НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ
ИНСТИТУТ ПРОБЛЕМ РЕГИСТРАЦИИ ИНФОРМАЦИИ НАН УКРАИНЫ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ

МАТЕРИАЛЫ XIX МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

ВЫПУСК 19

Киев – 2019

Рекомендовано к печати Ученым советом
Института проблем регистрации информации НАН Украины
(протокол № 3 от 24 декабря 2019 г.)

Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2019. – К.: ООО "Инжиниринг", 2019. – 236 с. ISBN 978-966-2344-72-1

В сборник вошли материалы докладов, представленных на XVI Международной научно-практической конференции «Информационные технологии и безопасность» (ИТБ-2019, 28 ноября 2019 года, г. Киев, Украина).

В сборнике представлены статьи, посвященные вопросам безопасности живучести критических инфраструктур, моделирования и противодействия информационным операциям, информационных технологий в управлении, методов и способов информационной поддержки принятия решений, комп'ютерного моделирования систем организационного управления, информационно-аналитических исследований на основе открытых источников информации, сценарного анализа при обеспечения информационной поддержки принятия решений, актуальным проблемам обеспечения информационной и кибернетической безопасности.

Для специалистов в области информационных технологий, информационной безопасности, информационного права а также для аспирантов и студентов старших курсов высшей школы соответствующих специальностей.

ISBN 978-966-2344-72-1

27. Kalichensky A.: The Concept of Creating the National Information and Communication Infrastructure of Ukraine. In: Regional Forum M SE, (2012), https: //www.itu.int/ITU-D/tech/events/2012/ Spectrum_ CIS_Kiev_Sept12/Presentatio ns / Session2 / A_Kalichensky _a.pdf.
28. Diorditsa I.V.: The presentation of the terminology of cybersecurity policy in the texts of regulatory acts of Ukraine. In: Scientific Bulletin of the International Humanities University. Jurisprudence Series, N 29 (1), pp. 64-67, (2017).
29. Gladun A., Rogushina J.: Use of Semantic Web Technologies and Multilinguistic Thesauri for Knowledge-Based Access to Biomedical Resources. In: International Journal of Intelligent Systems and Applications, №1, P.11-20, (2012), http://www.mecs-press.org/ ijisa/ijisa-v4-n1/IJISA-V4-N1-2.pdf.
30. Rogushina Yu.V. Use of Thesauri for Search of Complex Information Objects in the Web on Base of Ontologies. In: Problems in Programming, No. 4, pp.11-27. (2019) (in Ukrainian).

МЕТОДИ І ЗАСОБИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДТРИМКИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ ДЕРЖАВИ

Шнурко-Табакова Е.В.[1], Ланде Д.В. [1,2]

[1]ГО «Рада інформбезепеки та кіберзахисту»,

[2]ІПРІ НАН України

На цей час в Україні до протидії гібридним загрозам державі залучаються всі шари держави і суспільства, зокрема, силові структури держави, інші міністерства та відомства, недержавні організації, бізнес, громадянські об'єднання. З огляду на те, що ворог поряд із економічними, енергетичними, гуманітарними та іншими важелями, проти нашої країни широко застосовується інформаційна зброя, проводяться інформаційні операції, одним з першочергових завдань стає створення високоефективної системи інформаційно-аналітичної протидії гібридним загрозам держави.

Саме застосування таких підходів може забезпечити швидке оперативне реагування на загрози, виявлення інформаційних кампаній, атак, операцій [1], зокрема, виявлення мереж ворожих інформаційних ботів, прогнозування розвитку подій, явищ, процесів тощо.

Зокрема, потребує інформаційно-аналітичної підтримки протидія інформаційним операціям в мережі Інтернет, які умовно поділяються на «пропагандистські» (інформаційні впливи мають переважно пропагандистський характер), «дезінформаційні» (основною метою є дезінформація шляхом створення «фейків»), «маніпулятивні» (маніпулювання, модифікація установок людей), оборонні («контроперації» – нейтралізація інформаційного впливу супротивника).

