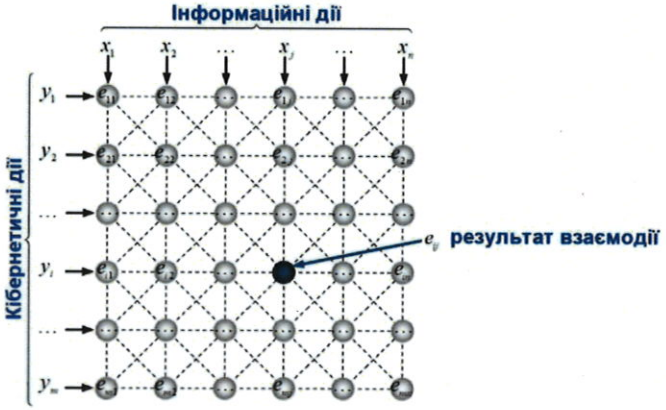
І. Грабар
Р. Грищук
К. Молодецька

БЕЗПЕКОВА СИНЕРГЕТИКА:
КІБЕРНЕТИЧНИЙ ТА ІНФОРМАЦІЙНИЙ АСПЕКТИ



Монографія

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ НАЦІОНАЛЬНИЙ АГРОЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ
ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

І. Г. Грабар, Р. В. Грищук,
К. В. Молодецька

Безпекова синергетика: кібернетичний та інформаційний аспекти

Монографія

За загальною редакцією
доктора технічних наук, професора Р. В. Грищука

Житомир
2019

УДК 004.056:004.738.5(045)
Г 75

Рекомендовано до друку вченою радою
Житомирського національного агроекологічного університету
(протокол № 4 від 21 листопада 2018 року)

Рецензенти:

В. О. Хорошко – доктор технічних наук, професор;
Н. Ф. Казакова – доктор технічних наук, доцент;
С. П. Євсеєв – доктор технічних наук, доцент.

Грабар І. Г.

Г 75 Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.
ISBN 978-617-7684-14-4

У монографії розглянуто теоретичні та практичні основи забезпечення інформаційної безпеки людини, суспільства, держави у кібернетичному та інформаційному просторах з використанням синергетичного підходу. Розкрито синергетичні ефекти, які виникають внаслідок ведення інформаційної та кіберборотьби, досліджено питання синергетичного управління взаємодією користувачів у інформаційному просторі соціальних інтернет-сервісів. Представлено практичні рекомендації щодо застосування розроблених методологічних засад та наведено модельні приклади.

Для фахівців у галузі інформаційної безпеки і наукових працівників та інженерно-технічних спеціалістів. Монографія може бути корисною для аспірантів, магістрантів і студентів, котрі спеціалізуються у сфері управління інформаційною безпекою та систем захисту інформації.

ISBN 978-617-7684-14-4

ЗМІСТ

CONTENTS IN BRIEF

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСКМ	–	автоматизованої системи контент-моніторингу;
ВС	–	віртуальна спільнота;
ЗМК	–	засоби масової комунікації;
е-ЗМК	–	електронні засоби масової комунікації;
ІБ	–	інформаційна безпека;
ІБД	–	інформаційна безпека держави;
ІКТ	–	інформаційно-комп'ютерні тенології;
ІП	–	інформаційне повідомлення;
ІПсО	–	інформаційно-психологічна операція;
ДА	–	дивний атрактор;
КС	–	комп'ютерна система;
МНК	–	метод найменших квадратів;
РЕБ	–	радіоелектронна боротьба;
СВА	–	система виявлення атак;
СІО	–	суб'єкти інформаційного обміну;
СІС	–	соціальні інтернет-сервіси;
СМ	–	соціальні мережі;
ФП	–	фазовий перехід.

ПЕРЕДМОВА

Ідеї синергетики
відіграють центральну роль
в останній за часом науковій революції
Елвін Тофлер

У сучасному інформаційному суспільстві широке поширення одержав такий тип віртуальних спільнот в соціальних інтернет-сервісах, як соціальні мережі, які окрім виконання функцій підтримки спілкування, обміну думками й одержання інформації їхніми членами – акторами останнім часом все частіше стають об'єктами й засобами інформаційного впливу й ареною інформаційного протиборства.

Віртуальні спільноти (англ. *virtual communities, e-communities*) (ВС) у широкому трактуванні – це новий тип соціальних утворень, які виникають і функціонують в електронному просторі й формуються, перш за все, за допомогою мережі Інтернет. ВС створюються з метою сприяння вирішенню своїх професійних потреб, політичних амбіцій, задоволення своїх інтересів у мистецтві, дозвіллі, тощо [1].

Термін "віртуальні спільноти" (*Virtual Community*) вперше ввів Г. Рейнгольд, який надав йому таке визначення: "Віртуальні спільноти є соціальними об'єднаннями, які виростають з Мережі, коли група людей підтримує відкрите обговорення достатньо довго і людяно, для того, щоб сформувати мережу особистих стосунків в кіберпросторі" [2].

Найбільш розповсюдженими нині віртуальними спільнотами є соціальні мережі (СМ). Різні фахівці дають дуже схожі визначення цьому явищу. Зокрема у [3] під соціальною мережею розуміють інтернет-сервіс за допомогою якого люди можуть здійснювати зв'язок між собою та об'єднуватися за специфічними інтересами. Завдання такого сервісу полягає у тому, щоб забезпечити користувачів всіма можливим шляхами для комунікації один з одним. Рекомендації Управління інформаційних технологій щодо поводження в соціальних та пірінгових мережах для персоналу Міністерства оборони України та Генерального штабу Збройних Сил України [4] дають таке визначення цьому явищу: СМ – це соціальна структура, яка являє собою інтерактивний розгалужений сайт, контент якого наповнюють учасники мережі. Підтримка зв'язку між учасниками соціальної мережі забезпечується *web*-сервісом внутрішньої пошти чи службою миттєвої відправки повідомлень.

Таким чином ВС в інформаційному просторі є принципово новою стійкою формою існування соціальних відносин, які перевершують соціальні соціуми за ступенем організованості та піддатливістю до впливу. Досвід інформаційних впливів через ВС переконливо свідчить про необхідність приділення посиленої уваги з боку держави до діяльності та розвитку "соціальних мереж". Водночас, така увага не повинна порушувати права людини, зафіксовані у законодавстві.

Одним з основних факторів, який суттєво стримує ефективне функціонування створюваної згідно з [5] Системи забезпечення інформаційної безпеки Міністерства оборони (МО) України та Збройних Сил (ЗС) України, є відсутність на озброєнні відповідних підрозділів органів військового управління новітніх спеціалізованих програмних та (або) апаратно-програмних засобів добування, обробки,

узагальнення та аналізу контентного забарвлення інформації про потенційні загрози інформаційній безпеці держави у воєнній сфері, за результатами моніторингу інформації з СМ.

Тому, для підвищення ефективності інформаційної діяльності органів військового управління в роботі розробляється та впроваджується автоматизована система контент-моніторингу та контент-аналізу соціальних інтернет-сервісів. Вона базується на принципах воєнно-технічного аналізу та орієнтується на використання сучасних інформаційних технологій. Для вирішення даного завдання в роботі приведено результати аналізу існуючих і перспективних засобів контент-моніторингу інформації з СМ, визначено їх переваги та недоліки, розроблено науково-технічні пропозиції для удосконалення методики контент-моніторингу інформації з СМ та визначено основні завдання й функції автоматизованої системи контент-моніторингу (АСКМ) інформації з СМ.

Розробленні програмні компоненти цієї системи рекомендовано застосовувати на постах *OSINT*-розвідки військових частин інформаційно-психологічних операцій, а також доцільно впровадити в освітній процес Житомирського військового інституту імені С. П. Корольова і Житомирського національного агроекологічного університету для підготовки військових фахівців та фахівців галузі інформа-ційних технологій.

Основами (засадами) державної інформаційної політики щодо забезпечення інформаційної безпеки (ІБ) є система заходів, спрямованих на:

запобігання інформаційним загрозам (викликам, впливам) шляхом превентивних заходів із забезпечення ІБ з метою попередження можливості їх виникнення;

виявлення інформаційних загроз та деструктивних впливів, яке полягає у систематичному моніторингу, аналізі й контролі можливості появи реальних або потенційних інформаційних загроз;

впровадження своєчасних заходів з нейтралізації інформаційних загроз/впливів, прогнозування інформаційних ризиків;

вживання заходів з ліквідації (локалізації) загроз/впливів;

ліквідацію наслідків негативних інформаційних впливів.

