ обеспечения нового уровня персональной свободы, но в реальности он создаёт механизмы дополнительной связности и большей зависимости. Возникает принципиально новый вид монополии – информационно-цифровой. Монополия эта будет носить глобальный характер [1].

В 2014 году GeneralElectric, AT&T, Cisco, IBM и Intel создали Консорциум промышленного Интернета [IndustrialInternetConsortium (IIC)], в который на данный момент также входят крупнейшие европейские компании. Консорциум занимается созданием «общего словаря понятий» и выработкой единых стандартов, приоритетом являются не технологии как таковые («смарт-фабрика», «смарт-дом», «смарт-город» и т.д.), а общая рентабельность активов и их финансовая отдача. При этом главный вопрос состоит не в том, сколько стоит сбор данных и их обработка, а в том, как эти данные можно использовать. Информация о составлении психологических портретов избирателя с помощью того же «Фейсбука» (биг дата) и формировании месседжей под конкретные группы людей во время референдума по Брекситу в Великобритании и на прошедших недавно в США выборах уже появилась в прессе. Главным параметром инвестиционной привлекательности и условием получения кредита становится полная выгрузка всей информации о себе в общее облако[1].

По проекту предприятия, отрасли и целые страны, использующие свой собственный информационный стандарт, не смогут работать в общей сети по единому протоколу. При этом в случае недостаточной лояльности

предприятия и страны, которые присоединятся к единому протоколу, можно будет отключить от общей системы одним нажатием кнопки.

В свою очередь технические решения, заложенные в «Индустрию-4.0», позволяют контролировать из одного центра параметры любого предприятия в любой точке мира и потребительское поведение любого человека планеты.

По логике глобальный стандарт проекта должен опираться на морально-этические, идеологические, правовые и политические императивы надгосударственного уровня. Кто эти императивы отберёт и утвердит? Кто обеспечит их исполнение? Что делать с носителями других этических норм, с национальными и конфессиональными различиями? Ответы на эти вопросы прикрывались рассуждениями об исключительности и избранности американской нации [1].

В результате внедрения проекта «Индустрия-4.0» по мнению создателя и бессменного президента Всемирного экономического форума Клауса Шваба изменится не только то, что мы делаем, но и то, кто мы есть. Фактически изменится наша индивидуальность: чувство уединения, понятие о собственности, модель потребления, представления о карьере и успехе, способы знакомства с людьми и общение.

Сначала удар по основам проекта «Индустрия-4.0» нанесли Джулиан Ассанж и Эдвард Сноуден, после разоблачений которых неожиданно выяснилось, что информационно прозрачный мир означает: не равноправный политический диалог, а возможность слушать своих союзников и партнёров в онлайн-режиме; не общие правила для бизнеса, а право штрафовать и банкротить предприятия-конкуренты; не равенство возможностей всех стран, а господство одной-единственной сверхдержавы[1].

Вторым ударом стал Брексит, обозначивший системный кризис ещё одного проекта глобализации - Евросоюза.

Наконец инаугурационная речь Дональда Трампа, ставшая гимном национальной Америке, фактически вынесла проекту приговор. Открыто выступили против американского проекта глобализации многие страны. Не удивительно, ведь роль периферии в новом проекте отводится Южной Америке, Мексике, Австралии и Канаде. Роль главного геополитического противника Америки переходит к Китаю, который быстрыми темпами продвигается вглубь континента в направлении Европы. Судьба Европы как одного из центров мировой силы вновь целиком и полностью зависит от Германии. Россия в этой борьбе становится привлекательной в силу её транзитного положения и ресурсного фактора. Отсюда просматривается следующий сценарий.

В докладе Национального совета по разведке США «Глобальные тенденции 2030: альтернативные миры» один из базовых сценариев развития событий называется «Заглохшие двигатели». В его основе – неспособность политической системы США решать возникающие мировые финансовые проблемы, вследствие чего мировая экономика и деловая активность «ложатся в дрейф». Согласно сценарию, ослабление роли Вашингтона ведёт к росту центробежных сил в ЕС и возрастанию влияния национально ориентированных партий. Несостоявшиеся государства дробятся по конфессиональным, племенным и этническим разломам. На Ближнем Востоке ожидается рост терроризма и потоков беженцев. При этом в докладе Национального совета по разведке США говорится: «У развивающихся экономик нет единой альтернативной идеи, они даже блоки полномасштабные (классические) не создают. Национальный эгоизм сильнее общего интереса». Это является главным вызовом для Индии, Китая, России и других стран БРИКС, как альтернативы проекту «Индустрия-4.0».

Таким образом пока несостоявшийся проект «Индустрия-4.0» следует рассматривать как попытку информационно-психологического

закабаления Человечества через цифровую монополизацию на стандарты и большие данные подавляющего большинства юридических и физических лиц планеты. В случае реализации проекта ни о какой безопасности личности и государства речи быть не может. Она будет полностью в руках «цифрового гегемона», образованного глобальными транснациональными корпорациями.

Литература

1. Совершенно секретно – [Электронный ресурс] – Режим доступа: http://www.sovsekretno.ru/articles/id/5626/
2. Hi-News.ru – [Электронный ресурс] – Режим доступа: https://hi-news.ru/business-analitics/industriya-4-0-chto-takoe-chetvertaya-promyshlennaya-revolyuciya.html
3. РБК – [Электронный ресурс] – Режим доступа: http://www.rbc.ru/opinions/economics/12/02/2016/56bd9a4a9a79474ca8d33733
4. Эксперт Online – [Электронный ресурс] – Режим доступа: http://expert.ru/2016/01/21/chetvertaya-promyishlennaya-revolyutsiya/
5. Theory&Practice – [Электронный ресурс] – Режим доступа: https://theoryandpractice.ru/posts/14610-konets-analogovogo-mira-industriya-4-0-ili-chto-prineset-s-soboy-chetvertaya-promyshlennaya-revolyutsiya
6. Furfur – [Электронный ресурс] – Режим доступа: http://www.furfur.me/furfur/changes/changes/216447-4-aya-promyshlennaya-revolyutsiya

Региональный учебно-научный центр по проблемам информационной безопасности

Воронежский научно-образовательный центр управления информационными рисками

УДК 004.056.57

ЭФФЕКТЫ СОВРЕМЕННОГО ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ПРОТИВОБОРСТВА И ПРОГНОЗИРОВАНИЕ ЕГО РЕЗУЛЬТАТОВ В СОЦИАЛЬНЫХ СЕТЯХ

О.А. Остапенко, В.В. Морковина, А.Н. Мокроусов, С.А. Ермаков, А.А. Остапенко

Информационно-психологическое пространство в силу его глобальности не имеет государственных границ, и поэтому нередко используется для вторжений в личную жизнь граждан и общественную деятельность социумов. Дело в том, что в этом многослойном и мультиразмерном пространстве нет всеобщей цензуры. Этот факт открывает широкие возможности для злоумышленников, включая спецслужбы отдельных государств и террористические организации. Причем наибольший интерес для них представляют социальные сети, охватывающие в своем информационном пространстве едва ли не треть Человечества. Здесь им открываются практически безграничные возможности для информационно-психологического воздействия на пользователей сети.

В результате социальные сети стали ареной не только для недобросовестной конкуренции, но и откровенного информационного противоборства, в котором активно участвуют и государственные структуры. Руководители ведущих стран прекрасно понимают, что от того, как выглядит их политика в соцсетях, во многом зависят общественное мнение и поддержка населения. Мало того, проигрыш в информационно-психологическом пространстве может привести к утрате власти и

политического влияния не только отдельного руководителя, но и целых стран.

В качестве иллюстрации вышесказанного рассмотрим наиболее крупные эффекты, которые зарегистрированы в последнее время в мировом информационно-психологическом пространстве. Они относятся к результатам стратегического противоборства наиболее влиятельных государственных образований, их достижениям и просчетам, обусловленным информационной политикой и реакцией на нее населения. Нижеприведенные примеры поучительны с точки зрения недооценки и необходимого внимания по отношению к проблеме обеспечения информационно-психологической безопасности нации, прежде всего в пространстве набирающих популярность социальных сетей.

Эффект Трампа. Дело здесь не только и не столько в Трампе, хотя и надо отдать должное его весьма эффективной предвыборной кампании, особенно в социальных сетях. И всё-таки, это всё – субъективный фактор. А объективные предпосылки его победы на выборах таковы:

1. У США уже не хватает ресурсов (финансовых, политических и военных) на безусловное доминирование в мире, всеобщую гегемонию во всех сферах человеческой деятельности на всех геополитических пространствах. Как и СССР, они надорвались, а в спину дышит Китай.

2. Это приводит к обострению внутренних противоречий, беспрецедентно «грязная» предвыборная гонка – яркое тому свидетельство.

