



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

ОГЛАВЛЕНИЕ

1 Особенности специализированных социальных сетей для авторских записей как объекта воздействия деструктивного вредоносного контента	9
1.1 Анализ структурно-функциональной специфики специализированных социальных сетей для авторских записей	9
1.2 Анализ специфики вредоносного контента, распространяемого в сетях для авторских записей	25
1.3 Анализ распространения вредоносного контента на примере реального «вброса» деструктивного контента	40
1.4 Выводы по первой главе	45
2 Сбор статистических данных, построение выборок матрицы взвешенной инцидентности и оценка степени их подобия	46
2.1 Сбор статистических данных сетей для авторских записей	46
2.2 Выборка матрицы взвешенной инцидентности и ее построение для специализированных сетей для авторских записей с сохранением подобия исходной топологии сети	51
2.3 Оценка степени подобия исходных и выборок матриц взвешенной инцидентности	55
2.4 Выводы по второй главе	63
3 Построение матриц взвешенной центральности, послойной внутрисетевой связанности, микро-фракталов заражения, а также оценка вероятности и ущерба для вредоносного контента в сетях для авторских записей	64
3.1 Построение матриц взвешенной центральности сетей для авторских записей	64
3.2 Построение матриц внутрисетевой послойной связанности выборок сети для авторских записей	70
3.3 Варианты построения микро-фракталов заражения, оценка вероятности и ущерба для вредоносного контента в сетях для авторских записей	76
3.4 Выводы по третьей главе	85



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

projectIT

projectIT

4 Моделирование эпидемических процессов для каждой разновидности сетей и различных вариантов атак на вершины с повышенной взвешенной центральностью с использованием автоматизированного ПО и анализ полученных результатов 86

projectIT

projectIT

4.1 Численное моделирование эпидемических процессов заражения для каждой разновидности сети с использованием автоматизированного ПО в контексте атак на критически важные узлы 86

projectIT

projectIT

projectIT

4.2 Анализ полученных результатов численного моделирования 96

projectIT

projectIT

4.3 Разработка рекомендация по управлению эпистойкостью в контексте атак на критически важные узлы различных сетей для авторских записей 99

4.4 Выводы по четвертой главе 103



Заключение

8 (952) 106-88-60



vk.com/a.projectit



a.projectit

104

Список литературы

105

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT



ВВЕДЕНИЕ

projectIT

projectIT

projectIT

Актуальность темы исследования. С развитием технологий появился такой вид информации, как электронный контент, потребляемый все большей частью современного общества. Вследствие этого распространенными стали различные электронные площадки[1][2], с одной стороны, для потребления контента пользователями, с другой, для авторов: мощный и достаточно простой инструмент для публикации и монетизации производимого контента. Так, самые читаемые авторы сетей для авторских записей, например, «Живой Журнал», «Twitter», «Blogger» получают большое количество денежных средств за счет показа рекламы пользователям[3].

projectIT

projectIT

projectIT

Очевидно, что данные публицисты ценят каждого подписавшегося пользователя, отдающего свое свободное время для потребления конкретного авторского контента[4], так как за это издатель получает денежное вознаграждение за использование рекламодателями данной площадки для показа рекламы. В следствии этого каждый, кто пользуется электронной площадкой для авторских записей с целью создания контента, старается удержать читающих его людей (которые являются критично важным активом, если говорить на языке «управления рисками», для автора) не только уникальностью, новизной информации, но и безопасностью потребления контента[5][6] на данной конкретной площадке.

projectIT

projectIT

projectIT

Таким образом, проблема управления рисками[7] в сетях для авторских записей становится очень остро, так как ни автор записей не желает заразить потребителей его контента вредоносным программным обеспечением[8] [9][10][11], так как это влечет потерю прибыли, ни потребитель контента не хочет оказаться инфицированным, потерять доверие к данному публицисту и перестать потреблять интересный для данного человека контент, как минимум, либо невольно оказаться дальнейшим распространителем эпидемии[12], потерять свои данные на компьютере, как максимум, поэтому в настоящее время ведется активное противоборство распространителей вредоносного контента, пытающихся за счет аудитории автора реализовать свои злонамеренные замыслы и авторов, которые

projectIT

projectIT

projectIT

стремятся максимально снизить информационные риски [13] [14], при удачном инфицировании потребителя контента.

