НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
імені І.Черняховського

КАФЕДРА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

МАТЕРІАЛИ
І МІЖВІДОМЧОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“Забезпечення інформаційної безпеки держави у воєнній сфері: проблеми та шляхи їх вирішення”

Видання університету
2021

Рекомендовано до друку рішенням кафедри застосування інформаційних технологій та інформаційної безпеки (затверджено протоколом від 26.11.2021 р. № 8)

“Забезпечення інформаційної безпеки держави у воєнній сфері: проблеми та шляхи їх вирішення” МАТЕРІАЛИ І МІЖВІДОМЧОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ 26 листопада 2021 року. – Київ: НУОУ, 2021. – 180 с.

Матеріали містять тези доповідей пленарного засідання та виступів доповідачів по секціях І міжвідомчої науково-практичної конференції за теоретичними та практичними результатами наукових досліджень і розробок, виконаних слухачами, науковими, науково-педагогічними працівниками, аспірантами та ад’юнктами, докторантами науково-дослідних установ та закладів освіти, представниками органів військового управління, військових частин Збройних Сил України та інших відомств, громадських організацій, Директорату політики цифрової трансформації та інформаційної безпеки у сфері оборони Міністерства оборони України; Управління стратегічних комунікацій Апарату Головнокомандувача Збройних Сил України; Служби безпеки України.

Національний університет оборони України імені Івана Черняховського, 2021

протидію інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти Збройних Сил України та інших військових формувань;

донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань.

Такий підхід забезпечує наявність належної урегулювання діяльності державних органів, складових сектору безпеки і оборони держави щодо виконання завдань забезпечення інформаційної безпеки держави у воєнній сфері.

ЛІТЕРАТУРА:

1. Стратегія кібербезпеки України “Безпечний кіберпростір – запорука успішного розвитку країни”, затверджена Указом Президента України від 26.08.2021 № 447/2021.

2. Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 17 вересня 2021 року №473/2021

Ланде Д.В. д.т.н., професор
ІПРІ НАН України
Шнурко-Табакова Е.В.
ГО Рада інформбезпеки та кіберзахисту

ПОДОЛАННЯ БАР‘ЄРІВ МЕРЕЖІ ІНТЕРНЕТ ДЛЯ ВИРІШЕННЯ ЗАДАЧ OSINT

Розглянуто наявні проблеми здійснення розвідки за відкритими джерелами OSINT і шляхи їх подолання.

На цей час існують суттєві технічні проблеми, які заважають здійсненню розвідки за відкритими джерелами в різних національних сегментах мережі Інтернет без застосування спеціальних інтегрованих систем контент-моніторингу, які містять у свому складі інтелектуальні пошукові засоби, мережі інформаційних проксі-серверів, засоби взаємодії і зовнішніми агрегаторами мережевих інформаційних ресурсів, інфраструктуру маскування і анонімізації.

Звичайно, на первинному рівні можливо використовувати дані, які доступні через традиційні мережеві пошукові системи,

розміщуються на відомих інтеграторах новин. У цьому випадку виникає ряд проблем, що заважають серйозному застосуванню мережевих ресурсів для задач аналітичної роботи:

В національному сегменті доступні далеко не всі ресурси, зокрема, не має доступу до деяких закордонних веб-сайтів і соціальних мереж.

Традиційні пошукові системи не завжди індексують новини, що розміщуються на глибинних рівнях веб-сайтів, не завжди новини індексуються ними своєчасно, погано охоплюються соціальні мережі, спеціальні бази даних, розміщені в Інтернеті.

У деяких випадках при неанонімізованому доступі веб-сайти або соціальні мережі, що приймають участь в інформаційних війнах, можуть видавати первинним користувачам спотворену інформацію, фейки. У деяких випадках доступ до інформації може бути заборонений, хоча ця інформація має статус відкритої для всіх.

Запити, що відповідають інформаційним потребам аналітиків, що передаються у незахищеному вигляді, можуть розкрити ці потреби для зацікавленої сторони - інформаційного противника.

Відсутність розвинених аналітичних засобів.

Для вирішення цих проблем, що стосуються OSINT (open source intelligence - розвідки за відкритими джерелами), мають застосовуватися сучасні інтегровані системи, яким притаманні такі властивості:

Розподілений збір інформації з веб-сайтів і соціальних мереж за допомогою ансамблів інтелектуальних агентів збору, розподілених у хмарному середовищі, що територіально охоплює різні країни. Ці агенти мають взаємодіяти між собою, обмінюватись інформацією, передавати цю інформацію в аналітичну частину системи OSINT.