3. Значительно изменилась структура информационного пространства, которое всё активнее завоёвывает Интернет, где фильтрация контента гораздо слабее, чем в конкурирующих с ним других электронных СМИ. Поэтому традиционная «долбежка» мозгов через телевидение, заказанная транснациональными корпорациями, уже не дает прежнего эффекта. Морочить мозги населению в интересах «олигархии» становится

гораздо сложнее, даже при современном уровне развития информационного оружия.

Наконец, развязав многочисленные военные конфликты в Северной Африке и на Ближнем Востоке, США потеряли морально-нравственное право на декларируемую ими исключительность своей нации.

С учетом вышеуказанного, США ожидает длительный период нестабильности с потерей позиций на внешнеполитической арене и глубокой внутренней конфронтацией. Их информационно-психологическое пространство «дало трещину». Сейчас Трамп, расширяя свою информационную команду, рассчитывает заделать эту трещину, прежде всего в социальных сетях.

Эффект Китая. Экономический взлёт КНР обусловлен не столько трудолюбием китайского народа, сколько алчностью Запада.

Китай во многом открыл свои границы для зарубежного капитала. В погоне за суперприбылью, обусловленной чрезвычайной дешевизной рабочей силы в КНР, транснациональные компании кинулись стремительно переносить свои производства и технологии в Китай. Получив с них весьма значительные налоги и быстро освоив их технологические достижения, китайцы довольно быстро наладили свои производства и заполонили Запад своей более дешёвой продукцией. Неслучайно Трамп твердит о возвращении производств в США. Однако уже поздно, так как «джинн выпущен из бутылки». Сегодня Китай куда большая «головная боль» для американцев, чем Россия.

Взаимопроникновение США и КНР отнюдь не коснулось информационного пространства Китая. Напротив, руководство КНР жестоко фильтрует информацию. Интернет-фильтр, названный «Великий китайский файрвол», является ярким тому свидетельством. Кроме того, ведущие мировые социальные сети заменены в КНР китайскими аналогами. Возможно, это перегиб, но он реализован в интересах

стабильности китайского общества, которому американцам можно только позавидовать.

В этом контексте, перед Китаем открывается окно новых возможностей в соперничестве с США. Информационно-психологическое единство общества и мощь его экономики позволяют руководству КНР выдвигать всё новые претензии на территории и рынки. Трамп рассчитывает активно противостоять этому, но пока это только благие пожелания. Долги США перед КНР весьма велики, а это мощный рычаг давления.

Ко всему прочему Китай вступил в стратегическое партнерство с Россией, а этот сплав финансовой, ресурсной и военной мощи испугает кого угодно. Поэтому Трамп попытается расстроить этот союз в интересах США.

Вместе с тем нужно помнить, что идея заселения китайцами Сибири не умерла в умах руководства КНР, ибо проблема перенаселения Китая никуда не исчезла.

Эффект Европы. Национальная безопасность – это построенный государством над обществом защитный купол, размещенный на трёх опорах: вера, семья и образование. Крылатая фраза о том, что “войну проигрывают не генералы, а учитель и священник” – яркое тому свидетельство.

Увы, Европа в своей безоглядной толерантности значительно подорвала вышеуказанные опоры. Если добавить к этому европейский мультикультурализм, уродливо проявляющийся в миграционной политике, то картина получается совсем удручающая.

Бензина в этот костер подливает бюрократия Европейского союза (ЕС), которая по-старинке пытается управлять континентом, манипулируя общественным мнением с помощью подконтрольных СМИ. Но сейчас, в эпоху Интернета «шила в мешке не утаишь», и политические провалы

следуют один за другим. Неслучайно британцы решили «отчалить» от европейского континента, а правящие круги Франции и Германии (ведущих стран ЕС) явно лихорадит в преддверии предстоящих выборов. «Мелкотравчатые» европейские лидеры, традиционно ориентированные на США, с приходом Трампа явно деморализованы. А их поддержка обществом достаточно слаба.

Информационное управление европейцами со стороны ЕС-бюрократии явно не срабатывает, и единая Европа «трещит по швам», обвиняя во всём случившемся Россию. При этом, стратегические просчеты с «арабской весной» и Украиной, где ЕС явно проявил авантюризм, идя в фарватере геополитики США, ещё далеко не в полной мере аукнулись европейцам. Настоящая расплата впереди. И это будет не российская агрессия, а грядущий масштабный «бунт» мигрантов, не настроенных на ассимиляцию и восприятие, так называемых, европейских ценностей. Информационно-психологический диссонанс здесь сделает своё дело, и детонатором, как и в «цветных революциях», могут стать соцсети. Даже попытка создания общеевропейской армии вряд ли остановит этот процесс.

Эффект России. Сейчас Российская Федерация находится на информационно-психологическом подъеме. К её голосу стала прислушиваться мировое сообщество. Наблюдается консолидация общества вокруг Президента РФ по вопросу защиты национальных интересов.

Конечно, четко обозначив свои позиции по ключевым геополитическим вопросам, Россия вызвала на себя шквал критики и санкций, но дальнейшие соглашательство с политикой США было чревато частичной потерей суверенитета, что собственно и произошло со многими странами Европы. Поэтому РФ реализует сейчас на Западе масштабную информационную кампанию по отстаиванию своих интересов. Надо

сказать, что эта программа осуществляется не без успеха и находит все больше позитивных откликов в западном обществе. В этой связи, ЕС стремится всячески ограничить возможность российских СМИ, ибо объективная картина мира, демонстрируемая ими, идет в разрез с субъективной политикой европейской бюрократии, открывает глаза народам Европы на просчеты руководства ЕС.

Осознавая бессмысленность военной конфронтации, стороны будут концентрировать своё внимание на информационном противоборстве, и Запад приложит максимум усилий для дестабилизации информационно-психологического пространства РФ, используя для этого временные экономические трудности России, провоцируя межнациональные и межконфессиональные конфликты внутри неё.

Наша задача состоит в том, чтобы защитить информационное пространство России от подобных посягательств. И здесь первостепенное внимание следует уделить социальным сетям как самому популярному информационному ресурсу трансграничного характера, который стал ареной ожесточенного противоборства конкурирующих контентов.

Поэтому далее рассмотрим процесс распространения и восприятия информационно-психологических конструкций (контентов) в социальных сетях и средства его формализованного описания, которые, как это будет показано далее, имеют довольно большое значения для прогнозирования результатов противоборства.

Прогнозирование результатов противоборства в социальных сетях. Социальные сети – сегодня самый мощный вещатель (миллиарды активных и пассивных пользователей). Пользователь – субъект сети, объективно заинтересованный в достижении максимальной популярности в социуме и в получении самой полезной информации через сетевые сервисы. В этом состоит феномен лавинообразного роста количества соцсетей различного назначения и их пользователей, а также -

ожесточенной конкурентной борьбы в этом информационном пространстве. Фактически речь идет о битве контентов за информационно-психологические предпочтения массы социально и экономически активных людей, охватывающей треть Человечества. Ставки весьма высоки и поэтому технологическая изощрённость конструирования и распространения контента в социальных сетях превышает всякие ожидания. И здесь краеугольным выступает вопрос об инструментарии – комплексе средств пошагового моделирования процесса диффузии контента в соцсетях, исходя из вероятностных параметров его восприятия. То есть остро необходим инструмент прогнозирования сетевого успеха контента, который желают использовать как всякий активный пользователь, так и многочисленные исследователи социальных сетей.

В этом отношении весьма полезными оказались наработки нашей научной школы [1-9] в области дискретного моделирования информационных процессов. Дело в том, что традиционный инструментарий моделирования диффузии наполнителя в сетевых структурах, широко используемый для описания медико-биологических эпидемий, в силу своего аналогового характера практически исчерпал свои возможности, оставив множество вопросов. Особенно ярко они проявились при моделировании эпидемических процессов социальных сетей, где дискретная природа состояний пользователей (заражен, латентен, иммунизирован и др.) очевидно требует разрешение следующих противоречий между:

- практической необходимостью учета часто применяемого репостинга деструктивного контента и невозможностью описания этого явления в аналоговых моделях;

- насущной потребностью моделирования атак сетей деструктивным контентом, распределенных как в пространстве сети (множество

источников), так и во времени (асинхронный вброс), и принципиальной неготовностью традиционных инструментов для анализа этой ситуации;

- актуальной необходимостью смены (управления защитой) параметров (вероятностных и пр.) сети на определенном шаге моделирования и неспособностью аналоговых моделей это сделать;

- реальной потребностью учета весов (значимости) пользователей в эпидемическом процессе и ориентированностью традиционного моделирования на не взвешенные сети;

- объективной необходимостью моделирования процессов столкновения конкурирующих контентов в вершинах сети, соответствующих её пользователям, и принципиальной невозможностью описания аналоговыми моделями такой ситуации.