Для рішення завдань інформаційно-аналітичної підтримки протидії загрозам такого роду мають застосовуватися найсучасніші методи і засоби аналітичної роботи, що базуються на використанні таких сучасних концепцій, як Data Science (наука про дані), Big Data (великі дані), Text/Data Mining (глибинний аналіз текстів/даних), методи нелінійного (кореляційного, фрактального) аналізу, Complex Networks (складні мережі), OSINT (розвідка за відкритими джерелами) тощо.

Для здійснення інформаційно-аналітичної підтримки мають застосовуватися методи і засоби, що дозволяють:

- виявляти кількісну динаміку, притаманну процесу чи явищу, наприклад, кількість подій або повідомлень щодо події в одиницю часу;
- визначати критичні, порогові точки, що відповідають кількісної динаміці явища;
- визначати прояви подій, процесів, об'єктів в критичних точках, наприклад, виявлення основних сюжетів повідомлень щодо обраного процесу або явища;
- ранжирування цих проявів і дослідження динаміки їх розвитку до та після певних критичних точок;
- здійснення статистичного, кореляційного і фрактального аналізу загальної динаміки і динаміки окремих проявів, на основі яких має здійснюватися прогнозування розвитку події, процесу і окремих його проявів.

Для дослідження взаємозв'язку реальних подій і публікацій про них в мережі Інтернет, зокрема, авторами використовується інформаційна OSINT-системах [2] InfoStream (http://online.infostream.ua), що забезпечує інтеграцію і моніторинг мережевих інформаційних ресурсів, а також аналітична система Attack Index (http://attackindex.com), що дозволяє визначати наявність і рівень інформаційних операцій на базі аналізу відкритих джерел. Використання статистичних методів аналізу інформаційних потоків, методів нелінійного, зокрема, фрактального аналізу, дозволяє прогнозувати розвиток подій або керованих інформаційних процесів. Шляхом застосування цих систем, даних, що отримуються від них, здійснюється як прогнозування реальних процесів, так і інтеграція із системами прийняття рішень.

Окремим питанням є методологія декомпозиції гібридних загроз до семантичного ядра, що має складати основу ключових запитів до інформаційно-аналітичних систем. Сучасні виклики вимагають створення системи рейтенгування загроз та регламентів відстеження ситуації в інформаційному просторі з безперервним супроводженням та реагування.

Сьогодні складні завдання інформаційно-аналітичної протидії, з одного боку, стимулюють розвиток систем керування знаннями, глибинного аналізу даних і текстів, а з іншого – найбільш розвинені із цих систем у явному вигляді містять адаптовані й готові до використання аналітичні блоки.

Для прийняття ґрунтовних рішень у галузі національної безпеки держави, зокрема щодо протидії гібридним загрозам, необхідне використання комплексних інформаційно-аналітичних систем, які дозволяють збирати, обробляти та узагальнювати інформацію, отриману з різних джерел із застосуванням різних технологічних рішень. Тому вже є широкий вибір засобів автоматизації інформаційно-аналітичної діяльності. Причому рівні функціональності таких систем можуть бути дуже різноманітним – від простих засобів контент-моніторингу та інформаційно-пошукових модулів, необхідних на етапі становлення аналітичних систем, до дорогих ресурсномістких систем керування знаннями та глибинного аналізу даних і текстів.

Зокрема, при аналізі тематичних інформаційних потоків із різних мережевих джерел, що аналізуються в системі контент-моніторингу, вирішується проблема формування і дослідження зв’язків інформаційних джерел, які розповсюджують маніпулятивну інформацію. При цьому підставою для можливого зв'язку між двома джерелами може служити той факт, що вони часто публікують документи, що збігаються або близькі за темою. За допомогою такої мережі можна визначити, які з інформаційних джерел з даної тематики є основними, найбільш впливовими, які схильні до певних інформаційних впливів. Підхід базується на тому факті, що джерела інформації ранжовані за обсягами публікацій виходячи з досвіду спостереження за ними протягом тривалого часу, тобто їм вже приписані деякі вагові значення.