Швидкий темп розвитку та впровадження у повсякденне життя комп'ютерної техніки та телекомунікаційних технологій тісно пов'язаний із розвитком мережі Інтернет, завдяки якій стає можливим доступ до електронних документів, представлених у різних форматах, як державних установ, інформаційних агентств, так і звичайних користувачів. Все більша частина користувачів використовує мережу Інтернет для задоволення потреб свого інформаційного забезпечення, пов'язаного як з професійною діяльністю, так і з особистими потребами.

Таким чином, електронні засоби масової інформації (ЗМІ) стрімко нарощують свою аудиторію, а отже перетворюються на потужний ресурс масштабного розповсюдження відповідного контенту серед населення, охоплюючи практично всі категорії та вікові групи.

В даний час, в умовах зовнішньої агресії РФ по відношенню до України, проведення Антитерористичної операції на території Донецької та Луганської областей, електронні ЗМІ широко використовуються противником для здійснення деструктивного інформаційно-психологічного впливу (ІПсВ) на військово-політичне керівництво, особовий склад та населення. Аналіз стрімкого розвитку інформацій-

ної зброї, здатної ефективно впливати на психіку людей та інформаційно-технологічну інфраструктуру держави, підтверджує ефективність програмування поведінки (діяльності) окремих людей і населення в цілому шляхом впливу на електронні банки даних, знань та інформації.

Сучасні можливості електронних ЗМІ, в поєднанні з науковою та публіцистичною літературою, періодикою дозволяють ефективно впливати на розум, свідомість і психіку мільйонів людей. Інформація та пропаганда стали сьогодні настільки могутніми, що здатні зумовлювати появу, перебіг і кінцевий результат політичних подій, навіть глобальних проблем миру й війни. Небезпека полягає в тому, що на перший план все більше висуваються інформаційно-психологічні технології, які дозволяють перетворити країну-опонента в регіон керованої кризи. У своїй основі такі технології являють собою процес впливу на джерела інформації прийняття стратегічних рішень, заохочення етнічного сепаратизму і внутрішньої регіоналізації, нав'язування чужої культури і побутового мислення, що унеможливлює стратегічне бачення державних проблем. У поєднанні з політико-дипломатичним тиском, що спирається на військову силу, такі технології стають більш ефективними, ніж застосування сучасних засобів збройної боротьби [1, 2].

Досвід військової агресії РФ проти України засвідчує той факт, що інформаційне протиборство стало не просто самостійним театром сучасної війни, але таким театром, хід та результати протиборства на якому в багатьох випадках виявляються більш важливими, ніж хід та результати власно збройного протиборства. Зміст процесів, що відбуваються у свідомості людей, які мають відношення до підготовки та веденню війн, мають ключове значення для її ходу та результату. Як наслідок, у разі вдалого вирішення завдання щодо впливу на свідомість цих людей у відповідному напрямку зацікавлена сторона отримує можливість спрямовувати хід війни у вигідне для себе русло [1, 2].

Додаткову цінність для загальної військової стратегії інформаційно-психологічних операцій (ІПсО) надає той факт, що на полі інформаційної війни відсутній безпосередній ризик отримання втрат. Наприклад, мета, яка шляхом бойової операції досягається ціною великих втрат вбитими та пораненими, завдяки ефективно спланованій та проведеній інформаційній компанії може бути досягнута безкровно, шляхом дезорганізації бойових порядків противника, зниженням морально-психологічного стану його військ, насадження серед них панічного страху чи, навпаки, пацифізму. При цьому слід зазначити, що ефективність впливу на свідомість цивільного населення у зоні конфлікту, а також нейтральних країн має не менше значення для успіху інформаційно-психологічного протиборства, ніж вплив на свідомість військовослужбовців. Інформаційний фон, що складається у суспільстві під час війни, позначається на відношенні населення до політики свого уряду та дій силовиків, на комплектуванні армії, функціонуванні воєнної економіки та інших сфер, що впливають на хід війни. Більше того, усі зусилля органів військового управління щодо захисту власних військ від ворожої пропаганди можуть бути нівельовані, якщо аналогічна робота з населенням не проводиться чи проводиться на недостатньому рівні, так як суспільне відношення щодо війни буде невідворотно транслюватись у збройні сили [1, 2].

Таким чином, моніторинг електронних ЗМІ з метою своєчасного виявлення інформаційних загроз та деструктивних ІПсВ на органи військового управління, особовий склад та населення є однією з основних складових забезпечення ІБ як

держави в цілому, так і її складових: органів управління, суспільства, окремої людини. Виходячи з вищезазначеного, актуальною є задача розробки програмної компоненти каталогізації та первинної обробки матеріалів електронних ЗМІ.

Матеріали монографії "Безпекова синергетика: кібернетичний та інформаційний аспекти" підготували Р. В. Грищук - розділ 1 і розділ 3, І. Г. Грабар - розділ 2, К. В. Молодецька - п. 1.2, 1.3 розділу 1 та п. 3.3, 3.4 розділу 3.

РОЗДІЛ 1
РОЛЬ ІНФОРМАЦІЙНОГО ТА КІБЕРПРОСТОРУ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

1.1. Соціальні інтернет-сервіси та причини їх популярності на прикладі соціальних мереж

Стрімкий розвиток високотехнологічного суспільства не в останню чергу обумовлений повсюдним проникненням в усі сфери його життєдіяльності новітніх досягнень у галузі інформаційних технологій. Як було показано в [1, 2] визначальну роль у такому суспільстві відіграють високі технології та новітні засоби масової комунікації на їх основі [3, 4]. Функція останніх при цьому зводиться до надання послуг мобільного соціального інтернет-сервісу (СІС), який забезпечує оперативний обмін інформаційними потоками між його суб'єктами та, як правило, при виконанні необхідних та достатніх умов спонукає до хаотично керованої вихідної дії [5].

Сучасні СІС представляють собою платформу або веб-сайти, які призначені для створення соціальних мереж або соціальних взаємозв'язків між людьми, які, наприклад, мають спільні інтереси, діяльність або утворюють реальні чи віртуальні об'єднання. Зазвичай СІС містять інформацію про кожного актора, яка називається профілем, його соціальні зв'язки з іншими акторами та віртуальними спільнотами, а також надають актору низку додаткових послуг. Більшість СІС мають веб-інтерфейс і виступають як засоби взаємодії акторів через мережу Інтернет.

Аналіз змісту категорії "соціальний інтернет-сервіс" (*social networking service*) у вітчизняній літературі показав, що він не має чіткої дефініції. Останні дослідження [6–8] зарубіжних вчених показали, що характерними ознаками сучасних СІС є:

1) СІС представляють собою *Web* 2.0 інтернет-додатки;

2) актори створюють контент, який визначає потенціал СІС;

3) засобами СІС актори створюють профілі, які підтримуються функціями;

4) СІС забезпечують взаємодію профілю актора з іншими акторами і/або віртуальними спільнотами.

Враховуючи останні дослідження [1, 6–9] і особливості їх застосування в різних сферах суспільної діяльності [10–12], сформулюємо такі дефініції категорій:

актор СІС – це користувач, який має профіль, створений засобами СІС;

соціальний інтернет-сервіс – це сервіс у мережі Інтернет для створення профілів акторів, встановлення ними взаємозв'язків з іншими акторами і віртуальними спільнотами та забезпечення інструментами комунікації, створення й поширення контенту різного типу.

Нині широке поширення одержав такий тип віртуальних спільнот в СІС як соціальні мережі (СМ) [13–15], що окрім виконання комунікаційних функцій між їх користувачами стають об'єктами інформаційного впливу та управління [16] і, як наслідок, ареною інформаційного протиборства [17].

Події, що відбуваються в Україні протягом останніх років, починаючи з 2013 р., показали реальні як деструктивні, так і позитивні можливості з використання соціальних мереж в інтересах інформаційного протиборства та поширення деструктивного контенту. Так, напередодні української Революції гідності Російською Федерацією використано усі можливості соціальних мереж для цілеспрямованого інформаційного впливу не тільки на громадян України та світове співтовариство, а й на власне населення, з метою формування вигідної для неї громадської думки [17–25].

Відомо, що до найбільш розповсюджених СМ, які використовуються громадянами на пострадянському просторі є такі мережі як *ВКонтакте*, *Одноклассники, Мой мир@Mail.ru, Мой круг, Соратники, Rambler Планета, Мир тесен, Привет.ру, RuSpace, Gosu, GameSport, FiXX.RU, TooDoo, Факультет.ру, НаВиду, Facebook*, *Classmates, MySpace, LinkedIn* та ін. Крім того останнім часом в силу суб'єктивних і об'єктивних причин інтенсивно починає поширюватися соціальна мережа *Google+*.

