INFORMATION WARFARE

DOI 10.20535/2411-1031.2019.7.2.190561
УДК 004.056.53

ЮРІЙ ДАНИК,
КОСТЯНТИН СОКОЛОВ,
ОЛЕГ ГУДИМА

ПІДХІД ДО АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ДЕСТРУКТИВНИХ КІБЕРВПЛИВІВ

Розглянуто питання аналізу інформації та виявлення деструктивних впливів у кіберпросторі та через кіберпростір. В 2019 році підтверджено світову тенденцію щодо зростання кількості користувачів сервісів соціальних інформаційних мереж. Тому на теперішній час зростає важливість забезпечення виконання завдань інформаційної та кібернетичної безпеки в електронних засобах масової інформації та аналізування кіберпростору. Враховуючи світові тенденції стосовно виявлення деструктивних кібервпливів та для виконання завдань визначених керівними документами держави необхідно здійснювати моніторинг кіберпростору та виявлення деструктивних кібервпливів (на етапах планування, підготовки та безпосередньо проведення інформаційних дій). Для реалізації вище зазначеного необхідне опрацювання питання розробки відповідних моделей і методів автоматичного виявлення деструктивних кібервпливів. З метою створення підґрунтя для проведення наукових досліджень здійснено вивчення: методів аналізу інформації, що є у кіберпросторі для виявлення деструктивних кібервпливів; переваг та недоліків відомих методів виявлення деструктивних кібервпливів; відомих систем моніторингу кіберпростору. Основними особливостями (функціями) відомих систем моніторингу кіберпростору є: пошук даних за ключовими словами та фіксація доступної інформації про розповсюджувачів інформації (їх загальна кількість, активність за певний період, аккаунти акторів, стать, вік, географічна локація, охоплення аудиторії). Таким чином, виникає потреба в визначенні підходів при розробці методів і моделей підтримки прийняття рішень, що стосується виявлення деструктивних кібервпливів у кіберпросторі. При розробленні підходу щодо виявлення деструктивного кібервпливу на першому етапі застосовується метод онтології для структуризації інформації (рубрикації текстового контенту). Перевагами використання онтологічних схем у процесі виявлення інформаційного впливу є: наочність предметної галузі (проблеми) у табличному вигляді або у вигляді графів, виявлення прихованих зв’язків, накопичення та аналіз інформації в оперативному режимі, перевірка узгодженості фактів. На другому етапі застосовується фільтр-матриця, яка відображає процеси (планування, підготовки та безпосередньо проведення інформаційних дій) класичної інформаційної операції збройних сил країн НАТО. У перспективах подальших досліджень стоїть завдання щодо розробки методу автоматизованого виявлення деструктивних кібервпливів у кіберпросторі.

Ключові слова: кіберпростір, безпека, деструктивний, кібервплив, виявлення, моніторинг, метод.

Постановка проблеми. У світі [1] - [3] спостерігається тенденція щодо зростання кількості користувачів сервісів соціальних інформаційних мереж. Крім того, протягом останніх десяти років користувачів соціальних мереж у два рази більше стали витрачати на соціальні мережі. Тому на теперішній час особливої ваги набуває завдання інформаційної та кібернетичної безпеки в електронних засобах масової інформації та здійснення аналізу кіберпростору з метою виявлення деструктивних кібервпливів.

Питанням інформаційної та кібернетичної безпеки в електронних засобах масової інформації в країнах світу приділяється суттєва увага. На саміті НАТО в Варшаві [4] - [6] на Кібер-конференції з інформаційного забезпечення НАТО [7] та на засіданні Північноатлантичної ради [8] було зосереджено увагу на важливості запобігання, виявлення та ліквідації деструктивного впливу (інформаційних загроз) у кіберпросторі.

Відповідно до меморандуму 2017 р. у Гельсінкі (Фінляндія) за участю США, Франції, Німеччини, Швеції, Польщі, Фінляндії, Латвії, Литви створено Європейський центр з протидії гібридним загрозам. Який є міждержавним, європейським Центром боротьби з гібридними загрозами – кібератаками, пропагандою та дезінформацією. Передбачається, що Центр формуватиме мережу експертів для країн-учасниць та буде тісно співпрацювати з Євросоюзом і НАТО.

Війська (сили) кібероборони формуються практично у всіх державах – членах НАТО. Так, наприклад, у 2016 році було створено Командування кібер-інформаційного простору ФРН з статусом окремого виду збройних сил. Велика Британія з метою протистояння російській загрозі в 2019-2020 роках має намір створити кібервійська. Кібервійська нараховуватимуть 2 тисячі осіб, а фінансування, на початковому етапі становитиме понад 250 мільйонів фунтів стерлінгів.

В Україні основні завданні щодо захисту кіберпростору визначені в [9] - [11].

Враховуючи світові тенденції та на виконання завдань визначених керівними документами держави набувають актуальності питання моніторингу кіберпростору та виявлення деструктивних кібервпливів (на етапах планування, підготовки та безпосередньо проведення інформаційних дій). Для реалізації вище зазначеного необхідна розробка відповідних моделей і методів.

При розробці методів (моделей) моніторингу соціальних мереж можуть використовуватися нейронні мережі, які застосовуються до різних типів даних, але мають недоліків, а саме: складність змістовної інтерпретації нейронних мереж та недетермінованість. Моделі на базі нейронних мереж не дозволяють однозначно та прозоро визначити внесок кожного показника у кінцевий результат.