Таким чином встановлюється зв'язок джерела інформації з іншим, більш рейтинговим, якщо він існує і опублікував інформацію раніше. Побудована таким чином мережу (Рис. 1) відображає зв'язок джерел по заданій тематиці, дозволяє визначати лідерів серед них, робити припущення щодо першоджерел інформації. Наприклад, на Рис. 5 показана мережа зв'язків джерел інформації із соціальних мереж, що відображають тематику «Формула Штанмайера» у жовтні-листопаді 2019 р за даними системи контент-моніторингу.

Сучасні системи інформаційно-аналітичної протидії гібридним загрозам забезпечують вирішення цілого комплексу проблем, серед яких збір інформації про об'єкти, визначення зв'язків об'єктів, виявлення тенденцій, прогнозування. Не слід вважати, що такі системи є цілком автоматичними, навпаки, у таких системах широко використовується людський досвід, знання експертів. Функціональні можливості таких систем мають виконувати діагностику, прогнозування розвитку ситуацій. Поряд з цим, нині очевидно, що реальний прорив у сфері і інформаційно-аналітичної роботи можливий лише в результаті агрегування усіх наведених напрямків.

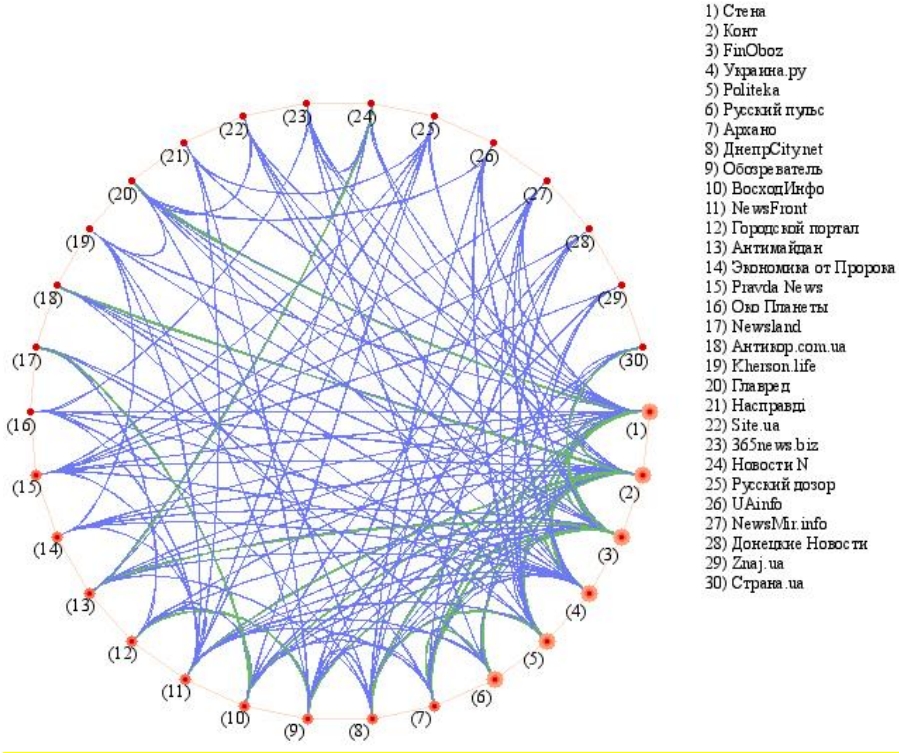

Рисунок 1 – Мережа джерел інформації за тематикою «Формула Штанмайера»

Література

1. Information Operations Recognition. From Nonlinear Analysis to Decision-Making / A. Dodonov, D. Lande, V. Tsyganok, O. Andriichuk, S. Kadenko, A. Graivoronskaya – LAP Lambert Academic Publishing, 2019. - 292 p.
2. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system // Theoretical and Applied Cybersecurity, 2019. - N. 1. - pp. 103-108.
3. Ландэ Д.В., Снарский А.А. Применение графов горизонтальной видимости в информационной аналитике // CEUR Workshop Proceedings. Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017) . – С. 86-91.