ВКонтакте (*vk.com*) – найбільша соціальна мережа в Рунеті. Вона заснована ще в 2006 р. П. Дуровим. Нині дана мережа позиціонується як сучасний, мобільний інтернет-майданчик для спілкування між учасниками її віртуальних спільнот. Її можливості дозволяють іншим СІС використовувати спеціально розроблені інструменти – віджети для інтеграції її з іншими соціальними мережами та сервісами. Так згідно з офіційними даними СМ *ВКонтакте* станом на 2016 р. можливості віджетів користувачами використовуються у такій пропорції: 47% – для новинних стрічок та профілів; 12 % – для фотографій; 8% – для віртуальних спільнот; 8% – для повідомлень; 4% – для аудіо та відео; 3% – для додатків; 18% – для інших розділів.

Аналіз використання віджетів користувачами СМ *ВКонтакте* дозволяє зробити висновок про те, що дана мережа є більш інформативною, оскільки майже половину від усіх її ресурсних можливостей користувачами використовується для обміну новинними стрічками і профілями. Віджети дозволяють вбудовувати у персональні сторінки користувачів коментарі, посилання на віртуальні спільноти, системи опитувань, а також відкривають можливості для репостінгу контенту й обміну посиланнями з іншими користувачами. Соціальна мережа *ВКонтакте* має і мобільну версію *m.vk.com*, що забезпечує їй додаткові можливості з розширення аудиторії прихильників, особливо соціально активного віку від 18 до 34 років. Таким чином, СМ *ВКонтакте*, в якій уже зареєстровані більше ніж 350 млн. аккаунтів [26] й надалі залишається головним конкурентом іншим соціальним мережам в Рунеті. Якщо враховувати той факт, що щоденна аудиторія в даній СМ в 2016 р. складає не менше 74 млн, а в лютому цього ж року перевищила позначку в 81 млн., то можна спрогнозувати й надалі утримання даною мережею першого місця з відвідуваності та кількості прихильників.

Для того, щоб встановити причини популярності СІС на прикладі СМ *ВКонтакте,* розглянемо базовий спектр комунікаційних послуг, що надається цією мережею. *По-перше*, дописувач, користувач або просто особа, яка цікавиться інформацією про персональну сторінку будь-якого користувача, що становить інтерес, у разі її відкритості останньої, має доступ до таких персональних даних як: дата і місце народження; місце навчання та проживання; номер мобільного телефону; наявність близьких родичів та друзів; дані про місце проживання тощо (рис. 1.1).

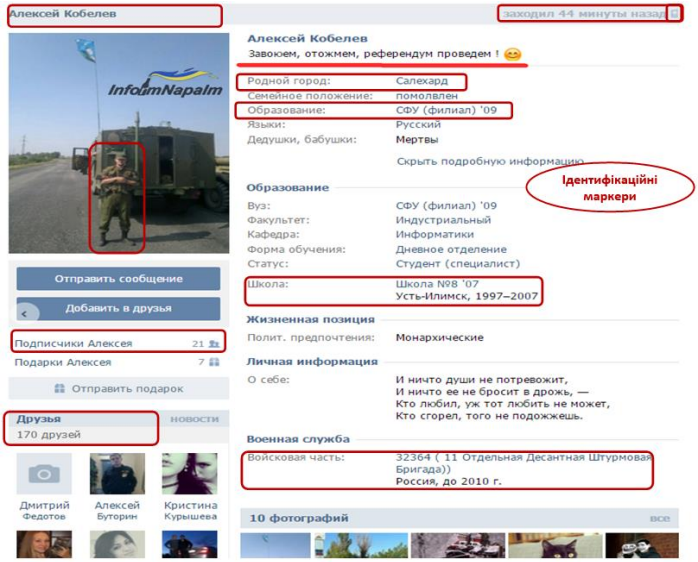


Рис. 1.1. Ідентифікаційні маркери сторінки користувача в соціальній мережі ВКонтакте (на прикладі сторінки російського найманця під час агресії Російської Федерації проти України 2014 р., за даними сайту INFORMNAPALM.ORG)

При цьому слід зважити на те, що такі дані будуть достовірними тільки у тому разі, якщо вони не є фейком (підробленням або підміною реальних даних). *По-друге,* під час аналізу сторінки відкривається можливість доступу до переліку груп (віртуальних спільнот) до складу яких входить чи інформацією з яких цікавить користувач. *По-третє,* є можливість доступу до фото-, відео- та аудіоконтенту, як створеного користувачем із зазначенням до нього деяких маркерів, наприклад, дати, часу, геоданих тощо, так і перепощуваного з інших джерел. *По-четверте,* відкривається доступ до новинної стрічки, що відкриває можливості до її вивчення та ґрунтовного аналізу. Особливістю СМ *ВКонтакте* є фіксація на сторінці користувача такого маркера, як час онлайн перебування у мережі або останній час відвідування сторінки (див. рис. 1.1).

Розглянемо іншу, не менш популярну в Рунеті СМ – *Одноклассники.* Проект заснований А. Попковим у 2005 р., а нині підтримується російською технологічною компанією *Mail.Ru Group* [27]. За даними *LiveInternet* щоденна аудиторія сайту, наприклад за квітень 2016 р., складає 46,9 млн відвідувачів, що на 40% менше за СМ *ВКонтакте* за аналогічний період. Нині, станом на серпень 2016 року аудиторія мережі складає близько 51 млн користувачів [28]. Характерною рисою СМ *Одноклассники,* порівняно з СМ *ВКонтакте* є звуження віку найбільш активної аудиторії з 26 до 35 років та зміщення акцентів на користувачів віком до 45 років й старше (рис. 1.2) [28].

Таким чином, однією з причин популярності СМ *Одноклассники*, як показує наведений приклад, є можливість створення комунікаційного майданчика для спілкування між бувшими співвітчизниками, які нині в силу політико-історичних обставин проживають в державах СНД та в інших регіонах світу. Іншими словами – це комунікація між людьми, які в недалекому минулому мали щось спільне, яке їх

об'єднувало за деякими спільними ознаками. В першу чергу – це школа, місто, держава, історія тощо.

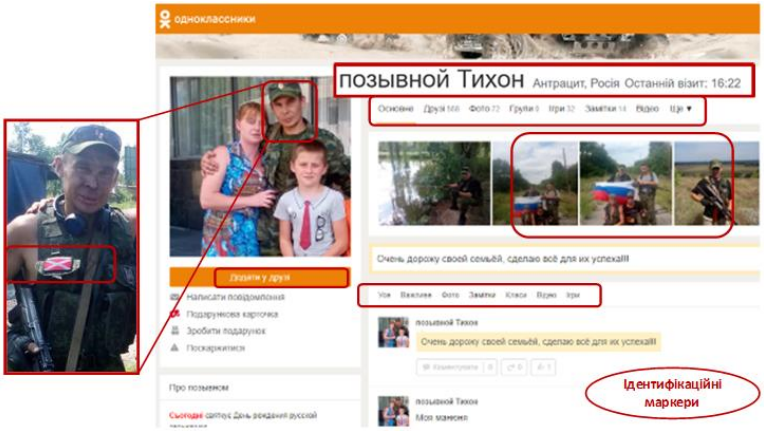


Рис. 1.2. Ідентифікаційні маркери сторінки користувача в соціальній мережі Однокласники (на прикладі сторінки російського найманця під час агресії Російської Федерації проти України 2016 р., за даними сайту https://ok.ru/profile/579853900854?st.filterGroupId=203)

Розглянемо іншу СМ, яка серед інших відомих соціальних проектів у мережі Інтернет є найпопулярнішою за кількістю учасників. Це СМ *Facebook*, яка заснована в 2004 р. М. Цукербергом. У розрізі останніх подій в Україні вона також використовується користувачами як інструмент інформаційної боротьби (рис. 1.3.).