Для фільтрації контенту одним з сучасних рішень, щодо забезпечення ефективного моніторингу за різними станами інформаційних процесів, та їх впливу на суб'єктну діяльність, є онтологічне моделювання. Теорія графів дозволяє в свою чергу провести аналіз джерел інформації.

Аналіз останніх досліджень і публікацій. Теоретичну основу розробки методів і моделей контент-моніторингу кіберпростору становлять [12] - [14], [17] - [19].

Основні теоретичні засади формальних математичних моделей онтологій розроблено у роботі [20] та інших в яких запропоновано онтологію розглядати як тривимірний кортеж; використання онтологій під час функціонування прикладних інформаційних систем описано в роботі [31] та інших; проблему побудови інтелектуальних систем на основі онтологій розглянуто у роботах [15], [28], [21]-[27], [32]-[35], [29]; проблему опрацювання текстів для автоматизованої побудови онтології досліджено у роботі [30] та інших. Аналізуючи роботи загалом, можна зробити висновок, що наукові дослідження в галузі розроблення та використання онтологій активно розвиваються. Вище зазначене свідчать про актуальність проблематики побудови методів (моделей) автоматизованого виявлення деструктивного впливу у кіберпросторі з використанням онтологій.

Постановка завдання. Існуючі засоби моніторингу не в повній мірі відповідають визначеним завданням, так як об'єми інформації, яка підлягає моніторингу на предмет виявлення деструктивних кібердій постійно зростають. При цьому, оперативність моніторингу, яка забезпечується існуючими методами є недостатньою. Необхідним стає якісне вивчення смислів і контекстів, для виявлення ознак деструктивності кібервпливів та прогнозування їх наслідків. Актуальним є питання достовірності та оперативності виявлення деструктивних кібердій (на етапах їх планування, підготовки та безпосередньо проведення).

Метою статті є розгляд підходу до формування математичного апарату щодо виявлення деструктивних кібервпливів та кібердій (на етапах планування, підготовки та безпосередньо їх проведення) у кіберпросторі та через кіберпростір.

Виклад основного матеріалу дослідження. В умовах зародження в кіберпросторі нових і становлення вже існуючих соціальних Інтернет формацій, так званих віртуальних спільнот, що володіють принципово іншими (в порівнянні з традиційними формами впливу на соціальні структури в індустріальному суспільстві) можливостями з надання впливу на традиційні громадські та державні структури, поява яких пов'язана з програмами створення оперативного доступу по каналах відкритих телекомунікаційних мереж до розподілених інтелектуальних і матеріальних ресурсів в будь-якій точці земної кулі на якісно новий рівень виходить проблема інформаційної безпеки у кіберпросторі.

Прикладами актуальних загроз інформаційній безпеці, які реалізуються через кіберпростір, щодо Міністерства оборони України є: поширення у світовому інформаційному просторі (кіберпросторі) викривленої, недостовірної та упередженої інформації, що завдає шкоди Міністерству оборони України та Збройним Силам України; зовнішні негативні інформаційні впливи на свідомість особового складу Збройних Сил України через засоби масової інформації, а також мережу Інтернет.

Саме ці фактори і є визначальними щодо актуальності контент-моніторингу кіберпростору, з метою передбачення ситуацій переростання деструктивної інформації в деструктивний вплив і як наслідок реалізації загроз безпеці держави.

Під деструктивною інформацією будемо розуміти –контент що несе спотворену інформацію та віруси.

Головними функціями більшості систем, які використовуються для моніторингу кіберпростору є пошук даних по заданих ключових словах та фіксація доступної інформації про розповсюджувачів заданої інформації: їх загальна кількість, активність за певний період, аккаунти акторів, стать, вік, географічна локація, охоплення аудиторії.

Ці системи мають істотні недоліки. Головний з них неповнота збору інформації. Велика кількість необхідних повідомлень вони не фіксують, що пов'язане із системними обмеженнями у соціальних мережах на копіювання інформації (задана кількість запитів з одного аккаунту). Крім того, зберігається велика кількість інформації "сміття" (малозначних повідомлень) у базі даних, що ускладнює пошук і аналіз дійсно важливої інформації. Адаптація існуючих систем під специфічні завдання аналітичної роботи є досить тривалим і затратним заходом.

Встановлено, що широко поширені комерційні засоби контент-моніторингу інформації у соціальних мережах та засоби вільного доступу, у переважній більшості не є адаптованими під специфічний спектр воєнних завдань. Вони також характеризуються високою вартістю та мають закриті програмні коди із закладеними в них механізмами безпеки, що на практиці виключає їх модернізацію в інтересах вирішення цільових завдань.

Розроблене останнім часом в ЗС України програмне забезпечення має ряд недоліків, а саме: неповнота збору інформації; відсутня або ускладнена синхронізація бази даних окремих автоматизованих робочих місць; оновлення програмного забезпечення та виконання його налаштування необхідно проводити на кожному автоматизованому робочому місці.

Існуючі засоби моніторингу не в повній мірі відповідають визначеним в роботі завданням, так як оперативного моніторингу поточної ситуації в нашому випадку недостатньо, необхідним стає якісне вивчення смислів і контекстів, які дають підставу для прогнозування та оцінки достовірності інформації.

