

ВІЙСЬКОВИЙ ІНСТИТУТ  
ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ  
ІМЕНІ ГЕРОЇВ КРУТ

МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ  
ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ



СИСТЕМИ І ТЕХНОЛОГІЇ ЗВ'ЯЗКУ,  
ІНФОРМАТИЗАЦІЇ ТА КІБЕРБЕЗПЕКИ:  
АКТУАЛЬНІ ПИТАННЯ І ТЕНДЕНЦІЇ РОЗВИТКУ

КИЇВ - 2021

**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

**ВІЙСЬКОВИЙ ІНСТИТУТ  
ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ  
ІМЕНІ ГЕРОЇВ КРУТ**



**I МІЖНАРОДНА  
НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ**

**“Системи і технології зв’язку, інформатизації та  
кібербезпеки: актуальні питання і тенденції розвитку”**

**25 – 26 листопада 2021 року**

**(Доповіді та тези доповідей)**

**Київ – 2021**

**ББК**  
Ц4 (4Укр)39  
П-768

У збірнику матеріалів першої міжнародної науково-технічної конференції опубліковано доповіді та тези доповідей вчених, науково-педагогічних та наукових працівників, докторантів, ад'юнктів, здобувачів, курсантів Військового інституту телекомунікацій та інформатизації імені Герої Крут та інших вищих навчальних закладів, представників промисловості в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення, застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил. Метою конференції є аналіз стану та обмін досвідом з питань систем і технологій зв'язку, інформатизації та кібербезпеки з урахуванням досвіду застосування у Збройних Силах України.

76.	<b>Ланде Д.В., Шнурко-Табаква Е.В.</b> Автономні інтелектуальні системи OSINT	180
77.	<b>Лебідь Є.В., Скринніков І.І., Дрозд А.В., Антонюк Д.І.</b> Застосування систем позиціонування в робототехнічних комплексах військового призначення	182
78.	<b>Левченко В.В., Артюх С.Г.</b> Аналіз використання платформ віртуалізації в захищених мережах	183
79.	<b>Легкобит В.С., Гавриленко Р.В.</b> Метод аналізу ієрархій при вирішенні задач пов'язаних з розрахунком показників пріоритетності логістичного забезпечення підрозділів ЗСУ	184
80.	<b>Легкобит В.С., Мірошниченко А.О.</b> Консолідація даних в системах OLAP на основі APACHE DRUID	186
81.	<b>Легкобит В.С., Дацков Д.О.</b> Технічні аспекти реалізації процесів ETL в контексті мінімізації необхідних ресурсів шляхом застосування системи CHANGE DATA CAPTURE (cdc)	187
82.	<b>Легкобит В.С., Коваленко А.С.</b> Аналіз ефективності експлуатації веб-додатків на основі технології progressive Web Apps	188
83.	<b>Легкобит В.С., Фисун А.С.</b> Аналіз підходів до динамічної візуалізації вмісту .DOCX файлів за допомогою бібліотек JAVASCRIPT	189
84.	<b>Лисенко О.І., Явіся В.С., Новіков В.І., Сушин І.О.</b> Застосування бездротових сенсорних мереж на базі безпілотних літальних апаратів у військових цілях	190
85.	<b>Лисенко О.І., Явіся В.С., Сушин І.О.</b> Підхід до побудови системи стабілізації мультикоптерних дронів	192
86.	<b>Лисенко О.І., Явіся В.С., Сушин І.О.</b> Спосіб забезпечення стійкого управління дронами	193
87.	<b>Ліщинська Х.І., Сеник А.П., Хобор О.Р., Севериненко Д.Ю.</b> Прогнозування метеорологічних ризиків зміни самопочуття військовослужбовців з використанням інформаційних технологій	195
88.	<b>Любарський С.В., Михайлов В.Р.</b> Математична модель забезпечення інформаційної безпеки при розробці інформаційних систем на платформах Mern, Django-Flask стеків	196
89.	<b>Любарський С.В., Михайлов М.Р.</b> Підвищення швидкості взаємодії з оглядачами мобільних платформ сайту Збройних Сил України	197
90.	<b>Любарський С.В., Уставицький Р.А.</b> Реалізація модулю пошуку контентно-залежної інформації в web-орієнтованому порталі Moodle	198
91.	<b>Ляшенко В.Р., Османов Р.Н.</b> Аналіз методів забезпечення завадозахищеності радіорелейних інтервалів у тактичній ланці управління	199
92.	<b>Ляшенко Г.Т., Черниш Ю.О., Шемендюк О.В.</b> Розробка математичної моделі захисту інформаційних систем спеціального призначення	200
93.	<b>Макаренко О.О., Петрова Д.В.</b> Перспективи використання технології "блокчейн" у сфері оборони	202
94.	<b>Макарчук О. М.</b> Комбінований метод пошуку екстремуму мультимодальних функцій	204
95.	<b>Мартиненко А.Г., Лукашенко Є.О.</b> Аналіз застосування геоінформаційних систем в інформаційних системах Збройних Сил України	205
96.	<b>Мартинюк В.В., Мальцева І.Р., Бондаренко Т.В.</b> Аналіз використання засобів радіоелектронної боротьби у сучасних операціях	206
97.	<b>Масесов М.О., Новицький Д.В., Шугалій О.О., Пономаренко З.М.</b> Перспективи розвитку тропосферного зв'язку у Збройних Силах України	208
98.	<b>Михайлюк С.С.</b> Резервування об'єктів телекомунікаційних систем і мереж загального та спеціального призначення з комплексним використанням надлишковості	209
99.	<b>Міночкін А.І., Зінченко М.О., Живило Є.О., Плугова О.Б.</b> Розробка підходів до визначення складових кібероборони, як системи організації та ведення кібердій	210
100.	<b>Міхєєв Ю. І., Носова Г. Д., Павленко М. М.</b> Автоматизація процесу відслідковування динаміки поширення деструктивного інформаційно-психологічного впливу в мережі інтернет	212
101.	<b>Могилевич Д.І., Сінько В.В.</b> Моделі надійності об'єктів телекомунікаційного обладнання мережі військового зв'язку	213
102.	<b>Насібов Яшар</b> Єдна інфраструктура даних: побудова smart розумних міст в країнах, що розвиваються	214
103.	<b>Нерознак Є.І., Меркотан Д.Ю., Сова О.Я.</b> Методи та алгоритми балансування навантаження в кластерних системах на основі елементів штучного інтелекту	215
104.	<b>Нестеренко М.М., Кулікова О.С.</b> Програмний модуль побудови рейтингу курсантів факультету ВВНЗ на основі платформи NODE.JS	218
105.	<b>Нестеренко М.М., Сорока Д.В.</b> Підсистема розрахунку навантаження науково-педагогічних працівників ВВНЗ на основі стеку технологій MERN	219
106.	<b>Нестеренко М.М., Степаненко С.Ю., Ковальчук Д.О.</b> Програмно-апаратний модуль підсистеми виявлення аварійних ситуацій на об'єктах військового призначення на основі технології WEB OF THINGS	220
107.	<b>Олексіюк В.В., Балик І.В., Касалапов А.Д.,</b> Завдання розвідки робототехнічних комплексів	221