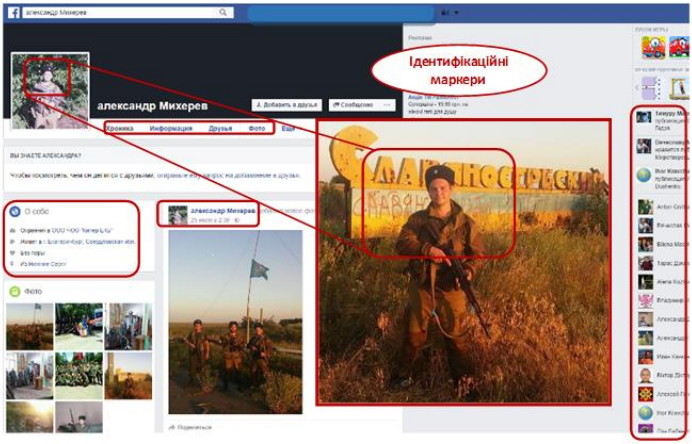


Рис. 1.3. Ідентифікаційні маркери сторінки користувача в СМ Facebook (на прикладі сторінки російського найманця під час агресії Російської Федерації проти України 2016 р., за даними сайту https://www.facebook.com/mikherev.a.a)

Станом на 25 квітня 2016 р. користувачами *Facebook* були 5,4 млн українців [29], що склало близько 0,4% від усієї аудиторії даної соціальної мережі за 2016 р. Сторінка окремого активного користувача СМ *Facebook*, на прикладі сторінки російського найманця (див. рис. 1.3), містить значну кількість ідентифікаційних ма-

ркерів. Але розробник мережі потурбувався й про те, що доступ до ідентифікаційних маркерів і контенту на персональній сторінці може бути обмеженим. Так, незареєстрований у даній СМ користувач не має доступу до ідентифікаційних маркерів або контенту користувача яким він цікавиться.

До основних причин, які забезпечили популярність СМ *Facebook*, порівняно з іншими СІС, можна віднести такі:

найбільша аудиторія, яка в другому кварталі 2016 р. налічує близько 1,71 млрд користувачів в цілому та активних користувачів близько 1,13 млрд, зокрема [30];

найбільша аудиторія мобільних активних користувачів (1,57 млрд в червні 2016 р.);

третину активних користувачів складає соціально активний прошарок суспільства – молодь у віці від 24 до 35 років;

темп зростання потенціальної аудиторії активного користувача СМ *Facebook* нарощується за геометричною прогресією [31]. Але справедливо слідує зауважити те, що її зростання через деякий часовий інтервал буде обмежено;

розміщення кожним активним користувачем за добу в середньому близько чотирьох одиниць різноманітного контенту тощо.

Twitter (англ. *Twitter* – "щебетати") (*twitter.com*) – СІС, що дозволяє користувачам відправляти короткі текстові замітки (обсягом до 140 символів), використовуючи веб-інтерфейс, *SMS*, засоби миттєвого обміну повідомленнями або сторонні програми клієнти. Створений Дж. Дорсом в 2006 р. Станом на початок 2015 р. сервіс нараховує понад 300 млн користувачів, з них 50 млн користуються *Twitter* щодня. Переважна більшість – близько 55% користуються *Twitter* через мобільні гаджети [3]. Причиною популярності *Twitter* є публічна доступність розміщених в мережі повідомлень (рис. 1.4).

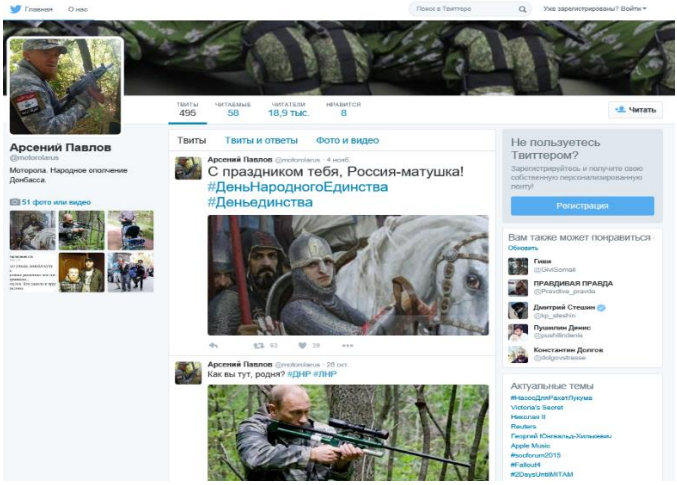


Рис. 1.4. Сторінка акаунту донецького терориста в СМ Twitter

Google+ (plus.google.com) – СМ розроблена компанією *Google*. Вона офіційно почала свою роботу в 2011 р. На початок 2015 р. кількість зареєстрованих в *Google+* користувачів перевищувала 200 млн чол. [3]. Сервіс відкриває можливості до спілкування через Інтернет за допомогою спеціальних компонентів: кола, теми,

відеозустрічі, мобільна версія. Основними причинами популярності СМ *Google+* є надання таких сервісів, при цьому інформація, який діляться учасники мережі, впливає на персоналізацію результатів пошуку у найбільшій інформаційно-пошуковій системі *Google*. В основі роботи *Google+* покладено концепцію кіл (*Circles*), завдяки яким актор регулює своє спілкування. На основі кіл користувач ділиться контентом, визначаючи, які кола будуть мати доступ до інформації, а які – ні. Обмін користувальницькими матеріалами здійснюється через спеціальну стрічку. Компанією *Google* була представлена також і мобільна версія цієї СМ, у якій є дві унікальних функції: миттєве завантаження фото й чат (*Huddle*).

Україна не стоїть осторонь процесів соціальної комунікації. Останнім часом, особливо після початку російської агресії в Україні з'явилися та набувають популярності вітчизняні СМ. На поточний час їх нараховується близько двадцяти. Розглянемо найбільш поширені з них [4].

WeUA – одна з наймолодших та найперспективніших національних СМ. Після запуску СМ 1 квітня 2014 р. сайт піддався потужній *DDoS* атаці. Нині вона перейменована у *INREPUBLIC*. Станом на червень 2015 р. *WeUA* налічувала понад 155 тис. зареєстрованих користувачів. Інтерфейс цієї СМ нагадує *ВКонтакте* та *Facebook*. Але порівняно з ними функціонал у *WeUA* був недостатньо розвиненим, тому дана СМ постійно доопрацьовувалася розробниками. 1 січня 2016 р. проект мав оновитись, попередню реєстрацію було продовжено до 1 лютого. Станом на 1 лютого 2016 р. відкрита реєстрація продовжувалась, почався тестовий режим.

Українці. Мережа *Українці* була створена в січні 2009 р. та має перспективи розвитку з точки зору інтерфейсу і креативності оформлення. Кількість користувачів у ній нараховує близько 10 тис. У мережі не підтримується ні музика, ні відео. Поняття стрічки відсутнє. СМ *Українці* може бути корисною акторам, в спілкуванні яких переважає текстова інформація.

vReale – це СМ, назва якої запозичена з відомої мережі *ВКонтакте*. СМ надає можливість моментальної реєстрації та містить лічильник користувачів. На даний час зареєстрованих користувачів більше 28 тис. СМ перебуває на стадії активного розвитку.

Друзі. Мережа була започаткована у 2009 р. та з початку була копією *ВКонтакте*. Але згодом дизайн сайту приведено до стилю *Windows 8*. Функціонально СМ *Друзі* є поєднанням функцій таких мереж як *ВКонтакте*, *Facebook* та *МойМир*. У СМ поширюється різноманітний контент: музика, відео, фото, текстові додатки. Однією з причин, яка може надати їй популярності є наявність онлайн телебачення та радіо, гостьової сторінки тощо.

Friends.ua – СМ яка не схожа на конкурентів ні інтерфейсом, ні опціями. У СМ відсутні аудіозаписи, натомість є форум та щоденники типу мікроблогу. Логіка та компонування цієї СМ повторює ідею порталу *online.ua*. Нині в СМ *Friends.ua* зареєстровано більше 95 тис. акторів.

Українці онлайн. Це один із СІС сайту *Онлайн.ЮА* (*online.ua*). У даній СМ основна увага приділяється текстовим записам та блогам. Фото з відео реалізовані посередньо, аудіо та додатки відсутні.

У всіх СМ, в тому числі й розглянутих, існує пакет документів, які надаються адміністраціями сайтів, у відкритому доступі. Аналіз документів, які регламентують порядок реєстрації в розглянутих СМ, правила захисту інформації про акторів та збереження конфідеційності особистих даних показав що:

1. Достовірність розміщених даних завжди сумнівна, перевірити їх неможливо.

2. Навіть достовірна інформація доступна лише настільки, наскільки користувач не приховує її вбудованими у самій мережі налаштуваннями безпеки.

3. Незареєстрований у СМ актор не має доступу до повного переліку усіх можливих персональних даних.