Базовими є такі методи:

- аналітичного читання – передбачає виокремлення ключових тем кожного абзацу; виділення ключової теми усього тексту; встановлення зв'язків між абзацами та співвідношення абзаців із усім текстом. Метод дає змогу виявити суперечності між деякими складовими тексту, визначити ставлення автора до тексту (факти викладаються однобічно чи висловлюються різні думки, чи висловлює автор гумор, чи намагається емоційно підкреслити власну думку);

- контент-аналіз – якісно-кількісний метод аналізу, який полягає у систематичній числовій обробці, оцінці й інтерпретації форми та змісту джерела інформації. Кількісна складова передбачає фіксацію частоти появи у тексті певних характеристик (одиниць) змісту. Якісна складова передбачає отримання висновків на основі певних характеристик змісту. Контент-аналіз матеріалів ЗМІ дає змогу співставляти усі три змістові складові масової комунікації: тенденції соціальної дійсності (суспільних явищ); соціальні характеристики джерела поширення інформації (його ідеологічну спрямованість, стратегії тощо); соціальні риси адресата.

Завдяки цьому розкривається прихована, неочевидна при звичайному читанні, інформація про стан і властивості соціальної дійсності; наміри автора цього тексту та потенційну реакцію адресата;

- побудова онтології – це спосіб подання знань у вигляді набору базових понять (об'єктів) деякої предметної галузі, описової інформації про них та зв'язків між об'єктами. Перевагами використання онтологічних схем у процесі виявлення інформаційного впливу є: наочність, візуалізація предметної галузі (проблеми) у табличному вигляді або у вигляді графів; виявлення прихованих зв'язків; накопичення та аналіз інформації в оперативному режимі; перевірка узгодженості фактів.

Онтологія [20] - [23] – це детальна формалізація деякої області знань за допомогою концептуальної схеми. Така схема, зазвичай, складається з ієрархічної структури даних, що містить всі релевантні класи об'єктів, їх зв'язків, теорем та обмежень, які прийняті у певній предметній області. У галузі штучного інтелекту відоме таке поняття: онтологія – це комплекс понять від найзагальніших до конкретних, які передбачають повний спектр об'єктів та відношень, подій та процесів, а також значень (атрибутів та відношень), які визначаються, якщо це потрібно, в часі та просторі. Ця система понять зв'язується як універсальними залежностями типу "загальне–частинне", "частина– ціле", "причина–наслідок" тощо, так і специфічними, залежно від моделі предметної області. Онтологія – це модель предметної області, яка використовує всі доступні.

Сьогодні проблема пошуку інформації у великих масивах є дуже актуальною. Ця проблема ускладнюється ще й тим, що сучасні пошукові механізми здійснюють пошук інформації без урахування семантики слів, що входять до запиту, а також контексту, в якому вони використовуються.

Завдяки використання онтології можна здійснювати семантичний пошук. У зазначеному напрямку мають значні напрацювання фахівці кафедри інформаційних систем та мереж Національного університету "Львівська політехніка" (В. В. Литвин, В. А. Висоцька, Д. Г. Досин, М. Г. Гірняк) [21] - [27].

Забезпечення можливості використання знань предметної області стало однією з рушійних сил недавнього сплеску у вивченні онтологій. Наприклад, для моделей багатьох різних предметних областей необхідно сформулювати поняття часу. Цей термін містить поняття тимчасових інтервалів, моментів часу тощо. Якщо одна група вчених детально розробить таку онтологію, то інші можуть просто повторно використовувати її у своїх предметних областях. Крім того, якщо нам потрібно створити велику онтологію, ми можемо інтегрувати дещо з наявних онтологій, які описують частини великої предметної області. Ми також можемо повторно використовувати основну онтологію і розширити її для описування предметної області, яка нас цікавить [12].

Відокремлення знань предметної області від оперативних знань – це ще один варіант загального застосування онтологій. Ми можемо описати задачу конфігурації продукту з його компонентів відповідно до необхідної специфікації та впровадити програму, яка робить цю конфігурацію незалежною від продукту і самих компонентів. Після цього ми можемо розробити онтологію компонентів і характеристик комп'ютерних комплексів і застосувати цей алгоритм для конфігурації нестандартних комп'ютерних комплексів [12].

Розглянувши можливі змістові інтерпретації поняття “онтологія”, зупинимося докладніше на структурі онтології, її складових.

У загальному вигляді [23], [28] структура онтології являє собою набір елементів чотирьох категорій: поняття; відношення; аксіоми; окремі екземпляри.

Поняття [23], [28] розглядаються як концептуалізації класу всіх представників якоїсь сутності або явища. Класи (або поняття) є загальними категоріями, які можуть бути впорядковані ієрархічно. Кожен клас описує групу індивідуальних сутностей, які об’єднані на підставі наявності загальних властивостей.

Поняття можуть бути пов’язані різними відношеннями (наприклад, довжина, місце розташування), які пов’язують воєдино класи і описують їх. Найпоширенішим типом відношень, що використовується у всіх онтологіях, є відношення категоризації, тобто зарахування до певної категорії. Цей тип відношень має й інші назви [23], [24], [28], що вживаються в різних дослідженнях: таксономічне відношення; відношення IS-A; клас – підклас; родові відношення; відношення a-kind-of..

Аксіоми [23], [24], [28] задають умови співвіднесення категорій і відношень, вони виражають очевидні твердження, що зв’язують поняття і відношення. Під аксіомою можна розуміти твердження, що вводиться в онтологію в готовому вигляді, з якого можуть бути виведені інші твердження. Вони дають змогу виразити ту інформацію, яка не може бути відображена в онтології за допомогою побудови ієрархії понять і встановлення різних відношень між поняттями. Аксіоми дозволяють надалі здійснювати висновки в межах онтології. Вони можуть забезпечувати дослідників інформацією про правила, дають змогу автоматично додавати інформацію. Аксіоми можуть також являти собою обмеження, що накладаються на які-небудь відношення, що уможливлюють здійснення висновків.