В этой связи актуальным представляется – создание инструментария (математического и программного обеспечения) дискретного моделирования процессов распространения контента в социальных информационных сетях, разрешающего вышеперечисленные противоречия.

Литература

1. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G. Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. – 2013. – 25 (3). – P. 404-409.

2. The usefulness and viability of systems: Assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. – 2013. – 25 (4). – P. 675-679.

3. 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.

4. 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 Journal. – 2013. – 25 (3). – P. 410-415.

5. Email-flooder attacks: The estimation and regulation of damage / V.V. Butuzov, A.G. Ostapenko, P.A. Parinov, G.A. Ostapenko // Life Science Journal. – 2014. – 11 (7s). – P. 213-218.

6. 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.

7. 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.

8. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.

9. 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. – Vol. 86. – No.2. – P. 306-315.

Региональный учебно-научный центр по проблемам
информационной безопасности

Воронежский научно-образовательный центр управления
информационными рисками

УДК 004.056

СОЦИАЛЬНАЯ СЕТЬ FLICKR: СТРУКТУРНО – ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ РАСПРОСТРАНЕНИЯ КОНТЕНТА

С.В. Подопригорин, А.В. Паринов, А.С. Пахомова, Д.Н. Рахманин, А.В. Бабурин, В.И. Борисов, А.Ю. Савинков

Flickr — фотохостинг, предназначенный для хранения и дальнейшего использования пользователем цифровых фотографий и видеороликов. Является одним из первых сервисов Web 2.0, то есть одним из самых популярных сайтов для размещения фотографий. По состоянию на 4 августа 2011 года сервис имел в своей базе более 6 млрд. изображений, загруженных его пользователями. Также, по данным за август 2011 года, на сервисе был зарегистрирован 51 миллион человек, а общая посещаемость составляла 80 миллионов уникальных пользователей [1].

Функциональную специфику Flickr можно определить следующим перечнем [2,3]:

1. Хранение.
2. Организация и навигация.
3. Дополнительные сервисы.
4. Теги.

При анализе аудитории данной социальной сети целесообразно выделить и обозначить на схеме (рис. 1) три основных типа, задействованных в публикации, просмотре, комментировании и обсуждении тех или иных статей в соответствующих разделах [3,4]:

1) Модераторы.
2) Авторизованные пользователи.

- Активные пользователи.
- Пассивные пользователи.

3) Неавторизованные пользователи.

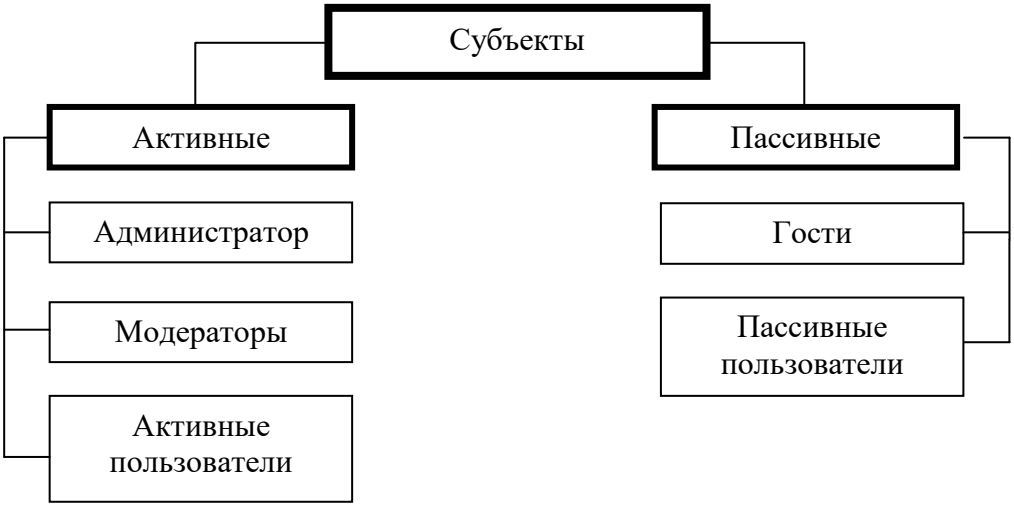

Рис. 1. Классификация субъектов социальной сети Flickr

Для данной социальной сети представление контента актуально в трех формах: текстовом, видео и графическом (рис. 2):

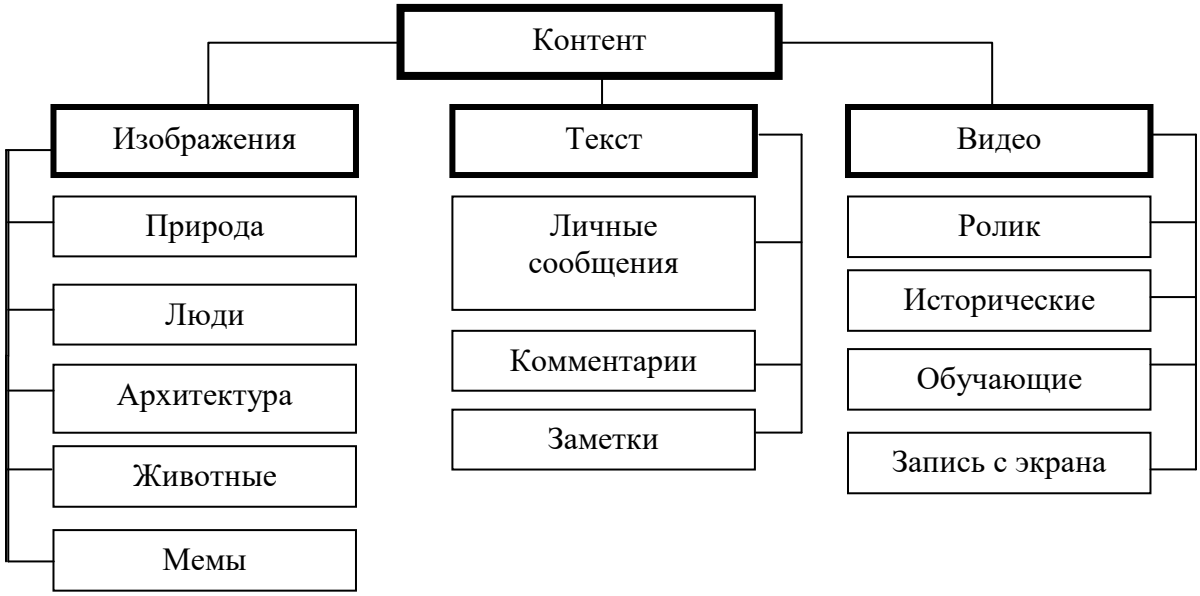

Рис. 2. Классификация контента в социальной сети Flickr

В социальной сети Flickr пользователи имеют определенный набор действий (функций), позволяющий им взаимодействовать с контентом. Все возможности, доступные субъектам данной социальной сети, можно классифицировать по двум признакам [4,5]:

1) По доступности, то есть все действия в данной социальной сети можно разделить на две основные группы: управленческие (доступные только модератору и администратору), и пользовательские, которые в свою очередь подразделяются на возможности, доступные только авторизованным пользователям и возможности, доступные неавторизованным пользователям (рис. 3).

2) Также целесообразно рассмотреть все действия в социальной сети по функциональной возможности, доступные авторизованным и неавторизованным пользователям (размещение, реагирование и т.п.).