Количество попыток распространения вредоносного контента постоянно возрастает что говорит о постоянном росте интереса злоумышленников к осуществлению различных злонамеренных планов посредством сетей для авторских записей, что влечет, несомненно, развитие как способов, средств, механизмов распространения деструктивного контента среди пользователей [15] [16] [17] так и разработку новых технологий по защите, методологий по управлению информационными рисками в сетях для авторских записей. Так, например, злоумышленнику достаточно разместить комментарий к авторской записи со ссылкой на вредоносное программное обеспечение и при высоком показателе посещений электронной площадки, вероятность и масштаб распространения вредоносного контента возрастает крайне стремительно [18].

Стоит отметить, что текущие исследования распространения вредоносного контента опираются на степени узлов [19] (агентов, авторов записей), что, очевидно, в настоящее время не отражает действительной ситуации в сетях для авторских записей, где первостепенное значение имеют веса ребер, то есть коэффициент влияния [20] [21] [22].

Иными словами, в настоящее время наиболее остро становится вопрос не количества, а «качества» пользователей данной сети и применительно к сетям для авторских записей, можно привести следующий пример, дающий понимание почему исследования в области взвешенных сетей наиболее актуальны.

В работе «модели влияния в социальных сетях» Губанова Д.А. впервые произведен обзор основных классов моделей социальных сетей, а также установлены соответствий между классами моделей и отражаемыми ими свойствами моделируемого объекта, учитывая при этом веса ребер [23] [24] [25]. Автор обращает внимание, что многие решения принимаются на основании мнения одного агента или группы агентов социальной сети, которые стремятся навязать свое мнение другим и что проблема управления мнениями пользователей сети стоит очень остро, так как предполагают специфику задач и



математического аппарата и методов их решения, что в настоящее время не исследовано.

Таким образом, актуальность исследования может быть обусловлена:

1) Широким охватом аудитории автора (так, например, у одного из популярных авторов сети Живой Журнал, количество среднемесячной аудитории составляет 3 миллиона 964 тысячи человек по состоянию на 31 декабря 2015 года)[26], что, при удачном управлении мнениями пользователей данной сети, может привести к деструктивно-управляющему воздействию;

2) Отсутствием исследований сетей для авторских записей, учитывая степени влияния агентов сети, при распространении вредоносного контента во взвешенной сети данного типа;

3) Отсутствие на настоящее время исследований в сфере управления рисками в сетях для авторских записей при распространении вредоносного контента, оказывающего деструктивно-управляющее воздействие на пользователей данной сети.

Степень проработанности темы исследования. Касательно вопросов исследования информационными рисками [27][28][29][30][18] в социальных сетях [7][31][14] и, в частности, риск-анализа состояний пользователей социальных сетей, опубликовано достаточно много работ, в которых проанализированы и структурированы как сами способы распространения вредоносного контента, так и были предложены меры и средства для противодействия. Однако, стоит отметить, что уже опубликованные работы применялись к широкому кругу сетей, что не дает в достаточной мере исследовать информационные риски в специализированных сетях для авторских записей. Так же не были классифицированы уязвимости пользователей конкретных специализированных сетей, что не позволяло построить риск-модель распространения вредоносного контента применительно к сетям для авторских записей.

Немаловажным фактором актуальности темы исследования является, что ранее популярные модели для невзвешенных сетей, которые считали ребра лишь



наличием или отсутствием связи между пользователями, не давали возможности узнать, как быстро информация распространится, степень влияния агента сети на других агентов и др., что приводит к невозможности моделирования различных процессов в реальных социальных сетях при распространении информационного деструктивного контента[22], а так же получения различных численных значений риска, ущерба, пользы, эпистойкости.