Поряд із зазначеними елементами онтології, в неї також входять так звані “Екземпляри”. У літературі вони можуть виступати також як такі примірники [21] - [24], [28]: конкретні екземпляри; інстанції; індивідуальні екземпляри.

Примірники [21] - [24], [28] – це окремі представники класу сутностей або явищ, це конкретні елементи якої небудь категорії.

Складові онтології підпорядковані своєрідній ієрархії. На нижньому рівні цієї ієрархії – екземпляри, конкретні індивіди, вище поняття, тобто категорії. На рівень вище розташовуються відношення між цими поняттями, а узагальнювальним і сполучним є ступінь правил або аксіом.

У роботах [23], [25], [26], [28] термін “онтологія” відображає широкий спектр структур, що представляють знання про ту чи іншу предметну область. Так, до онтологій можна зарахувати структури, що відрізняються різним ступенем формалізованості: глосарій; проста таксономія; тезаурус (таксономія з термінами); понятійна структура з довільним набором відношень; повністю аксіоматизована теорія. Однак у цих структурах не завжди представлені всі складові онтології.

Тому при розробці підходу до виявлення деструктивного впливу на першому етапі буде використано метод онтології для структуризації інформації (рубрикації текстового контенту), на другому етапі використано фільтр у вигляді матриці основу якої складає алгоритм та підходи що стосується класичної підготовки інформаційних операцій, що включають етапи планування операції, підготовки до операції і безпосередньо проведення самої операції.

В даному випадку розглядаємо семантичну задачу.

На першому етапі буде здійснено рубрикацію текстового контенту.

Спираючись на [16] аналіз лексико-граматичної та семантико-прагматичної побудови тексту використовують для автоматичної рубрикації контенту та формування дайджестів, що призводить до формування тематично підібраних масивів контенту (див. табл. 1).

Таблиця 1 – Основні етапи рубрикації текстового контенту

Назва	Призначення етапу
Підготовка	Визначення тематики/мети /об'єкта аналізу, хронологічні та географічні рамки, принципи відбору.
Збір даних	Формування класифікатора відбору ключових цитат та інструкції для кодувальника.
Формальний аналіз	Перетворення фрагментів тексту без аналізу його змісту. Морфологічні данні забезпечують доступ до змісту, опосередкованого через співвідношення одиниці змісту з одиницями виразу.
Змістовий аналіз	Аналіз елементів логіко-семантичних відношень між ними для подання семантики контенту.
Синтаксичний аналіз	Автоматично за наявності лексико-граматичних та граматичних даних до кожного слова синтаксично прив'язують словоформи у реченні.
Морфемний аналіз	Сегментування тексту, для виділення префіксів можливе без знання частин мови, а суфіксів- ні: потрібні різні їх набори та процедури відсікання суфіксів для кожної частини мови окремо.
Класифікація	Автоматичне опрацювання фрагментів текстового контенту для розпізнавання змісту.
Кодування	Кодування фрагментів текстового контенту.
Архівація	Збереження фрагментів текстового контенту в базі даних.

Класичний процес планування спільних інформаційних операцій представлений в табл. 2.

Кожний крок зазначеної таблиці представляється у вигляді матриць. Кожний елемент матриць відображає ознаки деструктивного впливу або ознаки етапів підготовки.

Перемножуючи результати рубрикації тексту, які представлені у вигляді архівів (матриць) на матриці які відображають ознаки етапів інформаційної операції (див. табл. 2) отримаємо значення, якщо воно рівне 1, значить в блоці інформації (рубриці), що аналізується присутні елементи деструктивного впливу (ознаки планування, підготовки та проведення інформаційної операції) і необхідно здійснювати заходи нейтралізації зазначеного контенту. У разі коли результат має значення 0. Пошук продовжується.

Таблиця 2 – Етапи (кроки) класичного процесу планування спільних інформаційних операцій країн НАТО.

Етап (крок)	Зміст етапу (кроку)
Крок 1	Отримання Завдання
Крок 2	Аналіз Завдання
Крок 3	Розвиток Варіантів Дій
Крок 4	Аналіз Варіантів Дій (Воєнна Гра/Wargaming)
Крок 5	Порівняння Варіантів Дій
Крок 6	Затвердження Варіантів Дій
Крок 7	Створення Бойового Наказу

Таким чином, в статті запропонований підхід щодо пошуку ознак деструктивних кібердій, який складається з наступних етапів:

з допомогою онтологічного методу здійснюється контент-аналіз тесту і здійснюється його рубрикація;

з використанням формалізованого алгоритму підготовки до проведення інформаційної операції здійснюється аналіз тексту на предмет ознак початку підготовки до інформаційної операції. В результаті робиться висновок про наявність ознак деструктивних кібердій. І формується завдання на планування заходів їх нейтралізації.

В подальшому розроблений підхід буде використаний при розробці методу автоматизованого виявлення деструктивного кібервпливу у кіберпросторі.

Висновки. 1. Сьогодні на Україну здійснюються потужні деструктивні інформаційні та кібер впливи в тому числі шляхом поширення неповної, спотвореної або упередженої інформації через кіберпростір. Тому актуальним завданням є виявлення деструктивних кібердій.