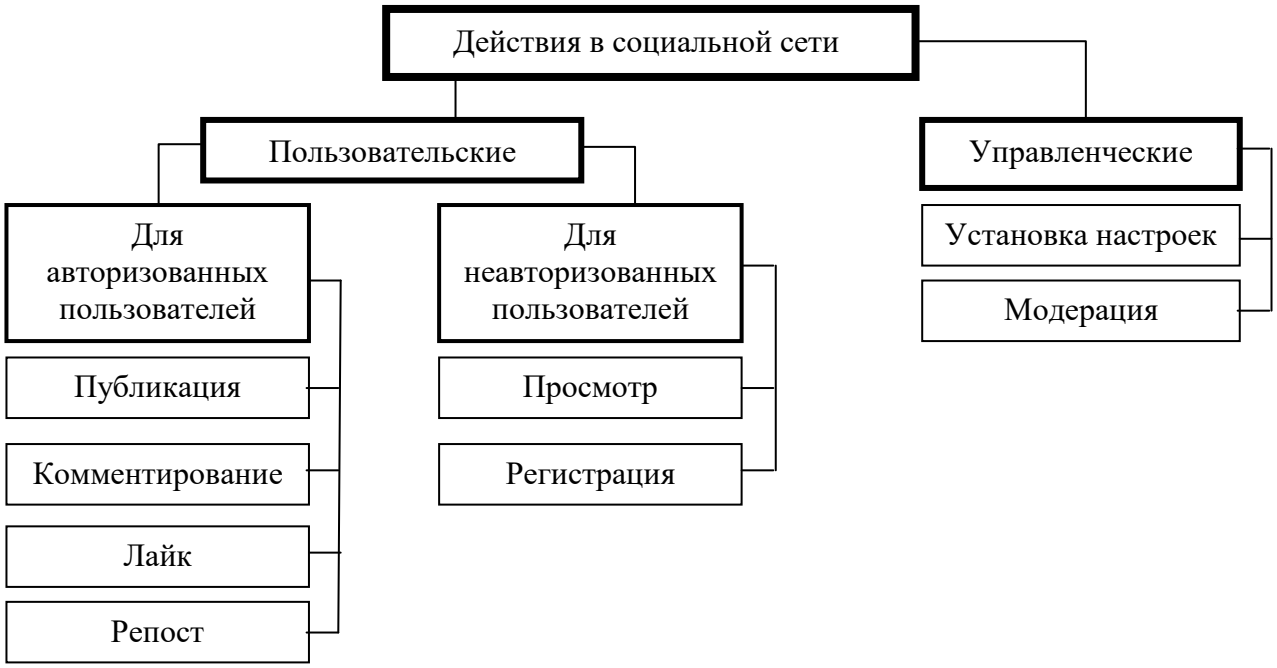

Рис. 3. Классификация действий субъектов в социальной сети Flickr

Классификация (рис. 3) способна дать представление о полном списке возможностей всех субъектов социальной сети Flickr, что позволит проанализировать их действие и поведение в различных ситуациях, а

также построить структурно-функциональную модель социальной сети Flickr [6-12].

К управленческим функциям можно отнести администрирование и модерацию.

Под администрированием, в данном контексте, понимается установление необходимых настроек сайта, доступным только администратору [1].

Под модерацией будем понимать действия привилегированных пользователей (модераторов) по слежению за выполнением другими пользователями установленными администратором правилам и проверку загружаемого ими контента на соответствие требованиям социальной сети [1].

Пользовательские функции в свою очередь подразделяются на функции доступные авторизованным и неавторизованным пользователям.

К числу функций авторизованных пользователей можно отнести все основные возможности, которые получает субъект после прохождения регистрации в социальной сети, включая такие функции как:

- Ознакомление.
- Комментирование.
- Оценка.
- Публикация.
- Распространение.

К возможностям неавторизованных пользователей относится намного меньше функций:

- Ознакомление.
- Распространение.

Однако они могут пройти процесс регистрации и получить расширенные возможности, доступные только авторизованным пользователям.

Далее рассмотрим вторую предложенную классификацию действий, доступных пользователям социальной сети, с позиции их функционала (рис. 4).

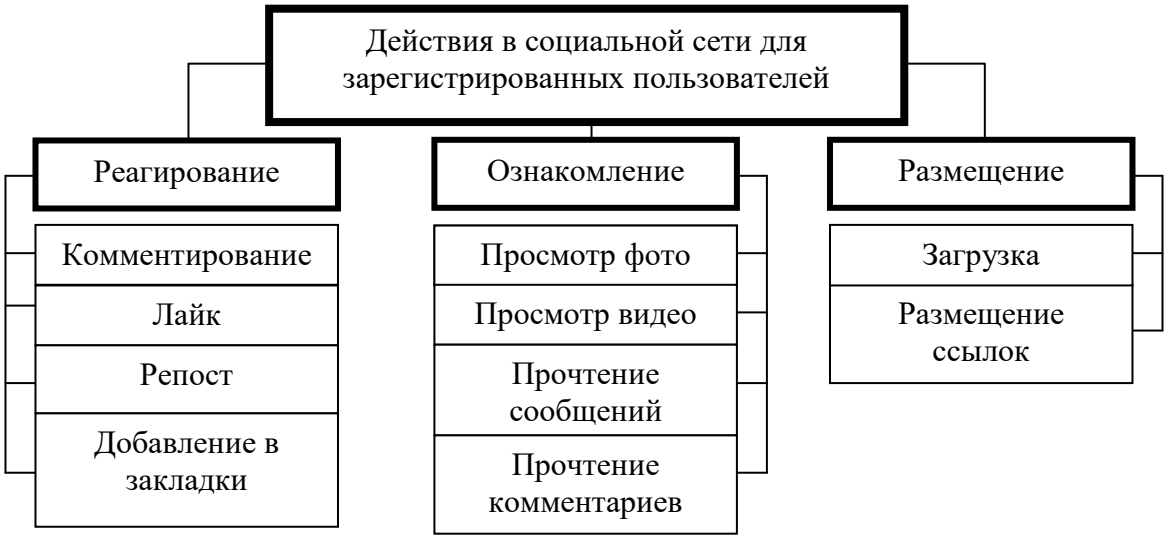

Рис. 4. Функциональная классификация действий субъектов в социальной сети Flickr

В данной классификации (рис. 4) действия, доступные пользователям, были разделены на три основные категории: размещение, ознакомление и реагирование.

В категории «размещение», пользователям доступно только одно действие – публикация.

В категории «ознакомление», пользователи способны прочитать статью или посмотреть видео, рекламу или фотографию.

Весь функционал пользователя социальной сети Flickr сосредоточен в категории «реагирование». В данную категорию попали действия, которые следуют после ознакомления пользователей с предложенным контентом.

С учетом полученных классификаций контента, субъектов и их действий, а также сетевых ресурсов данной социальной сети, предоставляется возможным построить структурно-функциональная модель социальной сети Flickrс учетом всех ее особенностей (рис.5). В

данной модели функциональные связи представляют собой сложную структуру взаимодействия контента, сетевых ресурсов и субъектов, функционирующих в заданном сетевом пространстве [13-15].

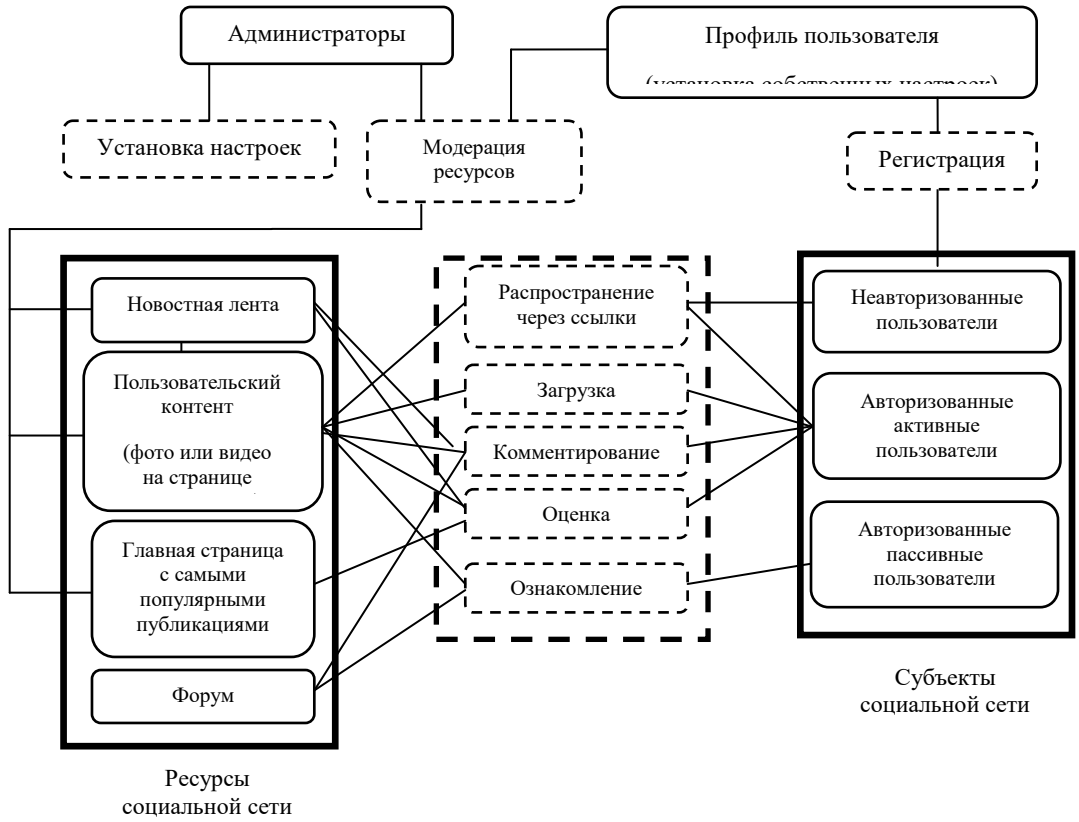

Рис. 5. Структурно-функциональная модель социальной сети Flickr

Таким образом, с учетом классификации контента, находящегося в социальной сети Flickr, его можно разделить на:

- положительный – это информация, которую пользователь социальной сети ожидает увидеть в данном контексте
- негативный (нежелательный) – это информация, которая может быть представлена в виде текста, изображения, видеофайла или ссылки на него, которые могут нести угрозу как информационно-психологического характера, так и угрозу реального заражения компьютера вредоносным ПО.