Таким образом, исследования касательно информационных рисков пользователей сетей для авторских записей при распространении вредоносного контента представляется актуальным.

Работа выполнена в соответствии с одним из основных направлений ФГБОУ ВПО «Воронежский государственный технический университет» «Управление информационными рисками и обеспечение безопасности инфокоммуникационных технологий» на базе Воронежского научно-образовательного центра управления информационными рисками.

Объектом исследования являются сети для авторских записей, которые подвергаются деструктивному воздействию вредоносного контента, распространяемого в данной сети.

Предметом исследования является микромодель процесса распространения и заражения пользователей сетей для авторских записей, получающих вредоносный контент на основе анализа микрофракталов для разновидностей сетей для авторских записей.

Цель исследования состоит в анализе информационных рисков пользователей сетей для авторских записей при распространении вредоносного контента. Для достижения цели представляется необходимым решить следующие задачи:

1) Исследование, анализ, классификация сетей для авторских записей и циркулирующего вредоносного контента, а также формализация сети как взвешенного графа с последующим сбором статистики на основе трёхместного предиката для построения матриц взвешенной инцидентности с последующей передачей партнеру по комплексной работе;



2) Получение от партнера по комплексной работе различных метрик и матриц взвешенной центральности, рассчитанных с помощью автоматизированного программного обеспечения, разработанного партнерами по комплексной работе, для каждой разновидности сетей для авторских записей;

3) Разработка микромоделей распространения деструктивного контента для разновидностей сети для авторских записей на основе структурно-функциональной специфики данных сетей, а также построение матриц послойной связности и взвешенной центральности для дальнейшего численного моделирования эпидемических процессов.

Результаты, выносимые на защиту. На защиту выносятся:

1) Матрицы взвешенной центральности, построенные на основе собранной статистики в виде трехместного предиката, которая отражает силу связи между узлами сети;

2) Матрицы взвешенной центральности, полученные с помощью разработанного специализированного программного обеспечения, позволяющие определить наиболее центральные вершины в различных сетях для авторских записей;

3) Микромодель распространения деструктивного контента, циркулирующего в сетях для авторских записей, полученная на основе разработанных микрофракталов и численного моделирования эпидемиологических процессов, что в итоге позволяет получить следующие численные значения: риск, ущерб, эпистойкость.

Методы исследования. В исследовании используются методы системного анализа, теории вероятностей, математической статистики, математического анализа, методы теории управления риском.

Новизна результатов состоит в следующем:

1) Впервые была построена матрица взвешенной инцидентности сетей для авторских записей на основе собранных статистических данных в виде трехместных предикатов;



2) Впервые на основе матриц взвешенной инцидентности были построены матрицы взвешенной центральности, отражающие вершины, требующие повышенной защиты в случае начала эпидемии, либо представляющие наибольшую опасность для сети в целом;

3) Впервые было проведено численное моделирование эпидемических процессов на основе построенных матриц послойной внутрисетевой связанности и разработанных микрофракталов распространения вредоносного контента разновидностей сетей для авторских записей.

Теоретическая значимость работы состоит в следующем:

1) Был произведен анализ и доказательство воздействия деструктивного контента на пользователей сетей для авторских записей, а также произведена оценка информационных рисков при эпидемических процессах на основе определенной ценности узлов сетей для авторских записей;

2) Построена микромодель, применив которую становится возможным оценить опасность распространения вредоносного контента среди пользователей сетей для авторских записей;

3) В методике анализа численных результатов моделирования и определении наиболее опасных вершин сети для авторских записей, что может послужить для дальнейшего управления информационными рисками в данной разновидности сетей;

Практическая ценность результатов:

1) На основе структурно-функциональных особенностей сетей для авторских записей и циркулирующего деструктивного контента были выявлены признаки вредоносного контента, а формализация сети в качестве взвешенного графа и применение ценности к каждой его вершине позволяет определить ущерб после реализации атаки;

2) Построенные микромодели распространения вредоносного контента и его влияние на пользователей данной сети дают возможность использовать разработанные модели для разнообразных видов контента, а также применительно к различным сетям для авторских записей;



3) Проведенный анализ матриц взвешенной инцидентности, взвешенной центральности позволяет определить логику связей между вершинами, а в результате анализа матрицы послойной внутрисетевой – позволяет однозначно сказать, как будет распространяться заражения пользователей сетей для авторских записей;

4) Численное моделирование эпидемиологических процессов распространения вредоносного контента позволило определить, насколько быстро произойдет заражение сети, как долго сеть будет оставаться «живой», а также получить значения риска, ущерба, пользы, эпистойкости сети на протяжении эпидемии.