Такі характерні риси "закриття" особистих даних мережі з одного боку слугують для забезпечення безпеки користувача, проте з іншого не дозволяють проводити якісно моніторинг віртуальної поведінки та реакцій на зовнішні впливи вибраних користувачів.

За численними дослідженнями [21, 22] та в результаті аналізу встановлено, що СІС все більше набувають популярності, постійно збільшується кількість зареєстрованих акаунтів та зростає потік публічної інформації, в тому числі й оперативної з місця подій. Тому інтернет-користувачі більше довіряють відгукам, залишених саме в СМ. Це і є основними причинами, що обумовлюють популярність СМ, а відповідно й доцільність їх використання як джерела розвідувальних відомостей для проведення контент-моніторингу.

1.2. Види сучасних соціальних інтернет-сервісів

Результати досліджень різноманіття сучасних СІС показали, що вони динамічно розвиваються і вдосконалюються [9]. Використаємо спільні принципи, покладені в основу їх функціонування, для розробки узагальненої класифікації СІС із застосуванням ознакового принципу на основі ієрархічного підходу [31]. Перевагою ієрархічної класифікації є простота, логічність побудови і висока інформаційна ємність, а жорсткість її структури забезпечить чітке віднесення окремого СІС до визначених функціональних груп.

Встановлено ознаки класифікації СІС, які наведені на рис. 1.5 [33]:

а) за способом доступу акторів до СІС:

1. Веб-браузер – доступ до сервісу реалізовано на основі веб-інтерфейсу;

2. Застосунок – передбачає розробку спеціального застосунку для роботи з СІС під управлінням операційної системи кінцевого пристрою користувача.

б) за доступністю СІС поділяють на:

1. Відкриті, які доступні для реєстрації всім користувачам;

2. Закриті – безпечні платформи, які використовуються обмеженим колом акторів, що відповідають заданим вимогам віртуальної спільноти. Наприклад, *ASmallWorld*, *BeautifulPeople*, *Decayenne*, *Qube*, *Teazel*, *HotEnough*, *Eleqt*.

в) за функціональним призначенням розрізняють такі СІС:

1. Соціальні пошукові системи (*social search*) – це сервіси, які дозволяють акторам самостійно визначати пріоритетні напрямки пошуку контенту, задавати ключові слова, обирати джерела контенту і форму подання результатів [10]. Такий пошук можна адаптувати до тематики віртуального співтовариства. Прикладами соціальних пошукових систем є *Google*, *Swiki*, *Rollyo*, *Flexum*.

2. Соціальні закладки (*social bookmark*) – централізована онлайн-служба, яка дозволяє акторам додавати, анотувати, редагувати і обмінюватися закладками, використовуючи теги [10, 12]. До соціальних закладок відносять *Blinklist*, *Delicious*, *BlogBookMark*, *Clipclip*, *Cloudytags*.

3. Вікі (*Wiki*) – інтернет-сервіс, побудований на основі технології створення колекції зв'язаних між собою записів, які можуть створювати і редагувати

ЛІТЕРАТУРА

1. Р. В. Грищук, та Ю. Г. Даник. *Основи кібернетичної безпеки : монографія*, Житомир: ЖНАЕУ, 2016.

2. Ю. Г. Даник, та О. О. Труш. "Особливості забезпечення національної безпеки у високотехнологічному суспільстві" – Харківський регіональний інститут державного управління НАДУ при Президентові України. [Електронний ресурс]. Доступно: http://ifs.kbuapa.kharkov.ua/e–book/db/2010–1 /doc/5/02.pdf.

3. Р. В. Грищук, Ю. Г. Даник, та О. В. Самчишин. "Мобільні соціальні інтернет-сервіси як один із різновидів масової комунікації на сучасному етапі", *Безпека інформації*. Т. 21, № 1, с. 16–20, 2015.

4. Ю. Г. Даник, Р. В. Грищук, та О. В. Самчишин. "Сучасні мобільні соціальні інтернет сервіси як один з перспективних засобів масової комунікації" на *Наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2015, с. 232–235.

5. H. H. Khondker. "Role of the New Media in the Arab Spring", *Globalizations*, vol. 8, no. 5, p. 675–679, 2011.

6. Jonathan A. Obar, and Steve Wildman. "Social media definition and the governance challenge: An introduction to the special issue", *Telecommunications policy*, 39 (9), pp. 745–750, 2015.

7. Andreas M. Kaplan, and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of social media", *Business Horizons*, 53 (1), p. 61, 2010.

8. D. M. Boyd, and N. B. Ellison. "Social Network Sites: Definition, History, and Scholarship", *Journal of computer-mediated communication*, 13 (1),pp. 210–230, 2007.

9. О. Якимчук. "Онлайнові соціальні мережі: перспективи розвитку", *Релігія та Соціум*, № 2(6), с. 199–205, 2011.

10. Luca Longo et al. "Enhancing Social Search: A Computational Collective Intelligence Model of Behavioural Traits, Trust and Time", *Transactions on Computational Collective Intelligence II : Lecture Notes in Computer Science*, vol. 6450, p. 46, 2010.

11. G. Michael, and Chr. Meinel. "Web Search Personalization Via Social Bookmarking and Tagging", *Lecture Notes in Computer Science*, pp. 367–380, 2007.

12. T. Aichner, and F. Jacob. "Measuring the Degree of Corporate Social Media Use", *International Journal of Market Research*, 57(2), pp. 257–275, 2015.

13. S. Wasserman, and K. Faust. *Social Network Analysis Theory and Applications*, New York: Cambridge University Press, 1994.

14. О. С. Онищенко, В. М. Горовий, В. І. Попик та ін. *Соціальні мережі як чинник розвитку громадянського суспільства: монографія*, Київ: НАН України, Нац. б-ка України ім. В. І. Вернадського, 2013.

15. В. М. Сазанов *Социальные сети – публичная сфера*, М.: Лаборатория СВМ, 2012.

16. Д. А. Губанов, Д. А. Новиков, и А. Г. Чхартишвили. *Социальные сети: модели информационного влияния, управления и противоборства*, М.: Изд. физ.-мат. лит., 2010.

17. Р. В. Грищук, І. О. Канкін, та В. В. Охрімчук. "Технологічні аспекти інформаційного протиборства на сучасному етапі", *Захист інформації*, т. 17, № 1, с. 80–86, 2015.

18. І. Гриненко, та Д. Прокоф'єва-Янчиленко. "Вплив віртуальних спільнот на інформаційну безпеку: сучасний стан та тенденції розвитку", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, № 1(23), с. 18–23, 2012.

19. А. М. Пелещишин, та Р. В. Гумінський. "Загрози інформаційної безпеки держави в соціальних мережах", *Наука і техніка Повітряних Сил Збройних Сил України*, №2, с. 192–199, 2013.

20. Г. Буркацька, А. Саприкін, та ін. *Протидія інформаційним війнам: інформація як щит і меч: бібліогр. покажч.*, К., 2014.

21. О. С. Онищенко, В. М. Горовий, В. І. Попик, та ін. *Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства: монографія*, К., 2014.

22. В. Горовий, О. Онищенко, В. Попик та ін. *Соціокультурні механізми формування ментального імунітету проти зовнішніх маніпуляцій свідомістю населення України: монографія.* Київ, 2015.

23. S. González-Bailón, and N. Wang "Networked discontent: The anatomy of protest campaigns in social media", *Social Networks*, № 44, pp. 95–104, 2016.

24. *Соціальні мережі як чинник інформаційної безпеки. Інформаційно-аналітичний бюлетень* – Центр досліджень соціальних комунікацій. [Електронний ресурс]. Доступно: http://nbuviap.gov.ua/index.php?option=com_content&view=category&layout=blog&id=26&Itemid=187.

25. Geers K. *Cyber War in Perspective : Russian Aggression against Ukraine*. Tallinn: CCDCOE, 2015.

26. *О сайте : Аудитория ВКонтакте* – Социальная сеть Вконтакте. [Электронный ресурс]. Доступно: https://vk.com/page-47200925_44240810.

27. *Направление бизнеса: Социальные сети* – Mail.Ru Group. [Электронный ресурс]. Доступно: https://corp.mail.ru/ru/company/social.

28. *Аудитория и возможности 2016 : Развлекательная социальная сеть Одноклассники* – INCIDE.RU. [Электронный ресурс]. Доступно: https://sales.mail.ru/media/presentations/OK_Mediakit_160315-2.pdf.