2. Організований інформаційний вплив на людей в кібепросторі та через кіберпростір є специфічним явищем сучасності, важливим і ефективним засобом досягнення різних цілей на тактичному, оперативному і стратегічному рівнях. Негативний інформаційний вплив інформаційних повідомлень все частіше використовується як зброя. Контент-моніторинг кіберпростору з метою виявлення деструктивного впливу дасть змогу підвищити ефективність забезпечення інформаційної та кібер- безпеки України у воєнній сфері та сприятиме: підвищенню ефективності оцінки, прогнозування розвитку суспільно-політичної та соціально-економічної обстановки; оперативній оцінці наслідків різних рішень і вибору з них найбільш раціональних в умовах деструктивного впливу (інформаційних загроз) та в особливий період; визначенню області ризику з найбільшою можливістю і величиною збитку у випадку реалізації ризиків; переходу від прийняття окремих рішень до вироблення комплексних сценаріїв (загальносистемних рішень).

3. Проведення контент-моніторингу кіберпростору та виявлення загроз інформаційній безпеці у воєнній сфері надаватиме якісну оцінку рівню інформаційного впливу на елементи інформаційної інфраструктури Міністерства оборони України та Збройних Сил України, а це, у свою чергу, дасть змогу розробляти адекватні контрзаходи з нейтралізації деструктивного впливу (інформаційних загроз).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] “Соціальні мережі: хто використовує і як?”, Gemius Україна. [Електронний ресурс]. Доступно: http://www.gemius.com.ua/e-commerce-novosti/socialni-merezhi-xto-vikoristovuje-i-jak.html. Дата звернення: Верес. 21, 2019.

[2] “Кількість користувачів Facebook в Україні досягла 13 мільйонів – дослідження”, *Media Sapiens*. [Електронний ресурс]. Доступно: https://ms.detector.media/mediaprosvita/research/kilkist_koristuvachiv_facebook_v_ukraini_dosyagla_13_milyoniv_doslidzhennya. Дата звернення: Верес. 21, 2019.

[3] О. Черниш, “Instagram в Україні росте швидше, ніж Facebook – дослідження”, *Громадський простір.* [Електронний ресурс]. Доступно: https://www.prostir.ua/?kb=instagram-v-ukrajini-roste-shvydshe-nizh-facebook-doslidzhennya. Дата звернення: Верес. 21, 2019.

[4] Д. Маркус, “Варшавський саміт НАТО і російська загроза”, *BBC News*. [Електронний ресурс]. Доступно: https://www.bbc.com/ukrainian/politics/2016/07/160708_warsaw_nato_summit_ozh. Дата звернення: Верес. 21, 2019.

[5] В. Рябих, “Саміт НАТО у Варшаві – підсумки й уроки”, *Укрінформ.* [Електронний ресурс]. Доступно: https://www.ukrinform.ua/rubric-other_news/2049186-samit-nato-u-varsavi-pidsumki-j-uroki.html. Дата звернення: Верес. 21, 2019.

[6] Заява за результатами саміту у Варшаві, *NATO – News*. [Електронний ресурс]. Доступно: https://www.nato.int/cps/uk/natohq/official_texts_133169.htm?selectedLocale=uk. Дата звернення: Верес. 21, 2019.
[7] Р. Геттемюллер "Кібератаки – це серйозно…", *NATO – News*. [Електронний ресурс]. Доступно:https://www.nato.int/cps/uk/natohq/news.htm?search_types=News&display_mode=news&keywordquery=Cyber%20defence%20&chunk=3. Дата звернення: груд. 21, 2019.
[8] Brussels Summit Declaration, *NATO – News.* [Online]. Available: https://www.nato.int/cps/uk/natohq/official_texts_156624.htm?selectedLocale=uk. Accessed on: Sept. 21, 2019.
[9] Верховна Рада України. *Закон № 2469-VIII від 21.06.2018 "Про національну безпеку України"*. [Електронний ресурс]. Доступно: https://zakon5.rada.gov.ua/laws/show/2469-19. Дата звернення: Верес. 21, 2019.
[10] Верховна Рада України. *Закон № 2163-VIII (із змінами) від 5 жовтня 2017 року, № 2469-VIII від 21.06.2018 "Про основні засади забезпечення кібербезпеки України"*. [Електронний ресурс]. Доступно: https://zakon5.rada.gov.ua/laws/show/2163-19.
[11] *Указі Президента України № 96/2016 від 15 березня 2016 року "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"*. [Електронний ресурс]. Доступно: https://zakon5.rada.gov.ua/laws/show/96/2016. Дата звернення: Верес. 21, 2019.
[12] А.В. Малишевский, *Качественные модели в теории сложных систем*. Москва, Российская Федерация: Наука. Физматлит., 1998.
[13] А.В. Лукацкий *Обнаружение атак: [Критерии атак и признаки их обнаружения. Источники информ. об атаках и методы их анализа. Классификация систем обнаружения атак. Критерии оценки систем обнаружения атак. Выбор и построение инфраструктуры обнаружения атак. Установка, размещение и эксплуатация систем обнаружения атак]*. Петербург, Российская Федерация: БХВ, 2003.
[14] Г. Хакен. *Синергетика*. Москва, Российская Федерация: Мир. 1980.
[15] О.В. Палагін, К.С. Малахов, В.Ю. Величко, та О.С. Щуров, "Проектування та програмна реалізація підсистеми створення та використання онтологічної бази знань публікацій наукового дослідника" *Проблеми програмування*, № 2, с. 72-81, 2017 [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Progr_2017_2_8. Дата звернення: Верес. 21, 2019.
[16] О.Є. Стрижак, "Інструменти інформаційно-аналітичного супроводу процесів моніторингу", *Екологічна безпека та природокористування*, Вип. 14, с. 180-191, 2014. [Електронний ресурс]. Доступно: http://nbuv.gov.ua /UJRN/ebpk_2014_14_20. Дата звернення: Верес. 21, 2019.
[17] Г. Буч. *Обьектно-ориентированное проектирование с примерами применения*. Москва, Российская Федерация: ООО "И. Д. Вильямс". 2008.
[18] О.Г. Славко, "Ідентифікація узагальнених параметрів математичної моделі компьютерної мережі в задачі забезпечення QOS", *Радіоелектронні і комп'ютерні системи*, № 3, с. 68–74, 2010.
[19] В.А. Куланов, "Об оценке диверсности реализации минимальних форм функций в различних базисах", *Радіоелектронні і компьютерні системи*, № 5 (32), 2008.
[20] T. Gruber, "A translation approach to portable ontologies", *Knowledge Acquisition*, № 5 (2), p. 199–220, 1993.
[21] В.В. Литвин, "Метод видобування знань з природомовних текстів для автоматизованої розбудови онтологій", *Автоматизовані системи управління та прилади автоматики*, №164, с. 67–72, 2013.
[22] В.В. Литвин, "Підхід до автоматичної побудови функцій інтерпретації під час навчання онтологій", *Вісн. Нац. ун-ту "Львівська політехніка". Інформаційні системи та мережі*, № 783, с. 361–368, 2014.
[23] В.В. Литвин, М.Я. Гопяк, О.В. Оборська, та Р.В. Вовнянка, "Метод побудови інтелектуальних агентів на основі адаптивних онтологій", *Lviv Polytechnic National University Institutional Repository*. [Електронний ресурс]. Доступно: http://ena.lp.edu.ua. Дата звернення: Верес. 21, 2019.