## АВТОНОМНІ ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ OSINT

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 своєму складі інтелектуальні пошукові засоби, мережі інформаційних проксі-серверів, засоби взаємодії і зовнішніми агрегаторами мережевих інформаційних ресурсів, інфраструктуру маскуванню 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, маскуванню, 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.

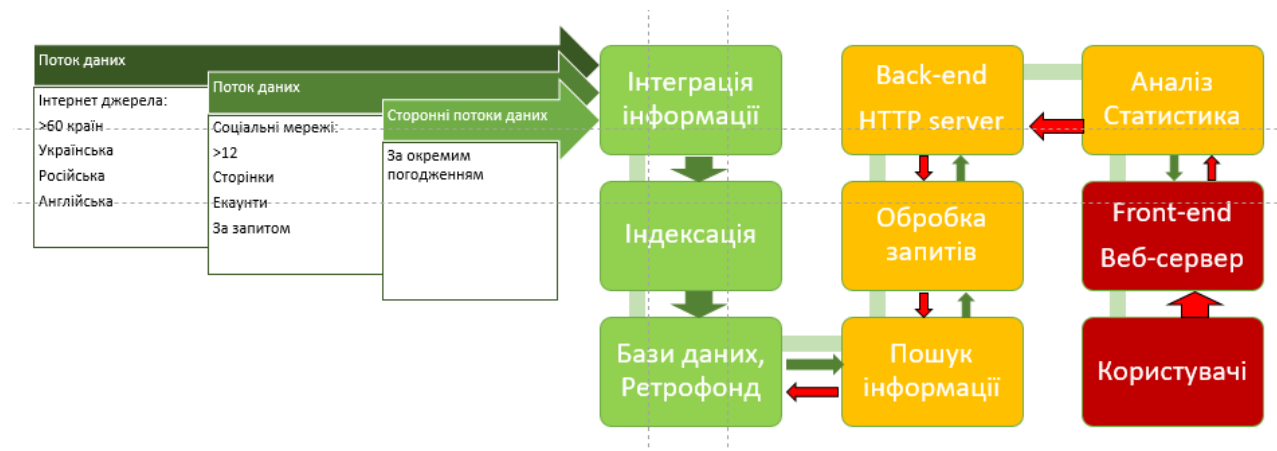


Рис.1 Блок схема ATTACK INDEX SERVER

### 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.