29. *Кількість користувачів Facebook в Україні почала рости швидше* – Media Sapiens. [Електронний ресурс]. Доступно: http://osvita.mediasapiens.ua/web/social/kilkist_koristuvachiv_facebook_v_ukraini_pochala_rosti_shvidshe.

30. *The Top 20 Valuable Facebook Statistics – Updated July 2016* – Zephoria Inc. [Електронний ресурс]. Доступно: https://zephoria.com/top-15-valuable-facebook-statistics.

31. *Facebook Reports Second Quarter 2016 Results* – PR Newswire. [Online]. Access: http://www.prnewswire.com/news-releases/facebook-reports-second-quarter-2016-results-300305084.html.

32. О. Г Корченко, С. В. Казмірчук, Є. В. Паціра, С. О. Гнатюк, та В. М. Кінзерявий. "Ознаковий принцип формування класифікацій кібератак", Вісн. СНУ ім. В. Даля, № 4, т. 1, с. 184–193, 2010.

33. К. В. Молодецька. "Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави", *Information technology and security*, vol. 4, № 1(6), с. 13–20, 2016.

34. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко. *Політика інформаційної безпеки: підручник.* К.: ПВП «Задруга», 2014.

35. Р. В. Грищук, та К. В. Молодецька. "Метод прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах", *Системи управління, навігації та зв'язку*, № 4(36), с. 60–65, 2015.

36. Закон України «Про інформацію» : [Електронний ресурс] / Офіційний портал Верховної ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2657-12 (дата доступу: 07.03.16). – Назва з екрану.

37. Золотар О. О. Класифікація загроз інформаційної безпеки / О. О. Золотар, І. О. Трубін // Інформація і право. – 2013. – № 3(9). – С. 105–112.

38. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський, *Інформаційна безпека України в умовах євроінтеграції*, К.: КНТ, 2006.

39. Офіційне представництво Президента України. (2017, Лют. 25). Указ Президента України №47/2017, *Доктрина інформаційної безпеки України.* [Електронний ресурс]. Доступно: http://www.president.gov.ua/documents/472017-21374.

40. Міністерство інформаційної політики України. (2015, Черв. 5). *Проект Концепції інформаційної безпеки України.* [Електронний ресурс]. Доступно: http://mip.gov.ua/documents/30.html. Дата звернення: Лист. 07, 2017.

41. Верховна Рада України. (2003, Черв. 19). Закон України № 964-15, *Про основи національної безпеки України.* [Електронний ресурс]. Доступно: http://zakon2.rada.gov.ua/laws/show/964-15. Дата звернення: Лист. 07, 2017.

42. Верховна Рада України. (2007, Січ. 09). Закон України №537-16, *Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки.* [Електронний ресурс]. Доступно: http://zakon4.rada.gov.ua/laws/show/537-16.

43. Р. В. Грищук, *Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень*, Житомир: Рута, 2010.

44. Р. В. Грищук, "Диференціально-ігрові моделі та методи моделювання процесів кібернападу", дис. д-ра техн. наук, Нац. авіац. ун-т, Київ, 2013.

45. К. В. Молодецька. "Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах", *Защита информации: сб. науч. труд.*, вып. 23, с. 75–87, 2016.

46. *Жорстка сила* – Wikipedia. [Online]. Access: https://uk.wikipedia.org/wiki/Жорстка_сила.

47. *М'яка сила* – Wikipedia. [Online]. Access: https://uk.wikipedia.org/wiki/М%27яка_сила.

48. *Розумна сила* – Wikipedia. [Online]. Access: https://uk.wikipedia.org/wiki/Розумна_сила.

49. B. H. Liddell Hart. *Strategy*, 1954.

50. Гончар О. http://newsdaily.com.ua/post/1176679.

51. І. Рущенко. *Російсько-українська гібридна війна: погляд соціолога*, Х., 2015.

52. Г. Хакен. *Синергетика. Иерархия неустойчивостей в самоорганизующихся системах и устройствах*, М.: Мир, 1985.

53. В. С. Иванова. "Механика разрушения и конструкционная прочность с позиций синергетики", *Вестник машиностроения*, №12, с. 8-12, 1989.

54. И. Пригожин. *От существующего к возникающему*, М.: Наука, 1985.

55. В. С. Иванова, и В. Ф. Терентьев. *Природа усталости металлов*, Металлургия, 1975.

56. В. С. Иванова. "Синергетика разрушения" в *Ресурс и прочность оборудования нефтеперерабатывающих заводов,* Уфа, с. 3–28, 1989.

57. В. С. Иванова. "Синергетическая модель разрушения металлов и сплавов по механизму отрыва (Тип 1)", *ФХММ*, т.24, С.51–56, 1988.

58. В. С. Иванова. *Разрушение металлов*, М.: Металлургия, 1979.

59. V. S. Ivanova. "Mechanics and synergetics of the selfsimilar growth of a fafique Chark", *Enqineering Fracture Mech.*, vol. 28, No. 5/6, pp. 733–739, 1987.

60. А. А. Шанявский, и А. Ю. Сасов. "Фурье-фрактографический автоматизированный РЭМ-анализ переодической структуры усталостных бороздок", ФХММ, №1, с. 65–70, 1990.

61. А. А. Шанявский. "Самоорганизация кинетики усталостных трещин", в кн. *Синергетика и усталостные разрушения металлов*, М.: Наука, с. 57–76, 1989.

62. Шанявский А.А. "Теория дискретного РУТ в металлах", *Изв. АН СССР, Металлы*,№ 3, с.159–163, 1984.

63. В. С. Иванова, и А. А. Шанявский. *Количественная фрактография. Усталостное разрушение*, Челябинск: Металлургия, 1988.

64. В. А. Борисенко. "Температурная зависимость прочности молибдена", *Проблемы прочности*, №12, с. 36-44, 1976.

65. Борисенко В.А. "Прочность и внутреннее трение молибдена", *Проблемы прочности,* №6, с. 77-82, 1976.

66. В. А. Борисенко, В. П. Кращенко, В. Е. Стаценко, и И. Г. Грабар. "Явление упорядоченной дискретности на температурных зависимостях прочностных характеристик технической меди", на II Всесоюзн. конф. *Прочность материалов и конструкций при низких температурах*, Киев, ИПП АН УССР, с. 16, 1986.

67. В. И. Трефилов, Ю. В. Мильман, и С. А. Фирстов. *Физические основы прочности тугоплавких металлов*, 1975.

68. *Деформационное упрочнение и разрушение поликристаллических металлов*, Ред. В. И. Трефилова, Киев: Наук. думка,1987.

69. Л. М. Рыбакова. "Исследование структурных нарушений – деструкции пластически деформированного металла", дисс. д-ра. техн. Наук, Москва, 1976.

70. А. И. Радченко. "Дискретно-вероятностная модель выработки ресурса деталей и элементов конструкций", в кн. *Вопросы эксплуатационной долговечности и живучести конструкций ЛА*, Киев: КИИГА, с. 3–12, 1982.

71. А. С. Баланкин, А. А. Любомудров, и И. Т. Севрюков. *Кинетическая теория кумулятивного бронепробивания*, М.: МО СССР, 1989.

72. А. С. Баланкин. "Кинетическая (флуктуационная) природа гидродинамического режима высокоскоростной деформации твердых тел", *Письма в ЖТФ*, т. 14, №13, 1988.

73. А. С. Баланкин. "Самоорганизация и диссипативные структуры в деформируемом теле", *Письма в ЖТФ*, т. 15, N19, 1989.

74. А. С. Баланкин. "Синергетика и механика деформируемого тела", *Письма в ЖТФ*, т. 59, N12, 1989.

75. Г. М. Бартенев. *Прочность и механизм разрушения полимеров*, М.: Химия, 1984.

76. В. Е. Панин. "Волновая пророда пластической деформации твердых тел", *Письма в ЖТФ*, т. 59, N12, с. 4–18, 1989.

77. В. Е. Панин, В. А. Лихачев, и Ю. В. Гриняев. *Структурные уровни деформации твердых тел*, Новосибирск: Наука, 1985.

78. В. А. Лихачев, В. Е. Панин, и Е. Э. Засимчук. *Кооперативные деформационные процессы и локализация деформации*, Киев: Наук. думка, 1989.

79. А. И. Олемской. "Фрактальная кинетика ползучести твердого тела", *ФТТ*, т. 30, №11, с. 3384–3394, 1988.

80. В. Е. Панин. "Новая область физики твердого тела", *Изв. ВУЗов. Физика*, №1, с. 3–8, 1987.