ПОКАЗНИК РЕЛАКСАЦІЇ В СКЛАДНИХ МЕРЕЖАХ

А.О. Снарський[1,2][0000-0002-4468-4542], Д.В. Ланде[1,2][0000-0003-3945-1178], О.О. Дмитренко [1][0000-0001-8501-5313]

[1]Інститут проблем реєстрації інформації НАН України, Київ, Україна
[2] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
dwlande@gmail.com asnarskii@gmail.com dmytrenko.o@gmail.com

Анотація. В роботі досліджуються нові характеристики вузлів мережевих структур – показник релаксації мережі та індивідуальний показник релаксації вузла. Для отримання показника релаксації застосовуються так звані уповільнені ітераційні алгоритми для HITS та PageRank. Встановлено, що на відновлення традиційних показників мережі, після збурення окремих вузлів, впливає її топологія. Як приклад, показник релаксації мережі та індивідуальний показник релаксації вузла були використані для дослідження структури мережі термінів, побудованої для предметної області “Кібербезпека”. Завдяки застосуванню показників релаксації вдалося визначити найбільш важливі змістовні компоненти мережі та ранжувати їх за введеними показниками. Отримане ранжування у порівнянні з ранжуванням за показникамиHITSта PageRank показує унікальністьзапропонованих показника релаксації мережі та індивідуального показника релаксації вузла.

Ключові слова:складна мережа, показник релаксації,індивідуальний показник релаксації,HITS, PageRank, предметна область, мережа термінів.

Вступ

Складні мережі широко поширені у природі. Більшість об'єктів у природі і суспільстві мають бінарні зв'язки, які можна представити у вигляді мережі. Топологічні властивості мереж, що розглядаються абстрактно від їх фізичної природи, але істотно визначають функціонування мереж, становлять предмет дослідження комплексних мереж. У багатьох прикладних галузях та сферах науки і техніки задачі аналізу топології мережі та дослідження особливостей її вузлівмають досить важливе значення.

Вивченням характеристик складних мереж займається область дискретної математики, що має назву теорія складних мереж (від англ. – ComplexNetworks) [1, 2], потужний математичний апарат якої дозволяє досліджувати, зокрема, поведінку окремих об’єктів такихмереж.

Наукові роботи вітчизняних та зарубіжних вчених В. М. Глушкова, В. М. Томашевського, П. Ердоша, А. Рені, М. Е. Дж. Ньюмана, Р. Альберт, А.-Л. Барабаші, Д. Дж. Ваттса, С. Г. Строґаца та інших дослідників внесли суттєвий вклад у розвиток теоретичних основ і практичних рішень для створення методів і засобів дослідження та проектування складних мереж. Пропонуються також нові методи до вирішення обчислювально складних задач, характерних для сучасних мережевих структур [1-3]. Незважаючи на наявність уже існуючих традиційних підходів, дослідження статистичних властивостей, які характеризують поведінку мереж; створення моделі мереж; прогнозування поведінки мереж при зміні структурних властивостей абопід час різних зовнішніх впливах – актуальні завдання теорії складних мереж.

У прикладних дослідженнях зазвичай застосовують типові для мережевого аналізу характеристики вузлів мережі, які описують її певну визначену властивість, найважливішими серед яких на цей час вважають степінь вузла та показники, що відповідають алгоритмам HITS та PageRank. Поруч із вже традиційними показниками мережі таких як HITS та PageRank в даній роботі були запропоновані та досліджені такі нові характеристики як: показник релаксації мережі та індивідуальний показник релаксації вузла.

СОДЕРЖАНИЕ