Необходимым элементом для анализа социальной сети Flickr является нахождение взвешенных метрик.

Статистические данные социальной сети Flickr, можно представить в виде трехместного предиката, в котором на первом месте располагается узел сети, из которого исходит ребро, подтверждающее связь между пользователями сети, на втором месте – узел, в который входит это же самое ребро, а на третьем – вес дуги, отражающий силу связи между вершинами. Вес дуги в данной социальной сети – количество данных (фотографий, видеофайлов и текстовых сообщений), переданных между пользователями в единицу времени [15]. Фрагмент такого предиката, представлен ниже (табл. 1).

Таблица 1 – Фрагмент трехместного предиката социальной сети Flickr

Идентификатор первой вершины	Идентификатор второй вершины	Вес связи
771	1390	9
771	1531	8
771	1763	4
772	1258	2
773	1425	4
776	935	10
777	806	8
777	1528	3
780	1691	4
780	940	1
781	1302	8

Формат данных в данном предикате соответствует формуле (1):

$$\Gamma(x_i, x_j, a_{ij}) \Leftrightarrow \Gamma(i, j, \delta(a_{ij})), \quad (1)$$

где i и j – номера вершин x_i и x_j в сети;

$\delta(a_{ij})$ - вес дуги a_{ij}, связывающей x_i и x_j, и направленной от i к j;

В данном случае вес дуги $\delta(a_{ij})$ можно определить как динамический ресурс, то есть передачу контента определенного объема V и его ценности C в сети в единицу времени и вычислить по формуле (2):

$$\delta(a_{ij}) = \frac{\partial[CV]}{\partial t} = \langle C \rangle V', \quad (2)$$

где $\langle C \rangle$ – усредненная ценность наполнителя (контента);

V' – интенсивность обмена контентом.

Суть алгоритма преобразования исходных данных социальной сети Flickr заключается в построении звездной матрицы, а затем матрицы взвешенной центральности.

На основе предложенного алгоритма преобразования исходных данных сети построим звездную матрица социальной сети Flickr,элементы строки которой соответствуют дугам, входящим в данную вершину, а элементы столбца – дугам, исходящим из вершины (табл. 2):

Таблица 2 – Звездная матрица социальной сети Flickr

№ узла	1	2	3	…	18	19	20	…	100	101	…	1764
1	-	6	3	…	0	0	0	…	2	0	…	0
2	1	-	0	…	0	2	0	…	0	4	…	0
3	0	0	-	…	0	0	0	…	0	3	…	0
⋮	⋮	⋮	⋮	⋱	⋮	⋮	⋮	…	⋮	⋮	…	⋮
18	0	0	0	…	-	0	0	…	0	0	…	0
19	0	3	0	…	0	-	0	…	0	8	…	0
20	0	0	0	…	3	0	-	…	0	0	…	0
⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋱	⋮	⋮	…	⋮
100	0	0	0	…	0	0	0	…	-	0	…	0
101	0	0	0	…	0	0	0	…	0	-	…	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱	⋮
1764	0	0	0	…	0	0	0	…	0	0	…	-

На втором шаге данного алгоритма определим количество входящих (степень входа) и исходящих дуг (степень исхода) для каждого узла социальной сети. Данная матрица будет необходима для последующих процедур моделирования процессов диффузии контента в социальной сети (табл. 3):

Таблица 3 – Диагональная матрица степеней вершин сети Flickr

№ узла	1	2	3	…	20	21	22	…	100	101	…	1764
1	364	0	0	…	0	0	0	…	0	0	…	0
2	0	253	0	…	0	0	0	…	0	0	…	0
3	0	0	200	…	0	0	0	…	0	0	…	0
⋮	⋮	⋮	⋮	⋱	⋮	⋮	⋮	…	⋮	⋮	…	⋮
20	0	0	0	…	30	0	0	…	0	0	…	0
21	0	0	0	…	0	101	0	…	0	0	…	0
22	0	0	0	…	0	0	56	…	0	0	…	0
⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋱	⋮	⋮	…	⋮
100	0	0	0	…	0	0	0	…	13	0	…	0
101	0	0	0	…	0	0	0	…	0	13	…	0
102	0	0	0	…	0	0	0	…	0	0	…	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱	⋮
1764	0	0	0	…	0	0	0	…	0	0	…	1

Следует заметить, что суммарный трафик сети не разделяет входящие и исходящие дуги. Поэтому для определения взвешенной центральности вершины x_s можно использовать сумму, которую далее следует пронормировать по суммарному трафику сети по формуле (3):

$$\sum_i \delta(a_{si}) + \sum_j \delta(a_{js}). \quad (3)$$

В результате (4) получим нормированную величину, которая будет характеризовать удельный вес трафика, проходящего через вершину x_s, по отношению ко всему трафику сети:

$$\delta(\bar{x}_s) = \frac{\left[\sum_i \delta(a_{si}) + \sum_j \delta(a_{js})\right]}{\sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij})}, \quad (4)$$

где $\delta(a_{si})$ – вес трафика в исходящей и узла a_{si} дуге;

$\delta(a_{si})$ – вес трафика во входящей в узел a_{js} дуге.

В итоге, следуя формуле (4), получим матрицу взвешенной центральности элементов исходной сети следующего вида (табл. 4):

Таблица 4 - Матрица взвешенной центральности социальной сети Flickr

№ узла	1	2	…	10	…	28	…	1001	…	1764
1	0,023	0	…	0	…	0	…	0	…	0
2	0	0,016	…	0	…	0	…	0	…	0
…	…	…	…	…	…	…	…	…	…	…
10	0	0	…	0,008	…	0	…	0	…	0
…	…	…	…	…	…	…	…	…	…	…
28	0	0	…	0	…	0,007	…	0	…	0
…	…	…	…	…	…	…	…	…	…	…
1001	0	0	…	0	…	0	…	0,0005	…	0
…	…	…	…	…	…	…	…	…	…	…
1764	0	0	…	0	…	0	…	0	…	0,00002

Далее преобразование исходных данных сети заключается в нахождении и построении диагональной матрицы удельного баланса трафика в вершинах социальной сети Flickr.

На данном этапе будет учитываться не сумма, а разность исходящего и входящего для вершины трафиков. Рассчитаем его по формуле (5):

$$\delta(\bar{B}_s) = \frac{\left[\sum_i \delta(a_{si}) - \sum_j \delta(a_{js})\right]}{\sum_{\substack{i,j \\ i \neq j}} \delta(a_{ij})}, \quad (5)$$

где: $\delta(a_{si})$ – вес трафика в исходящей и узла a_{si} дуге;

$\delta(a_{si})$ – вес трафика во входящей в узел a_{js} дуге.

В результате данных вычислений получим диагональную матрицу удельного баланса трафика в вершинах сети (табл. 5).

Таблица 5 - Матрица удельного баланса трафика в вершинах социальной сети Flickr

Номер узла	1	2	…	10	…	28	…	1001	…	1764
1	0,023	0	…	0	…	0	…	0	…	0
2	0	0,016	…	0	…	0	…	0	…	0
…	…	…	…	…	…	…	…	…	…	…
10	0	0	…	0,008	…	0	…	0	…	0
…	…	…	…	…	…	…	…	…	…	…
28	0	0	…	0	…	0,007	…	0	…	0
…	…	…	…	…	…	…	…	…	…	…
1001	0	0	…	0	…	0	…	-0,0005	…	0
…	…	…	…	…	…	…	…	…	…	…
1764	0	0	…	0	…	0	…	0	…	-0,00002

Так как социальная сеть достаточно велика, что затрудняет ее анализ, следует сделать некоторую выборку, которая в полной мере отражает все основные свойства сети. Тривиальный подход заключается в отборе вершин по их степени, то есть количеству инцидентным им дуг. Однако такой подход не учитывает тот факт, что каждая дуга имеет свой вес, т.е. отсутствует взвешенная оценка с точки зрения трафика.

Суть указанного алгоритма состоит в том, что из полученных квадратных матриц взвешенности следует получить усеченное количество узлов, которые способны с сохранением подобия описать исходную сетевую структуру [15].

Поэтому в предложенном алгоритме уместно использование квадратной матрицы взвешенной центральности элементов сети, а точнее – ее диагонали, где определена степень взвешенной центральности каждой вершины (табл. 6).