[24] Д.Г. Досин, В.В. Литвин, та Р.В. Вовнянка "Комп'ютерна система автоматизованої розбудови базової онтології Crocus", *Електротехнічні та комп'ютерні системи*, № 13(89), с. 135–143, 2014.

[25] В.В. Литвин, "Метод використання онтологій у петлі OODA", *Вісн. Нац. ун-ту "Львівська політехніка". Інформаційні системи та мережі,* № 783, с.137–145, 2014.

[26] В.В. Литвин, та О.В. Оборська, "Моделювання автоматизованої систем управління тактичної ланки на основі онтологічного підходу", *Вісник Кременчуцького національного університету імені Михайла Остроградського,* Вид. 5 (88), с. 92–97, 2014.

[27] В.В. Литвин, В.А. Висоцька, Д.Г. Досин, та М.Г. Гірняк, "Розроблення методів та засобів побудови інтелектуальних систем опрацювання інформаційних ресурсів з використанням онтологічного підходу", *Lviv Polytechnic National University Institutional Repository.* [Електронний ресурс]. Доступно: http://ena.lp.edu.ua. Дата звернення: Верес. 21, 2019.

[28] С.О. Довгий та ін., *Комп'ютерні онтології та їх використання у навчальному процесі. Теорія і практика: Монографія,* Київ, Україна:Інститут обдарованої дитини, 2013.

[29] С.В. Зинченко, "Концепция создания онтолого-управляемой информационной системы", *Інформаційні системи, механіка та керування*, Вип. № 1, с. 11, 2008.

[30] А.В. Палагин, Н.Г. Петренко, та А.О. Севрук, "Об одном подходе к формализованному представлению онтологии текстового документа", *Комп'ютерні засоби, мережі та системи*, №6, с. 14–20, 2007.

[31] М.А. Попова, "Методика побудови онтолого-керованих інформаційних ресурсів як елементу комп'ютерних ділових ігор для навчання фахівців в галузі екологічної безпеки", *Екологічна безпека та природокористування*, Вип. 10, 2012.

[32] А.В. Палагин, та Н.Г. Петренко, "Системно-онтологический анализ предметной области",. *УСиМ*, № 4, с. 3–14, 2009.

[33] О.В. Палагін, та М.Г. Петренко, "Розбудова абстрактної моделі мовно-онтологічної інформаційної системи", *Математичні машини і системи*, №1, с. 42–50, 2017.

[34] О.В. Палагін, М.Г. Петренко, та А.В. Михайлюк, "Розвиток та порівняльні характеристики логікоонтологічних формальних теорій", *Математичні машини і системи*, №2, с. 3–18, 2007.

[35] А.В. Палагин, та Н.Г. Петренко, "К вопросу системно-онтологической интеграции знаний предметной области", *Математические машины и системы*, №3,4, с. 63–75, 2007.

Стаття надійшла до редакції 25.09.2019.

REFERENCE

[1] "Social Networking: Who Uses and How ?", Gemius Ukraine. [Electronic resource]. Available: http://www.gemius.com.ua/e-commerce-novosti/socialni-merezhi-xto-vikoristovuje- i-jak.html. Accessed on: Sept. 21, 2019.

[2] "The number of Facebook users in Ukraine has reached 13 million - research", *Media Sapiens*. [Electronic resource]. Available: https://ms.detector.media/ mediaprosvita / research / kilkist_koristuvachiv_facebook_v_ukraini_dosyagla_13_milyoniv_doslidzhennya. Accessed on: Sept. 21, 2019.

