5. Корупція в Україні: причини поширення та механізми протидії. Зелена книга державної політики. Монографія. Автори: С. В. Дрьомов, Ю. Г. Кальниш (керівник авторського проекту), Д. Б. Клименко, Г. О. Усатий, Л. М. Усаченко; за ред. Ю. Г. Кальниша. - К.: ДП. «НВЦ «Пріоритети»». - 2010. - 88 с.

6. Іщенко М. П. Зростання ролі державних і громадських інституцій у протидії корупції // Наукове видання «Політико - правові і соціально - моральні фактори розвитку державної служби та запобігання корупції в Україні. Збірник матеріалів науково - практичного семінару 25 березня 2010 року; за ред. професора М. П. Іщенка. – С. 21 - 25.

Використання osint-розвідки для побудови моделі цільової аудиторії

Савчук В.С.
ад'юнкт науково-організаційного відділення.
Житомирський військовий інститут імені С.П. Корольова
Грищук Р.В.
доктор технічних наук , с.н.с.
начальник науково-дослідного відділу інформаційної
та кібернетичної безпеки наукового центру.
Житомирський військовий інститут
імені С. П. Корольова

Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції [1, с. 1]. В той же швидкий розвиток технологій та збільшення об'ємів інформації, що циркулюють у віртуальному середовищі призводить до зростання ролі й місця кібернетичної розвідки.

На даний час OSINT-розвідці відводиться ключова роль, адже 50-70% розвідувальної інформації добувається з відкритих джерел [2, с.216-224]. Зі збільшенням значення соціальних інтернет мереж значного розвитку набула OSINT-розвідка. Окрім цього, OSINT-розвідка є важливою складовою психологічних операцій. Так, при виготовленні продукції психологічного впливу важливим етапом є оцінка цільової аудиторії, що в свою чергу проводиться з використанням соціальних інтернет сервісів як джерела інформації [3, с.114-117].

Пропонується побудувати модель цільової аудиторії (ЦА) на основі даних отриманих шляхом OSINT-розвідки соціальних мереж. В загальному вигляді моделювання ЦА грунтується на теорії графів. Мережеві графи відображають як деяку сукупність вузлів, що мають зв'язок. На сьогодні розвитку набуває область соціальних наук, яка спрямована на розуміння поведінки соціальних груп, формування зв'язків між ними, вивчення характеристик лідерів думки, тому з метою побудови математичної моделі цільової аудиторії, на яку буде поширюватись психологічний вплив використано метод аналізу соціальних мереж [4, с. 67-70].

Першим кроком для побудови моделі є побудова контекстуального фону. Для цієї мети доречно застосувати OSINT-розвідку у соціальних мережах, зважаючи на її переваги, як оперативність та об'єм .

Eman 1. Виділення акторів із соціальної мережі, що за певною ознакою належать до ЦА $C^A = \left\{ c_i^A \in C \mid P\left(c_i^A\right) \right\} = \left\{ c_i^A \mid P\left(c_i^A\right) \right\}$, де C^A-множина акторів цільової аудиторії, С-множина акторів сІС та $P(c_i^A)$- ознака, за якою обираємо акторів до ЦА.

Eman 2. Побудова бази реляційних даних акторів ЦА, до якої мають війти друзі, інтереси, місце роботи чи навчання, родичі.

Eman 3. Обчислення нових характеристик для цільової аудиторії, такі як лідери думки, канали поширення інформації, спираючись на реляційні дані та метод аналізу соціальних мереж.

Модель, що містить таку інформацію дає можливість дослідити структуру ЦА та визначити акторів ЦА, яким властива найбільша кількість зв'язків та високий вплив на інших. Поширення будь-якої інформації в мережі найбільш ефективно, з точки зору оптимізації витрат, проводити з їх допомогою. Блокування такого члена мережі сповільнить і значно послабить поширення думок та соціальних настроїв серед загалу ЦА.

Таким чином OSINT-розвідка в соціальних мережах, що спрямована на пошук і добування інформації з доступних через мережу інтернет відкритих джерел дає можливість автоматизувати оцінку ЦА для виготовлення матеріалів психологічного впливу та планування психологічних операцій.

Література:

1. Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016.
2. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук / за заг. ред. Ю. Г. Даника – Житомир : ЖНАЕУ, 2016. – С. 216-224
3. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.
4. Мелешко Є.В Дослідження методів визначення центральності акторів у соціальних мережах для задач інформаційної безпеки/ Є.В. Мелешко, В.С. Гермак, С.М. Охотний // Системи управління, навігації та зв'язку Кіровоград: Кіровоградський національний технічний університет , 2016 № 4(40) с.67-70 ISSN 2073-7394

Перспективи використання інноваційних інформаційних технологій штучного інтелекту у складі технічних засобів моніторингу як складової системи охорони (оборони) берегових і прибережних споруд державного значення

Симоненков В.М.
старший науковий співробітник;
Науково-дослідний центр ЗС України «Державний океанаріум»
Литвин М.А.
студентка Національного авіаційного університету
Коновець В.І.
кандидат технічних наук, с.н.с.
провідний науковий співробітник;
Науково-дослідний центр ЗС України «Державний океанаріум»

Аналізуючи проблеми безпеки прибережної держави, корисно поглянути на морську сферу через призму просторового ландшафту її розміщення:

95% телекомунікацій світу проходять по підводних кабелях;

90% світової торгівлі переміщується морем;

50% нафти транспортують морським шляхом;

понад 40% населення світу мешкає в межах 100-150 км від узбережжя.

За останні десять-п’ятнадцять років у провідних країнах світу в галузі робототехніки відбулися кардинальні зміни, які пов’язані з масовим виробництвом і випробуваннями у реальних умовах бойових робототехнічних комплексів, у тому числі безпілотних літальних апаратів, наземних мобільних роботів та безекіпажних напівзанурених або підводних апаратів.

Ще вчора завдання створення робототехнічних комплексів, здатних нести бойовий заряд, була прерогативою держав з потужною технологічною базою, але зараз доступність технологій і можливість анонімного замовлення складних компонентів на глобальному комерційному ринку дозволяють виготовляти зразки такої техніки навіть інженерам середнього рівня. Фінансово така робота цілком під силу навіть невеликій групі кіберзлочинців у морський сфері.

Враховуючи те, що такі загрози носять складний та комплексний характер, питання побудови ефективної системи охорони (оборони) об’єктів необхідно вирішувати із застосуванням більш досконалих сучасних та перспективних технічних засобів моніторингу, в першу чергу, у складі відповідних стаціонарних та мобільних робототехнічних комплексів різного призначення.

На думку провідних фахівців світу, перспективні дослідження в області військової робототехніки спрямовані на поетапне нарощування можливостей дистанційно-керованих машин з поступовим виключенням функцій управління і контролю з боку людини-оператора.

З інформаційної точки зору, систему моніторингу обстановки із застосуванням перспективних роботизованих засобів можливо розглядати у вигляді програмно-апаратного комплексу, який призначений для виявлення вторгнень на об’єкти охорони (оборони) або спроб неправомірного доступу.