81. А. И. Олемский, и В. А. Петрунин. "Перестройка конденсированного состояния атомов в условиях интенсивного внешнего воздействия", *Известия ВУЗов. Физика*, №1, с. 82 -121, 1987.

82. В. И. Арнольд. "Теория катастроф", *Природа*, №10, с. 54–63, 1979.

83. В. И. Арнольд, А. Н. Варченко, и С. М. Гусейн-Заде. *Особенности дифференцируемых отображений*, М.: Наука, 1982.

84. В. И. Арнольд. "*Теория катастроф*", Современные проблемы математики. Фундаментальные направления, М.: ВИНИТИ, т. 5, с. 219–277, 1986.

85. E. Basar. *Biophysical and Phisiological system Analysis*, Addison-Wesley, Reading, MA, 1976.

86. T. H. Bullock, R. Orkand, and A. Grinnel. *Introduction to Nervous Systems*, Freeman, San Francisco, 1977.

87. W. Ebeling, and R. Feistel. *Physik der Selbstorganisation und Evolution*, Akademie - Verlag, Berlin, 1982.

88. R. W. Hockney, and C. R. Jesshope. *Parallel Computers*, Hilger, Bristol, 1981.

89. K. S. Fu. *Syntactic Pattern Recagnition Applications*, Springer, Berlin, Heidelberg, New York, 1976.

90. F. Cap. *Handbook on Plasma Instabilities*, Academie, New York, 1976.

91. А. Б. Михайловский. *Теория плазменных неустойчивостей*, М.: Атомиздат, 1977.

92. Х. Вильхельмсон, и Л. Вейланд. *Когерентное нелинейное взаимодействие волн в плазме*, М.: Энергоиздат, 1981.

93. В. Л. Поляченко, и А. М. Фридман. *Равновесие и устойчивость гравитирующих систем*, М.: Наука, 1976.

94. Н. Н. Горькавый, и А. М. Фридман. "Физика планетных колец", *УФН*, т.160, N2, с.169-237, 1990.

95. А. И. Троянский. "Особенности температурных зависимостей характеристик упругости твердых тел", автореф. дис. канд. техн. наук, ИПП АН УССР, Киев, 1990.

96. В. И. Муромцев, И. А. Дудак, и С. А. Кучеренко и др. "Обнаружение методом ЭПР релаксации флуктуаций квантовых переходов между структурными состояниями твердого тела", в кн. *Системы особых температурных точек твердых тел*, М.: Наука, с. 94–105, 1986.

97. *Синергетика и усталостное разрушение металлов*, Ред. В.С. Иванова, М.: Наука, 1989.

98. *Нелинейные волны. Структуры и бифуркации*, Ред. А. В. Гапонов-Грехов, М.: Наука, 1987.

99. *Фракталы в физике*, М.: Мир, 1988.

100. М. И. Рабинович, и М. М. Сущик. "Регулярная и хаотическая динамика структур в течениях жидкости", *УФН*, т. 160, N1, с. 3–64, 1990.

101. *Гидродинамические неустойчивости и переход к турбулентности*, Ред. Х. Суинни, и Дж. Голлаба, М.: Мир, 1984.

102. H. Benard. *Rev. Gen. Sci. Puser Appl.*, v. 11, p. 1261, 1990.

103. М. Фейгенбаум. "Универсальность в поведении нелинейных систем", *УФН*, т. 141, N2, с. 343–374, 1983.

104. Г. Шустер. *Детерминированный хаос. Введение*, М.: Мир, 1988.

105. В. С. Анищенко. *Сложные колебания в простых системах*, М.: Наука, 1990.

106. Г. Николис, и И. Пригожин. *Познание сложного*, М.: Мир, 1990.

107. Ф. Мун. *Хаотические колебания,* М.: Мир, 1990.

108. А. А. Шанявский. "Методология количественной фрактографии эксплуатационных усталостных разрушений деталей", автореф. дисс. д-ра. техн. наук, Москва, МАТИ, 1988.

109. В. С. Айфрамович. "Качественная теория стохастических автоколебаний", автореф. дисс. д-ра. физ.-мат. наук, Саратов, СГУ, 1990.

110. В. С. Анищенко. "Механизм развития и свойства хаотических колебаний в радиофизических системах с конечным числом степеней свободы", автореф. дисс. докт. физ.-мат. наук, Саратов, СГУ, 1986.

111. С. П. Кузнецов. "Нестационарные нелинейные процессы и стохастические колебания в распределенных системах радиофизики и электроники", автореф. дисс. докт. физ.-мат. наук, Саратов, СГУ, 1987.

112. В. В. Федоров. "Исследование и разработка научных основ прогнозирования повреждаемости и разрушения металлов", автореф. дисс. докт. техн. наук, М.: ВНИИЖГ, 1980.

113. В. В. Рыбин. "Физические основы развитой пластической деформации и вязкого разрушения поликристаллов", автореф. дисс. докт. физ.-мат. наук, Киев, ИФМ АН УССР, 1979.

114. А. А. Андронов, А. А. Вит, и С. Э. Хайкин. *Теория колебаний*, М.: Наука, 1981.

115. Л. Д. Ландау, и Е. М. Лифшиц. *Гидродинамика*, М.: Наука, 1988.

116. Ж. Йосс, и Д. Джозеф. *Элементарная теория устойчивости и бифуркаций*, М.: Мир, 1983.

117. М. И. Рабинович, и Д. И. Трубецков. *Введение в теорию колебаний и волн*. М.: Наука,1984.

118. Е. Б. Вул, Я. Г. Синай, и К. М. Ханкин. "Универсальность Фейгенбаума и термодинамический формализм", *УМН*, т. 39, N3, с. 3-37, 1984.

119. Y. Aizava. "Syrerqetic Approach to the Phenomena of Mode – Locking in Nonleniar Systems", *Progress of Theoretical Physics*, v. 56, N3, p. 703-716, 1976.

120. И. И. Блехман. *Синхронизация в природе и технике*, М.: Наука, 1981.

121. В. А. Васильев, Ю. М. Романовский, и В. Г. Яхно. *Автоволновые процессы*, М.: Наука, 1987.

122. А. С. Монин. "Тидродинамическая неустойчивость", *УФН*, т.150, N1, с. 61–105, 1986.

123. К. Дж. Вильсон. "Ренормализационная группа и критические явления", *УФН*, т. 141, N2, с. 194–220, 1983.

124. В. И. Арнольд. "Особенности, бифуркации и катастрофы", *УФН*, т.141, N4, с. 569–590, 1983.

125. В. И. Арнольд. "Лекции о бифуркациях и версальных семействах", *УМН*, т. 27, N5, с. 119–184, 1972.

126. В. С. Анишенко. "Взаимодействие странных аттракторов. Перемежаемость типа "хаос"-"хаос". - Письмо в ЖТФ. 1984, т.10, N 10, С.629-632.

127. В. Н. Штерн. *Динамика против термодинамики*, Новосибирск, Препринт Института теплофизики СО АН СССР, 1986.

128. *А. В. Гапонов-Грехов, М. И. Рабинович, и И. М. Старобинец.* "Рождение многомерного хаоса в активных решетках", *ДАН СССР*, т. 279, с. 596–601, 1984.

129. С. П. Кузнецов. "Ренормгруппа, универсальность и скейлинг в динамических одномерных автоволновых средах", *Изв. ВУЗов. Радиофизика*, т. 29, N8, с. 888–902, 1986.

130. В. А. Давыдов, и А. С. Михайлов. "Спиральные волны в распределенных активных средах" в кн. *Нелинейные волны. Структуры и бифуркации*, М.: Наука, с. 261–279, 1987.

131. B. B. Mandelbrot. *The Fractal Geometry of Nature,* Freeman, San Francisco, 1982.

132. И. Г. Грабар. "Исследование нелинейных явлений накопления усталостных повреждений в алюминиевом материале Д16АТВ", автореф. дисс. канд. техн. наук, Киев, КИИГА, 1983.

133. І. Г. Грабар. *Термоактиваційний аналіз та синергетика руйнування*, Житомир: ЖІТІ, 2002.

134. В. Грони. *Основи математичної кібернетики*, Житомир: ЖДТУ, 2004.

135. І. Г. Грабар, Ю. Г. Даник, и С. В. Ковбасюк. *Математичне моделювання та оптимізація складних систем*, Житомир, 2015.

136. І. Г. Грабар, і О. І. Грабар. “Моделювання кінетики хаотизації аттрактора Фейгенбаума і динаміка нелінійних систем”, *Вісник ЖДТУ*, №3, 2012.