[3] O. Chernysh, "Instagram in Ukraine is growing faster than Facebook – research", *Public space*. [Electronic resource]. Available: https://www.prostir.ua/?kb=instagram-v-ukrajini-roste-shvydshe-nizh-facebook-doslidzhennya. Accessed on: Sept. 21, 2019.

[4] D. Marcus, "Warsaw NATO Summit and the Russian Threat", *BBC News*. [Electronic resource]. Available: https://www.bbc.com/ukrainian/politics/2016/07/160708_warsaw_ nato_summit_ozh. Accessed on: Sept. 21, 2019.

[5] V. Ryabych, "The NATO Summit in Warsaw - Results and Lessons", *Ukrinform*. [Electronic resource]. Available: https://www.ukrinform.ua/rubric-other_news/2049186-samit-nato-u-varsavi-pidsumki-j-uroki.html. Accessed on: Sept. 21, 2019.

[6] Statement on the outcome of the Warsaw Summit, *NATO - News*. [Electronic resource]. Available: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale= en. Date of appeal: Sept. 21, 2019.

[7] R. Gettamuller "Cyberattacks Are Serious…", *NATO - News*. [Electronic resource]. Available: https: //www.nato.int/cps/en/natohq/news.htm? Search_types = News & display_mode = news & keywordquery = Cyber% 20defence% 20 & chunk = 3. Accessed on: Sept. 21, 2019.

[8] Brussels Summit Declaration, *NATO - News*. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en. Accessed on: Sept. 21, 2019.

[9] The Verkhovna Rada of Ukraine. *Law No. 2469-VIII of 21.06.2018 "On National Security of Ukraine"*. [Electronic resource]. Available at: https://zakon5.rada.gov.ua/laws/show/2469-19. Accessed on: Sept. 21, 2019.

[10] The Verkhovna Rada of Ukraine. *Law No. 2163-VIII (as amended) of October 5, 2017, No. 2469-VIII of June 21, 2018 "On Basic Principles of Cybersecurity of Ukraine".* [Electronic resource]. Available at: https://zakon5.rada.gov.ua/laws/show/2163-19. Accessed on: Sept. 21, 2019.

[11] *Presidential Decree No. 96/2016 of March 15, 2016 "On the decision of the National Security and Defense Council of Ukraine of January 27, 2016" On the Cybersecurity Strategy of Ukraine ".* [Electronic resource]. Available at: https://zakon5.rada.gov.ua/laws/show/96/2016. Accessed on: Sept. 21, 2019.

[12] A.V. Malishevsky, *Qualitative models in the theory of complex systems*. Moscow, Russian Federation: Science. Fizmatlit., 1998.

13] A.V. Lukatskiy *Detection of Attacks: [Criteria for attacks and signs of their detection. Sources of information. about attacks and methods of their analysis. Classification of attack detection systems. Evaluation criteria for attack detection systems. Selecting and building an attack detection infrastructure. Installation, deployment and operation of attack detection systems]*. Petersburg, Russian Federation: BHC, 2003.

[14] G. Hacken. *Synergetics*. Moscow, Russian Federation: World. 1980.

[15] O.V. Palagin, KS Malakhov, V.Yu. Velichko, and OS Shchurov "Design and program realization of the subsystem of creation and use of the ontological knowledge base of scientific researcher publications" *Programming Problems*, № 2, p. 72-81, 2017 [Online resource]. Available: http://nbuv.gov.ua/UJRN/Progr_2017_2_8. Accessed on: Sept. 21, 2019.

[16] AE Strizhak, "Tools of information and analytical support for monitoring processes", *Environmental Safety and Environmental Management,* Vol. 14, p. 180-191, 2014. [Electronic resource]. Available: http://nbuv.gov.ua / UJRN / ebpk_2014_14_20. Accessed on: Sept. 21, 2019.

[17] G. Butch, *Object-oriented design with examples of applications*. Moscow, Russian Federation: LLC "I. D. Williams", 2008.

[18] O.G. Slavko, "Identification of generalized parameters of a mathematical model of a computer network in the task of providing QOS," *Radio and Electronic and Computer Systems*, No. 3, p. 68–74, 2010.

[19] V.A. Kulanov, "On estimating the diversion of the implementation of minimal forms of functions in different bases", *Radioelectronic and Computer Systems*, No. 5 (32), 2008.

[20] T. Gruber, "A Translation Approach to Portable Ontologies," *Knowledge Acquisition*, No. 5 (2), p. 199–220, 1993.