Таблица 6 – Степени взвешенной центральности вершин

Номер узла	Степень взвешенной центральности узла
1	0,023
2	0,016
3	0,0013
6	0,0061
10	0,008
15	0,0047
28	0,007
1001	0,0005
1764	0,0002

Далее необходимо проранжировать степени узлов матрицы по убыванию (табл. 7):

Таблица 7 – Проранжированные степени взвешенной центральности вершин

Номер узла	Степень взвешенной центральности узла
1	0,023
2	0,016
3	0,0013
10	0,008
28	0,007
6	0,0061
15	0,0047
1001	0,0005
1764	0,0002

Затем просуммируем полученные значения до получения необходимого результата (точности модели). В нашем случае - до значения 0.95, так как для нас допустима 5% потеря трафика, полученная сумма должна быть не меньше 0,95 [16]. Этим критерием и ограничится репрезентативная, с точки зрения трафика, выборка, рассчитанная по формуле (5):

$$\delta(\bar{x}_s) = 0{,}02321 + 0{,}01611 + 0{,}01311 + \cdots + 0{,}00021 = 0{,}9512. \quad (5)$$

При данном суммировании получена выборка из 332 элементов.

Далее обнулим столбцы и стоки, на пересечении которых стояла исключенная вершина. На основе данного усечения построим следующую матрицу (табл. 8):

Таблица 8 – Проранжированная усеченная матрица социальной сети Flickr

Порядковый №		1	2	…	72	…	321	322	…	332
	№ узла	1	2	…	15	…	28	1001	…	1764
1	1	$3005 \cdot 10^{-7}$	0	…	0	…	0	0	…	0
2	2	0	0	…	0	…	0	0	…	0
3	3	0	$2778 \cdot 10^{-7}$	…	0	…	$1452{,}8 \cdot 10^{-7}$	0	…	0
…	…	…	…	…	…	…	…	…	…	…
71	10	0	0	…	$1585{,}6 \cdot 10^{-7}$	…	0	0	…	0
…	…	…	…	…	…	…	…	…	…	…
321	28	0	0	…	0	…	0	$1352{,}8 \cdot 10^{-7}$	…	0
322	1001	0	0		0		0	0		0
…	…	…	…	…	…	…	…		…	…
332	1764	0	0	…	0		0	0		0

На основе полученной статистики построим усеченный граф исследуемого участка социальной сети Flickr при помощи программного обеспечения Gephi (https://gephi.org) [17]. Полученные результаты проиллюстрированы на рисунке 6.

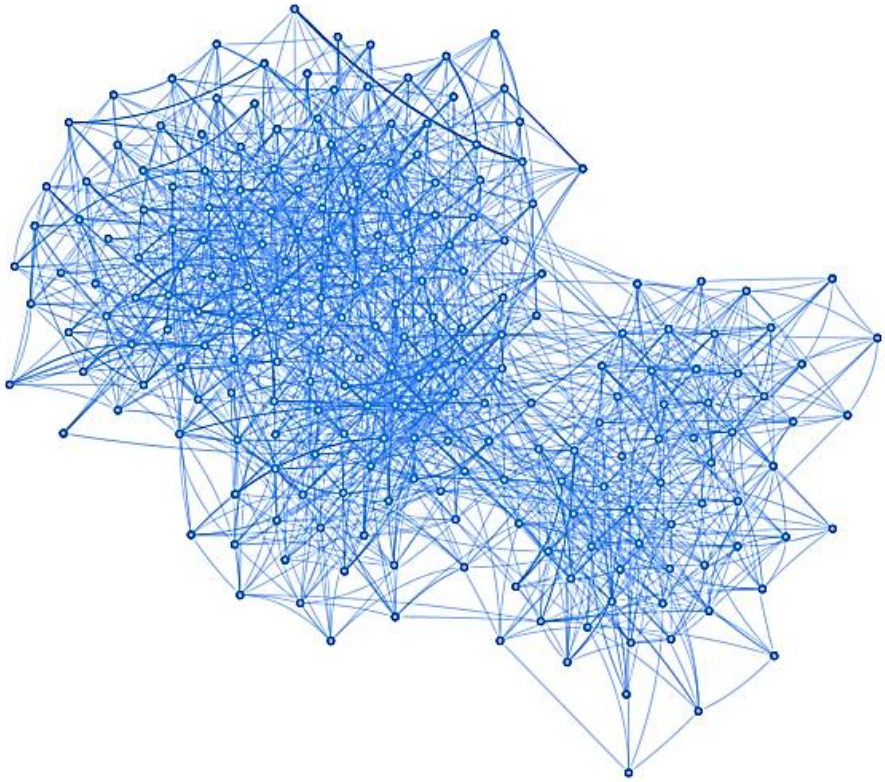

Рис. 6. Выборка социальной сети Flickr

Стоит отметить, что у данной социальной сети прослеживается небольшая кластерность. Это зависит от возможностей авторизованных пользователей, так как любой авторизованный пользователь может загрузить контент, прокомментировать его и сохранить к себе в закладки. При этом в данной социальной сети также существует система подписок, позволяющая при подписке на какую-либо страницу видеть загружаемый на нее контент, что способствует образованию кластеров вокруг наиболее популярных страниц.

Следующий этап алгоритма состоит в формировании итоговой матрицы в виде, удобном для последующего моделирования информационной диффузии.

Данная матрица представлена в таблице 9:

- недиагональные элементы равны ±1, так как интересует лишь факт смежности вершин истоков (+1) и стоков (-1). В некоторой степени это возврат к формату матрицы смежности;

- диагональные элементы имеют вес *k*, равный сумме элементов (+1) столбца.

Таблица 9 – Модифицированная матрицей смежности социальной сети Flickr

№ узла	1	2	3	…	20	21	22	…	100	101	102	…	362
1	364	-1	-1	…	-1	-1	-1	…	-1	-1	0	…	0
2	1	254	-1	…	-1	-1	0	…	0	0	0	…	0
3	1	1	202	…	0	-1	-1	…	0	0	0	…	0
⋮	⋮	⋮	⋮	⋱	⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮
20	1	0	0	…	44	0	-1	…	0	0	-1	…	0
21	1	1	1	…	0	110	0	…	0	0	0	…	0
22	1	1	1	…	1	0	62	…	0	0	-1	…	0
⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋱	⋮	⋮	⋮	…	⋮
100	1	1	0	…	0	0	0	…	19	-1	0	…	0
101	1	1	0	…	0	0	0	…	1	18	-1	…	0
102	0	1	0	…	1	0	1	…	0	1	39	…	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱	⋮
362	0	0	0	…	0	0	0	…	0	0	0	…	6

Таким образом, после применения предложенных преобразований исходных данных сети была получена репрезентативная выборка и получена визуальная модель сети Flickr вместе с соответствующими матрицами, способными охарактеризовать распространение контента в данной социальной сети.

Для того чтобы с уверенностью можно было пользоваться усеченной моделью, необходимо доказать подобие основной сети ее выборке. Одним из возможных способов доказать это (на основе доказательства о принадлежности полученной выборки сети к степенному закону распределения) является критерий Пирсона [18].

Посчитаем критерий Пирсона для выборки сети Flickr по формуле (6):

$$\chi^2_{набл} = \sum_{i=1}^{k} \frac{(n - np_i)^2}{np_i}, \quad (6)$$

где n – объем выборки;

p_i - вероятность попадания случайной величины X.

Тогда, следуя представленной формуле (6), рассчитаем значение χ^2. В данном случае $\chi^2 = 5.54$. Теперь посчитаем $n = 14$ (выборка) – 1 (количество параметров в плотности степенного распределения) = 13 (число степеней свободы). Выберем уровень значимости $\alpha = 0{,}05$, тогда $p = 1 - \alpha = 0.95$ [18]. Табличное значение $\chi^2(13)$ равно 5.89. Получается, что табличное значение χ^2 больше вычисленного. Следовательно, гипотеза верна, и приведенное степенное распределение согласуется с результатами эксперимента, что и требовалось доказать.

Следующим шагом, рассчитаем среднеквадратические отклонение (СКО) для исходной сети и полученной репрезентативной выборки по формулам (7) и (8):

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i, \quad (7)$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(X_i - \overline{X}\right)^2}, \quad (8)$$

где: n – общее число вершин;

X_i– i-ый элемент выборки;

$\overline{X}$– среднее арифметическое выборки;

σ– среднеквадратическое отклонение.

Тогда получим: $\sigma_1 = 0.303$ – СКО генеральной совокупности; $\sigma_2 = 0.281$ – СКО репрезентативной выборки.

Отклонение между эталоном (генеральной совокупностью) и полученной выборкой получилось равным 4,79%. Это доказывает, что репрезентативная выборка подобна генеральной совокупности с заданной точностью 5% [16]. Наглядно это можно изобразить на гистограмме распределения вершин (рис. 7), оси которой являются k (степень вершины) и P(k) (вероятность попадания вершины со степенью k в заданный интервал).