Агенти добування інформації мають реалізовувати запрограмовані і налаштовані сценарії збору інформації, взаємодіяти із веб-сайтами, соціальними мережами, базами даних глибинного вебу, агрегаторами новин переважно (за можливістю) у анонімному режимі.

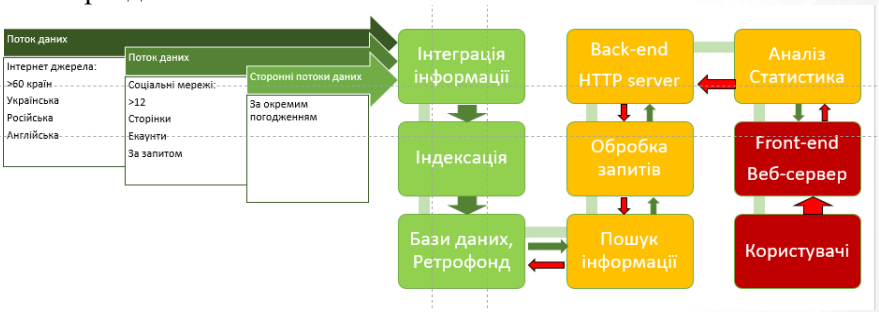
Застосування агентів добування інформації як основи системи інформаційних проксі серверів має забезпечувати повноту інформації у випадку блокування окремих агентів, запобігати спотворенню і дублюванню інформації, що передається до баз даних

системи OSINT.

Мають застосовуватися засоби анонімізації, маскування, VPN, тощо для недопущення витоку інформаційних потреб аналітиків OSINT при добуванні і обробці даних.

Аналітичні засоби мають обробляти інформаційні потоки у режимі онлайн, реалізовувати процедури інформаційного пошуку, виявлення інформаційних атак, операцій, ранжування факторів впливів, формування і аналізу моделей предметних галузей (онтологій) тощо.

Приклад реалізації автономної програмно – технічної системи з анонімізацією моніторингу інформації та її аналітичною обробкою представлено на мал. 1. OSINT має базуватися на науково – методичному підґрунті, оновлюватися у відповідності до нових викликів та розробок, надавати можливість об’єктивізації висновків за рахунок якості даних, незалежність результатів сервісу AttackIndex.com від суб'єктивних факторів (думок окремих експертів чи інженерів розробників, їх упереджень, термінологічний популізм), також забезпечує отримання об'єктивних даних, об'єктивну аналітику великих даних, репрезентативність зібраних даних та результатів аналітичної обробки, своєчасне виявлення нових трендів.



Мал.1. БЛОК СХЕМА ATTACK INDEX SERVER

Висновки. В доповіді представлені основні проблеми і вимоги, що ставляться перед системами OSINT для подолання бар´єрів, притаманних мережевому інформаційному середовищу. На прикладі системи Attack Index показано, що на цей час можливо побудувати систему державного рівня в галузі безпеки і оборони, яка буде реалізовувати завдання OSINT на базі сучасних інтелектуальних технологій.

ЛІТЕРАТУРА:

1. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system // Theoretical and Applied Cybersecurity, 2019. - N. 1. - pp. 103-108.

2. “Army techniques publication no. 2-22.9.” Headquarters Department of the Army Washington, DC, 7 2012. (FMI 2-22.9).

3. 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.

4. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Компьютерная конкурентная разведка - К.: ТОВ "Інжиніринг", 2021. - 354 с.

5. Lande D.; Subach I.; Puchkov O.; Soboliev A. A Clustering Method for Information Summarization and Modelling a Subject Domain Information & Security: An International Journal 50, no. 1 (2021): 79-86. DOI: doi.org/10.11610/isij.5013

6. Ланде Д.В., Ліненко Ю.О. Мережева модель правових обмежень доступу до Інтернету у світі // Інформація і право, 2019. - N 2 (28). - С. 26-31.

Войтко О.В., к.військ.н.
НУОУ

РЕАЛІЗАЦІЯ СТРАТЕГІЧНОГО НАРАТИВУ ДЕРЖАВИ НА ОСНОВІ МОДЕЛІ РОЗПОВСЮДЖЕННЯ ІНФОРИАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ.

Вивчення та проведення досліджень щодо процесів розповсюдження та отримання інформації з засобів масової інформації та інформації, що циркулює в соціальних мережах залишається перспективним науковим напрямком, як для аналітиків, маркетологів так і для проведення спеціальних інформаційних та психологічних дій в інтересах застосування військ (сил).

Аналіз соціальної мережі або декількох мереж дозволяє скласти соціальний зв'язок між користувачами і контентом соціальної мережі та визначити перспективні напрямки задоволення їхніх інтересів(потреб) до інформації, що безпосередньо буде

ЗМІСТ