[21] V.V. Litvin, "Method of extracting knowledge of natural-language texts for automated ontology development,", *Automated Control Systems and Automation Devices*, No. 164, p. 67–72, 2013.
[22] V.V. Litvin, "An Approach to the Automatic Construction of Interpretation Functions in Ontology Learning,", *Visn. Nat. University of Lviv Polytechnic. Information Systems and Networks*, № 783, p. 361–368, 2014.
[23] V.V. Litvin, M.Ya. Gopiak, OV Oborskaya, and RV Vovnyanka, "A method for constructing intelligent agents based on adaptive ontologies", *Lviv Polytechnic National University Institutional Repository.* [Electronic resource]. Available at: http://ena.lp.edu.ua. Date of appeal: Sept. 21, 2019.
[24] D.G. Dosin, V.V. Lytvyn, and R.V. Vovnyanka, "Computer System for Automated Development of Crocus Basic Ontology," *Electrical and Computer Systems*, No. 13 (89), p. 135–143, 2014.
[25] V.V. Litvin, "A Method for Using Ontologies in the OODA Loop," *Visn. Nat. University of Lviv Polytechnic. Information Systems and Networks*, № 783, p.137–145, 2014.
[26] V.V. Lytvyn, and O.V. Oborskaya, "Modeling of an Automated Tactical Link Control System on the Basis of an Ontological Approach", *Bulletin of Kremenchuk Mykhailo Ostrogradsky National University*, Ed. 5 (88), p.92–97, 2014.
[27] V.V. Litvin, V.A. Vysotska, D.G. Dosin, and M.G. Girnyak, "Development of methods and tools for building intelligent information resource processing systems using ontological approach", *Lviv Polytechnic National University Institutional Repository.* [Electronic resource]. Available at: http://ena.lp.edu.ua. Date of appeal: Sept. 21, 2019.
[28] S.O. Long and atc., *Computer ontologies and their use in the educational process. Theory and Practice: Monograph*, Kyiv, Ukraine: Gifted Child Institute, 2013.
[29] S.V. Zinchenko "Concept of creation of ontologically-managed information system", *Information systems, mechanics and control*, Iss. № 1, p. Nov 11, 2008
[30] A.V. Palagin, N.G. Petrenko, and A.O. Sevruk, "On an Approach to a Formalized Representation of a Text Document Ontology", *Computer Tools, Networks and Systems*, No. 6, p. 14–20, 2007.
[31] M.A. Popova, "Methodology for building ontologically-managed information resources as an element of computer-based business games for the training of environmental security professionals," *Environmental Safety and Environmental Management*, vol. Oct 10, 2012
[32] A.V. Palagin, and N.G. Petrenko, "System-ontological analysis of the domain", *USiM*, No. 4, p. 3-14, 2009.
[33] O.V. Pologin, and M.G. Petrenko, "Development of an abstract model of linguistic-ontological information system", *Mathematical Machines and Systems*, No. 1, p. 42–50, 2017.
[34] O.V. Pologin, M.G. Petrenko, and A.V. Mikhailuk, "Development and Comparative Characteristics of Logic-Ontological Formal Theories", *Mathematical Machines and Systems*, No. 2, p. 3-18, 2007
[35] A.V. Palagin, and N.G. Petrenko, "On the question of system-ontological integration of domain knowledge", *Mathematical Machines and Systems*, No. 3,4, p. 63–75, 2007

YURII DANYK,
KOSTIANTYN SOKOLOV,
OLEH HUDYMA

THE APPROACH TO AUTOMATED DETECTION OF DESTRUCTIVE CYBER INFLUENCES

Issues of information analysis and detection of destructive effects in cyberspace and across cyberspace are considered. In 2019, we confirmed the global trend in the growth of the

number of users of social information network services. Therefore, the importance of ensuring the fulfillment of information and cyber security tasks in electronic media and cyberspace analysis is increasing today. Taking into account the global trends in the detection of destructive cyber influences and in order to fulfill the tasks defined by the governing documents of the state, it is necessary to monitor cyberspace and the detection of destructive cyber influences (at the stages of planning, preparation and direct information actions). To implement the above, it is necessary to address the issue of developing appropriate models and methods for the automatic detection of destructive cyber influences. In order to create a basis for scientific research, the following studies were conducted: methods of analysis of information available in cyberspace for the detection of destructive cyber influences; advantages and disadvantages of known methods of detecting destructive cyber-influences; known cyberspace monitoring systems. The main features (functions) of known cyberspace monitoring systems are: keyword data search and fixation of available information about information disseminators (their total number, activity over a certain period, actor accounts, gender, age, geographical location, audience reach). There is a need to identify approaches in developing decision support methods and models regarding the detection of destructive cyber influences in cyberspace. In developing an approach to detecting destructive cyber-influences, an ontology method is used in the first stage to structure information (text content rubrics). Advantages of using ontological diagrams in the process of information impact detection are: the presentation of the subject area (problems) in tabular or graph form, the detection of hidden relationships, the accumulation and analysis of information online, checking the consistency of facts. In the second stage, a filter-matrix is applied that reflects the processes (planning, preparation and direct implementation of information actions) of a classic NATO information operation. The prospect of further research is to develop a method for the automated detection of destructive cyber influences in cyberspace.

Keywords: cyberspace, security, destructive, cyber impact, detection, monitoring, method.

Даник Юрій Григорович, доктор технічних наук, професор, заслужений діяч науки і техніки України, начальник, Інститут інформаційних технологій Національного університету оборони України імені Івана Черняховського, Київ, Україна.

ORCID: 0000-0001-6990-8656.

E-mail: zhvinau@ukr.net.

Соколов Костянтин Олександрович, начальник, Управління інформаційних технологій Міністерства оборони України, Київ, Україна.

ORCID: 0000-0002-5182-5569.

E-mail: saks555skat@gmail.com.

Гудима Олег Петрович, кандидат технічних наук, старший науковий співробітник, начальник відділу інформаційних ресурсів, Управління інформаційних технологій Міністерства оборони України, Київ, Україна.

ORCID: 0000-0002-3494-8583.

E-mail: Olgud18@gmail.com.

Danyk Yurii, doctor of technical sciences, professor, honored worker of science and technology of Ukraine, head, Institute of information technologies of National University of Defense of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

Sokolov Kostiantyn, head, Department of information technology, Ministry of defense of Ukraine, Kyiv, Ukraine.

Hudyma Oleh, candidate of technical sciences, senior researcher, head, Branch of information resources, Department of information technology, Ministry of Defense of Ukraine, Kyiv, Ukraine.