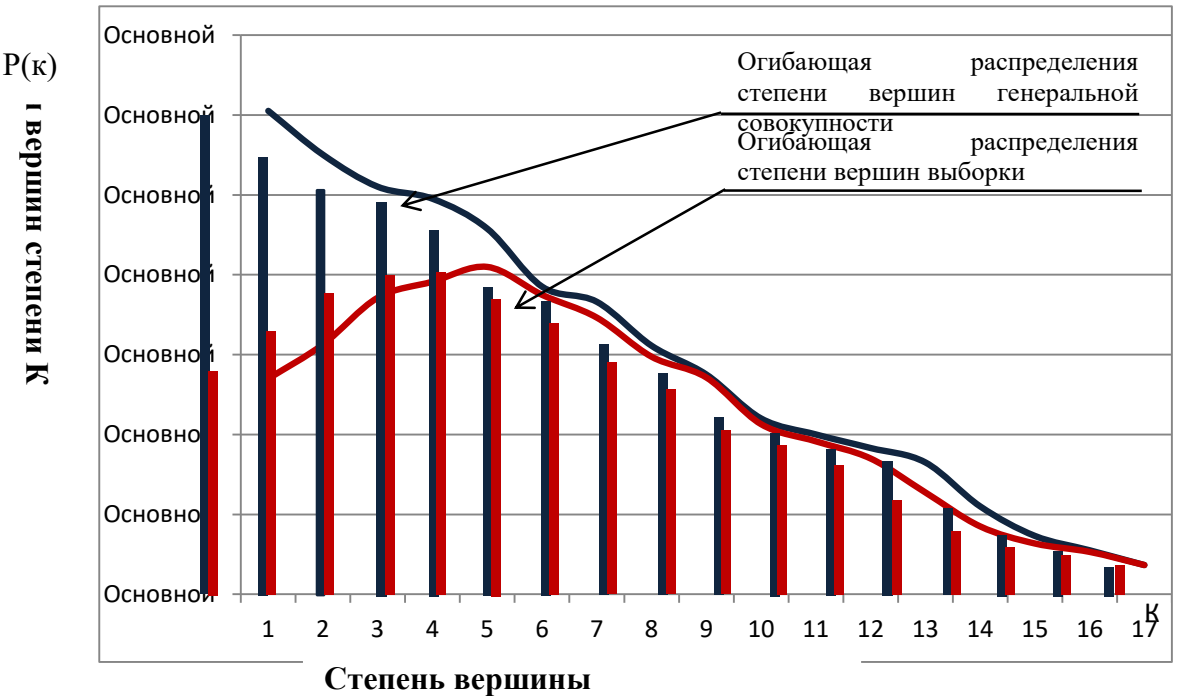

Рис. 7. Соотношение распределения генеральной совокупности и выборки.

Таким образом, доказано подобие генеральной совокупности основной сети и полученной в результате применения алгоритма выборки, а также сделан вывод, что выборка для сети Flickr соответствует степенному закону, поэтому она является подобной своей основной сети.

Это поможет в исследовании, состоящем в оценке и регулировании рисков, возникающих в сети при воздействии на нее деструктивного или

вредоносного контента [19-21]. Для этого необходимо в дальнейшем решить следующие задачи:

1. Используя построенную модель сети, смоделировать сетевой эпидемический процесс.

2. Предложить управление рисками с учетом определенного вероятного ущерба информационной эпидемии по суммарному весу матриц смежности, матриц взвешенности и послойной внутрисетевой связности [22-24].

Литература:

1. Информация о социальной сети Flickr. - Электрон. Дан. - Режим доступа: https://ru.wikipedia.org/wiki/Flickr

2. 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.

3. Principles of scientific research team formation and evolution Proc. Natl. Acad. Sci. USA 2014. – P. 89-91.

4. Evolution and convergence of the patterns of international scientific collaboration Proc. Natl. Acad. Sci. USA 2016. – P. 57-61.

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

6. Antsupov, A. Ya. Conflictology: the textbook for higher education institutions / A.Ya. Antsupov, A. I. Shilov. - 3rd prod., reslave, and additional - SPb.: St. Petersburg, 2007. – 591 p.

7. Bachilo, I. L. About the concept of legal support of informatization of Russia. Legislative problems of informatization of society/I.L. Bachilo, G. V. Belov / - M.: World, 1992. – 400 p.

8. Bachilo, I. L. Information right. The textbook Under the editorship

of the academician of RAS B. N. Topomina/I.L. Bachilo, V. N. Lopatin, M. A. Fedotov and other / SPb.: Legal center, 2001. – 789 p.

9. Bachilo, I. L. Information right: fundamentals of practical informatics: Education guidance / I.L. Bachilo / - M: Edition of Mr. M. Yu. Tikhomirov, 2001. – 352 p.

10. Byrd, K. War with many unknowns / K. Byrd//Computerra. - M. Moscow: 2009. - No. 20. – P. 5-9.

11. Grinyaev, S. Russia in global information society: threats, risks and possible ways of their neutralization / S. Grinyaev, - Access mode: http://www.noravank.am/upload/pdf/419_ru.pdf.

12. Kalashnikov, A.O. Attacks to information and technological infrastructure of crucial objects: assessment and regulation of risks: Monograph / A.O. Kalashnikov, E. V. Yermilov, O. N. Choporov, K. A. Razinkin, N. I. Barannikov; under the editorship of the Member correspondent of RAS D. A. Novikov. - Voronezh: Scientific Book publishing house. 2013. – 160 p.

13. Стрельников А. Н. Социальные сети: механизмы работы и пути развития. Электронные данные - Режим доступа: http://www.rae.ru/forum2011/153/1796.

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

15. Social Network Analysis John Scott от 19 ноября 2013 г. SAGE - Электрон. дан. - Режим доступа: http://www.pnas.Org/content/98/2/404.full.

16. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН ДА. Новикова. - Москва, 2010. – 116 с.

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

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

c.

19. 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.

20. 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 Journal. -2013. -25 (3). – P. 410-415.

21. 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.

22. 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.

23. 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.

24. 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.

Региональный учебно-научный центр по проблемам
информационной безопасности

Воронежский научно-образовательный центр управления
информационными рисками

УДК 004.056.57

РЕКОМЕНДАЦИИ ПО УПРАВЛЕНИЮ РИСКАМИ И СТРУКТУРНОЙ ЖИВУЧЕСТЬЮ ПРИ УГРОЗЕ РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В КОРПОРАТИВНОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ С ЯРКО ВЫРАЖЕННОЙ КЛАСТЕРИЗАЦИЕЙ

В.А. Волков, Е.Н. Пономаренко, О.Н. Чопоров,
Н.М. Радько, Ю.К. Язов

Объектом исследования является корпоративная информационно-телекоммуникационная сеть с ярко выраженной кластеризацией, в которой имеет место распространение деструктивного контента.

В исследуемой сети на первых шагах распространения нежелательной информации структурно-функциональные особенности сети допускают вывод из строя множества ключевых узлов, по этой причине важнейшей задачей является снижение рисков и повышение структурной живучести.

Минимизировать риски и повысить структурную живучесть при распространении деструктивного контента в корпоративной информационно-телекоммуникационной сети с ярко выраженной кластеризацией можно различными способами.

Будь то конечные пользователи, файловый сервер, почтовый сервер, веб-сервер или же прокси-сервер, настоятельно рекомендуется установление продуктов, направленных на защиту от вредоносного программного обеспечения.

На центральных узлах сети рекомендуется возвести системы обнаружения вторжений (СОВ). Их установка может быть

нецелесообразна в некоторых случаях, поэтому решение об установке напрямую зависит от материальных средств, которые готовы затратить предприятия на ее реализацию. Существует два вида СОВ по принципу действия: пассивная и активная. В пассивной СОВ при обнаружении нарушения безопасности информация о нарушении записывается в отчет приложения, а также отправляется уведомление на консоль и/или администратору системы по определенному каналу связи. В активной системе, также известной как Система Предотвращения Вторжений (IPS — Intrusion Prevention System), СОВ ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника. Ответные действия могут проводиться автоматически либо по команде оператора [1].

Также для защиты от несанкционированного доступа могут применяться межсетевые экраны, которые пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами [2].

Хотя и СОВ, и межсетевой экран относятся к средствам обеспечения информационной безопасности, межсетевой экран отличается тем, что ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети. СОВ, в свою очередь, пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил и анализа сигнатур известных компьютерных атак.

В исследуемых сетях целесообразно применять и статическую, и динамическую фильтрацию вредоносного контента, так как они дополняют друг друга.

