Якщо розглядати окремо інформаційну, психологічну та кібернетичну операції, то, використовуючи модель інформаційного простору (інформаційного середовища), можна зробити висновок, що за своєю сутністю кібернетичні операції спрямовані на фізичну та логічну складові інформаційного простору, психологічні – на соціальну складову, а інформаційна операція інтегрує в собі всі їх заходи.

Отже, у сучасних гібридних війнах інформаційні операції є складовою стратегічних комунікацій держави, поєднують у собі заходи і відповідні ефекти психологічних і кібернетичних операцій, спрямовані на нейтральні цільові аудиторії та цільові аудиторії противника, в умовах сучасного світу можуть самостійно досягати необхідних результатів. Необхідними умовами для їх успішного ведення є розуміння їх ролі, місця і можливих результатів воєнно-політичним керівництвом та наявність необхідних сил і засобів для їх ведення.

Шнурко-Табакова Е. В.
Громадська організація «Рада інформбезепеки та кіберзахисту»
Ланде Д. В., д-р техн. наук, проф.
Інститут проблем реєстрації інформації Національної академії наук України

МЕТОДИ І ЗАСОБИ АНАЛІТИЧНОЇ ПІДТРИМКИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ ДЕРЖАВИ

У наш час в Україні до протидії гібридним загрозам державі залучаються всі шари держави і суспільства, зокрема, силові структури, міністерства та відомства, недержавні організації, бізнес, громадські об’єднання. З огляду на те, що ворог поряд із економічними, енергетичними, гуманітарними та іншими важелями широко застосовує інформаційну зброю, проводить 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 атак і операцій, зокрема виявлення мереж ворожих інформаційних ботів, прогнозування розвитку подій, явищ, процесів тощо.

На нашу думку, потребує інформаційно-аналітичної підтримки протидія інформаційним операціям у мережі Інтернет, які умовно поділяються на пропагандистські (інформаційні впливи мають переважно пропагандистський характер), дезінформаційні (основною метою є дезінформація шляхом поширення «фейків»), маніпулятивні (маніпулювання, модифікація настанов), оборонні (контроперації – нейтралізація інформаційного впливу противника).

Для виконання 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 повідомлень щодо події в одиницю часу;

визначати критичні, порогові точки, які відповідають кількісній динаміці явища;

визначати прояви подій, процесів, об’єктів у критичних точках, наприклад, виявляти основні сюжети повідомлень щодо обраного процесу або явища;

ранжувати ці прояви і досліджувати динаміку їх розвитку до та після певних критичних точок;

здійснювати статистичний, кореляційний і фрактальний аналіз загальної динаміки і динаміки окремих проявів, на основі яких прогнозувати розвиток події, процесу й окремих їх проявів.

Для дослідження взаємозв'язку реальних подій і публікацій про них у мережі Інтернет авторами використовується інформаційна OSINT-система InfoStream, що забезпечує інтеграцію та моніторинг мережевих інформаційних ресурсів, а також аналітична система AttackIndex.com, яка 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 й 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 і реагуванням.

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 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 різноманітних технологічних рішень. Тому вже є широкий вибір засобів автоматизації інформаційно-аналітичної діяльності, причому рівні функціональності таких систем можуть бути дуже різноманітними: 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.

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 них широко використовується людський досвід, знання експертів. Функціональні можливості таких систем мають виконувати діагностику, прогнозування розвитку ситуацій. Очевидно, що реальний прорив у сфері інформаційно-аналітичної роботи можливий лише в результаті агрегування усіх наведених напрямків.