ВВЕДЕНИЕ

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, 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].

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 площадки.

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

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.

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 послойной 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 касаемо 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 «магистрали», 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.