Суть статической фильтрации заключается в следующем. Пакетный файрвол инспектирует входящий трафик, анализируя информацию

сетевого и транспортного уровней модели OSI. Если пакет, не удовлетворяет правилам заданным в списке контроля доступа - Access Control List (ACL), по которым он может быть пропущен в защищенную сеть, пакет отбрасывается. Преимущество статической пакетной фильтрации в ее быстродействии. Основной особенностью статической фильтрации является блокирование нежелательных web-ресурсов. К разновидностям реализации таких блокировок относятся следующие блокировки: по имени DNS или IP- адресу; по ключевым словам контента; по типу файла; фильтрация через HTTP прокси-сервер [3].

Недостатком данного вида фильтрации является то, что пользователь может ввести адрес, который не принадлежит ни одному из списков. Тогда система фильтрации не опознает страницу и допустит пользователя к содержимому, что может привести к негативным последствиям. Для устранения этого недостатка используют динамическую фильтрацию [3].

Технология динамической фильтрации обеспечивает лучшую комбинацию безопасности и производительности. Используется не только ACL, но также анализируется состояние сессии, записываемое в базу, которую называют таблицей состояния (state table). Принцип работы состоит в том, чтобы анализировать содержимое веб-страницы до загрузки на устройство пользователя и в зависимости от настроек фильтра показывать страницу частично, если был найден негативный контент [3]. Данная разновидность фильтрации сканирует страницу заново с момента последнего сканирования, чтобы проверить её и занести данные в таблицу состояния.

Немаловажным является общий уровень «грамотности» пользователей в сфере информационной безопасности, он должен быть высоким для всех пользователей сети. Повышение данного уровня может осуществляться посредством организации плановых мероприятий сотрудниками IT-отдела. Это необходимо для предотвращения

возможности проведения информационно-психологических и компьютерных атак.

При наличии «экономической поддержки» со стороны начальства отличным решением будет выступать сегментация сети посредством выделения нескольких узлов, к которым будут обращаться другие узлы. Структура сети при этом будет иметь следующий вид (рис. 1):

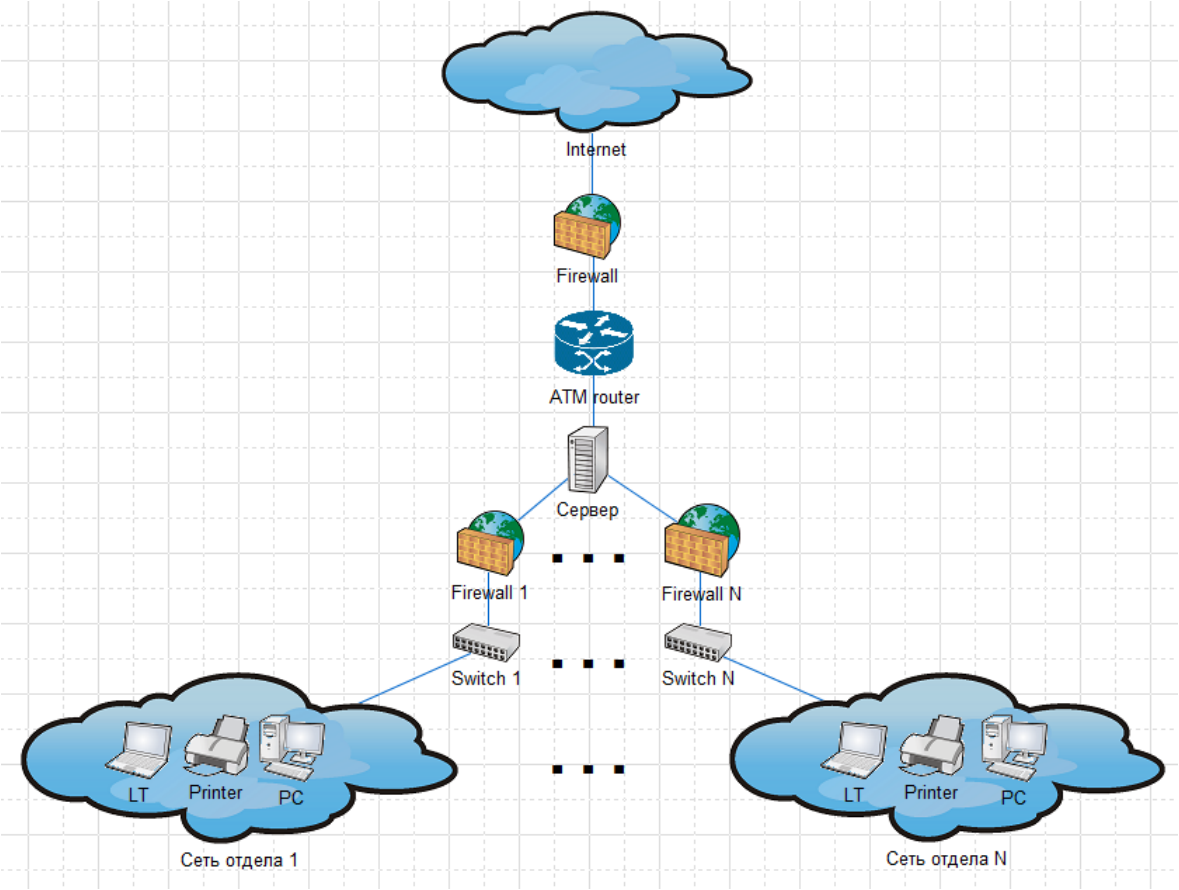

Рис. 1. Рекомендуемая структура корпоративной сети

В случае невозможности разделения всех отделов на подсети, некоторые смежные по функциям отделы можно совместить в одну подсеть.

Одной из основных рекомендаций выступает обеспечение пользователей минимальными привилегиями, необходимыми для выполнения конкретной работы, что может затруднить распространение деструктивного контента в сети.

Также, место расположения защитных механизмов должно быть конфиденциальной информацией, что может затруднить несанкционированный доступ к информации изнутри сети.

Анализ эпидемического процесса проводился с ориентиром на случай моделирования, при котором атаке подвергался один узел сети, являющийся непосредственным участником определенного кластера сети, т.е. сотрудник отдела или службы предприятия, а один шаг эпидемического процесса равнялся 30 минутам реального времени.

Исходя из вышенаписанного, можно предложить следующие рекомендации по минимизации рисков и повышения структурной живучести сети при распространении деструктивного контента:

1) Необходимо единовременное установление защитного программного обеспечения (ПО) на всех компьютерах сети.

2) Проводить обновление баз сигнатур вредоносного ПО каждые 4 часа рабочего времени.

3) Обновление системного ПО проводить не реже одного раза в день до начала эксплуатации компьютеров работниками.

4) Единовременно возвести пассивную систему обнаружения вторжений (СОВ) на центральных узлах сети или в ее сегментах.

5) Калибровку СОВ проводить не реже одного раза в неделю в свободное от эксплуатации время.

6) Единовременно установить межсетевые экраны (МЭ) с блокировкой внешних ресурсов, не относящихся к деятельности предприятия.

7) Проводить повторную настройку МЭ через один рабочий день и при добавлении новых внешних ресурсов в список блокировок.

8) Единовременное возведение системы динамической фильтрации и проведение ее повторной настройки аналогично настройке МЭ.

9) В начале каждой рабочей недели проводить инструктаж по информационной безопасности среди сотрудников для повышения общего уровня «грамотности» пользователей в сфере информационной безопасности.

10) Проведение единовременной сегментации сети.

11) Анализ и изменение структуры сети проводить каждый раз при добавлении в нее новых элементов.

12) Единовременное выделение минимальных необходимых привилегий пользователей.

13) Проводить проверку и переопределение привилегий пользователей не реже одного раза в рабочую неделю и при изменении привилегий у существующих пользователей.

14) Смена паролей пользователей должна производиться не реже одного раза в квартал; для облегчения запоминания паролей их состав должен содержать два несвязанных между собой слова.

15) Единовременное сокрытие местоположения систем защиты.

Принятие определенных решений по защите информации основывается на анализе иерархической структуры сети (рис. 1).

Литература:

1 IDS/IPS — Системы обнаружения и предотвращения вторжений. – Электрон. дан. – Режим доступа: http://www.netconfig.ru/server/ids-ips/.

2 Что такое межсетевой экран? – Электрон. дан. – Режим доступа: http://www.cisco.com/c/ru_ru/products/security/firewalls/what-is-a-firewall.html.

3 Технологии фаерволов. – Электрон. дан. – Режим доступа: http://www.ciscolab.ru/security/1-tehnologii-faervolov.html.

Региональный учебно-научный центр по проблемам информационной безопасности

Воронежский научно-образовательный центр управления информационными рисками

Научное издание

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Сборник научных трудов

Вып. 1 (15), 2017

Под редакцией чл.-корр. РАН В.И. Борисова

Главный редактор А.Г. Остапенко

Издание публикуется в авторской редакции

Компьютерная верстка Е.Ю. Чапурин

Дизайн обложки С.А. Кравец

Подписано в печать __.12.17. Формат __. Усл. печ. л. __.

Заказ ____Тираж 500 экз.