Методы исследования. В исследовании применяются методы системного анализа, математического и риск – анализа, теории вероятностей и математической статистики, теории графов, а также применение специализированного компьютерного программного обеспечения, разработанного партнерами по комплексной работе.





ЗАКЛЮЧЕНИЕ

Таким образом, проведенное в данной выпускной квалификационной работе исследование, цель которого состоит в анализе информационных рисков пользователей сетей для авторских записей при распространении вредоносного контента, порождает ряд задач, которые необходимо было решить.

При решении первой задачи, была описана структурно-функциональная специфика специализированных сетей для авторских записей, после чего стало очевидным, что несмотря на схожую структуру, основанную на графах, данные сети имеют значительные специфические различия, а анализ специфики и классификация вредоносного контента, циркулирующего в данных сетях, позволил наиболее точным образом описать распространение данного контента по специализированным сетям для авторских записей. Так же был произведен анализ распространения вредоносного контента на примере реального заражения, а также разработаны схемы распространения контента при взаимодействии пользователя с хэш-тегами, сообществами.

Так же были собраны взвешенные статистические данные сетей для авторских записей, после чего стало возможным построить выборку матрицы взвешенной инцидентности, то есть уменьшение размеров исходной матриц до приемлемых для анализа размеров, а именно – до 400 вершин. Наряду с этим было доказано, что разработанный партнером по комплексной работе алгоритм выборки матрицы взвешенной инцидентности сохраняет топологию и иные свойства исходной сети, что позволяет минимизировать ресурсы для анализа сетей для авторских записей в контексте распространения вредоносного контента.

При решении второй задачи, от партнера по комплексной работе были получены различные метрики сетей для авторских записей, что позволяет оперировать конкретными числовыми характеристиками данных сетей, а также матрицы взвешенной центральности, на основе которых становится возможным определить наиболее приоритетные цели для злоумышленников в контексте распространения вредоносного контента.



При решении третьей задачи, была разработана микромодель распространения деструктивного контента в специализированных сетях для авторских записей, что позволяет применить данную модель и получить различные числовые характеристики эпидемиологических процессов. Так же, от партнера по комплексной работе были получены матрицы послышной внутрисетевой связанности, что дает возможность визуально увидеть «маршрут» распространения вредоносного контента, а построенные микрофракталы для разновидностей сетей предоставляют возможность провести эпидемиологическое моделирование и получить численные характеристики эпидемий, а именно: риск, польза, ущерб, эпистойкость и получить их в виде графиков, а так же разработка рекомендаций по управлению эпистойкостью в контексте атак на критически важные вершины.

Кроме того, после анализа полученных данных, можно судить о корреляции структурно-функциональной специфики различных сетей для авторских записей и смоделированных эпидемиологических процессов, что в дальнейших исследованиях становится возможным проведение как полного риск-анализа данных сетей, так и управления информационными рисками.

Однако, данная выпускная работа не охватывает всю специфику проблематики касаясь информационных рисков специализированных сетей для авторских записей, поэтому можно сформулировать несколько задач для будущих исследований:

- 1) Разработка и применение алгоритмов для оперирования взвешенной центральности ребер, что позволяет оценить наиболее уязвимые «магистральи», по которым может распространяться вредоносный контент;
- 2) Проведение детального риск-анализа пользователей сетей для авторских записей, учитывая всевозможную специфику данных сетей;
- 3) Разработка различных методик управления информационными рисками.