137. І. Г. Грабар, і О. І. Грабар. “Кількісна оцінка висоти хаосу дивних ат тракторів в задачах динаміки нелінійних систем”, *Вісник ЖНАЕУ*, №2, 2012.

138. І. Г. Грабар. “Моделювання висоти і структури хаосу”, на Всеукр. конф. *Інформатика та системні науки*, Полтава, 2016.

139. І. Г. Грабар, О. І. Грабар, О. А. Гутніченко, і Ю. О. Кубрак. *Перколяційно-фрактальні матеріали*, Житомир: ЖДТУ, 2007.

140. І. Г. Грабар. “Перколяційно-фрактальні моделі в сучасному матеріалознавстві”, *Наукові нотатки ЛНТУ*, 2015.

141. І. Г. Грабар, Є. І. Хадаківський, О. В. Вознюк, і Л. Ю. Возна. *Синергетика економічних систем*, Житомир: ЖДТУ, 2003.

142. С. А. Алиев. *Размытие фазовых переходов в полупроводниках и высокотемпературных сверхпроводниках. Монография*, Баку, Элм, 2007.

143. С. А. Алиев, и Ф. Ф. Алиев. *Неорганические Материалы*, 1985.

144. Sabir Aliev, Ziraddin Gasanov, Zakir Agayev, and Rasim Guseynov. *Abhandlungen der WGB*, Band 3, Berlin, 2003.

145. Б. Н. Ролов. *Размытие фазовые переходы Рига*, 1972.

146. Б. Н. Ролов, и В. Э. Юркевич. *Физика размытых фазовых переходов*, Изд. Рост. Университета, 1983.

147. Л. Г. Качурин, и В. Г. Морачевский. *Кинетика фазовых переходов воды в атмосфере*, Л.: ЛГУ, 1965.

148. А. И. Алымов, и М. Х. Шоршоров. “Влияние размерных факторов на температуру плавления и поверхностное натяжение ультрадисперсных частиц”, *Изв. РАН. Металлы*, №2, с. 29–31, 1999.

149. С. А. Безносюк, и А. Е. Бандин. “Компьютерное модели-рование плавления сферических наночастиц металлов”, *Полифункциональные химические материалы и технологии : сб. статей*, т. 1, 2007.

150. В. В. Новиков, С. В. Филиппова, и О. В. Мовчанюк. “Перколяционная модель фінансового рынка”, *Труды Одесского политехнического университета*, #2, с. 237–240, 2009.

151. Ю. Ф. Зуев и др. “Структурные перестройки в супрамолекулярной каталитической системе АОТ-ИОНАТ-ВОДА в присутствии моно- и полиэтиленгликоля”, *Журнал чтруктурной химии*, т. 46, с. 888–894, 2005.

152. Ю. Ф. Зуев, и др. “Особенности иммобилизации субстракта и каталитическая активность трипсина в обращенной микроэмульсии”, *Вестн. Моск. ун-та. Сер. 2. Химия*, Т. 44. №1, 2003.

153. А. И. Тупицына, и Ю. А. Фадин. “Исследование проницаемости и перколяционных свойств системы твердых прямоугольных частиц методом компьютерного моделирования”, *ЖТФ*, т. 86, №10, 2016.

154. P. F. Verhulst. “Notice sur la loi que la population poursuit dans son accroissement”, *Correspondance mathématique et physique*, 10, p. 113–121, 1838.

155. М. В. Постникова, и др. “Ротовая жидкость, как объект оценки функционального состояния организма человека”, *Вестник Волгогр. гос. универ. Сер. 3. Экон. Экол.*, №1(18), с. 251–256, 2011.

156. Ж. В. Головенько, С. Л. Гафнер, и Ю. Я. Гафнер. “Исследование структурных состояний нанокластеров золота методом молекулярной динамики”, *Известия ВУЗов. Физика*, т. 51, №11/3, с. 186–190, 2008.

157. Ph.Buffat, J.-P. Borei. “Size effect on the melting temperature of gold particles”, *Phys.Rev.*, v. 13, p.2287–2298, 1976.

158. В. М. Самсонов, и др. “Молекулярнодинамические исследования плавления и кристаллизации наночастиц”, *Кристаллография*, т. 54, №3, с. 530–536, 2009.

159. S. Lai. *Phys.Rev.Lett.,* 77, 99, 1996.

160. В. П. Коверда, В. Н. Скоков, и В. П. Скрипов. *ФММ*, 51, с. 238, 1981.

161. К. Ю. Богданов. *Что могут нанотехнологии*, М., 2008.

162. К. Богданов. Сайт Богданова про нанотехнологии. [Электронный ресурс]. Доступно: http://nanoeducation.ucoz.ru/0485234_60713_bogdanov.

163. Ю. Ф. Зуев. "Динамическая структура и механизмы каталитического действия микрогетерогенных систем на основе поверхностно-активных веществ", автореф. дисс. д. х. н., Казань, 2006.

164. Д. А. Файзуллин, Т. А. Коннова, Т. Эртле, и Ю. Ф. Зуев. "Самоассоциация и вторичная структура бета-казеина", на VI Российском симпозиуме *Белки и пептиды* , Москва, с. 11–15, 2013.

165. И. Пригожин, и И. Стенгерс. *Время, хаос, квант. К решению парадокса времени*, М., УРСС, 2003.

166. *J.* Calhoun. *Environment and Population: Problems and Adaptation: An Experimental Book Integrating Statements by 162 Contributors*, Praeger, 1983.

167. Г. Рейнгольд. *Умная толпа: новая социальная революция*, ФАИР-ПРЕСС, 2006.

168. И. И. Белгородов. "Перенаселение или грядущее вымирание? Мировые демографические тенденции", на *XVIII Азиатско-Тихоокеанском конгрессе*, Астана, Казахстан, 2011.

169. М. Ф. Иванов, А. Д. Каверин, Б. А. Клумов, и В. Е. Фортов. "От горения и детонации к окислам азота", *УФН*, т. 184, №3, с. 248–264, 2014.

170. R.I.M. Dunbar. "Coevolution of neocortical size, group size and language in humans", *Behavioral and Brain Sciences*, №16(4), p. 681–735, 1993.

171. [Электронный ресурс]. Доступно: http://scienceoftheinvisible.blogspot.ru/2007/10/dunbars-number.html

172. [Электронный ресурс]. Доступно: http://scisne.net/a-931.

173. [Электронный ресурс]. Доступно: http://www.nwsem.com/

174. [Электронный ресурс]. Доступно: https://grabberz.com/showthread.php?p=346576

175. [Электронный ресурс]. Доступно: http://youarenotsosmart.ru/2012/05/dunbars-number/

176. А. Фет. *Инстинкт и социальное поведение*, Rehoboth, New Mexico, USA, 2015.

177. С. П. Капица. *Очерк теории роста человечества демографическая революция и информационное общество*, М.: РАН, 2008.

178. С. П. Капица, С. П. Курдюмов, и Г. Г. Малинецкий. *Синергетика и прогнозы будущего,* Наука, Москва, 1997.

179. С. П. Капица. *Общая теория роста человечества*, Наука, Москва, 1999.

180. S. P. Kapitza. *Global Population Blow up and After. The demographic revolution and information society. A Report to the Club of Rome,* Global Marshall Plan Initiative, Hamburg; Moscow, 2007.

181. С. П. Капица. *Сколько людей жило, живет и будет жить на земле. Очерк теории роста человечества*, Москва 1999.

182. С. П. Капица, "Математическая модель роста населения мира", *Математическое моделирование*, т. 4, N6, 1992.

183. С. П. Капица, "Феноменологическая теория роста населения Земли", *Успехи физ. наук*, т. 166, N1, 1996.

184. В. Майер-Шенбергер, *Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим*, М. : Манн, Иванов и Фербер, 2014.

185. [Электронный ресурс]. Доступно:http://habrahabr.ru/flovs/develop/

186. [Электронный ресурс]. Доступно: https://cloud.google.com/products/big-data

187. Дж. Брайант, и С. Томпсон, *Основы воздействия СМИ*, М.: Издательский дом "Вильямс", 2004.

188. Вильям Л. Саймон, и Кевин Митник. *Искусство обмана,* Компания АйТи, 2004.

189. В. Н. Дружинин, *Экспериментальная психология*, СПб: Питер, 2000.

190. Е. Н. Князева, и С. П. Курдюмов, "Синергетика как новое мировоззрение", *Вопросы философии*, №12, 1992.

191. І. Г. Грабар, "Термоактиваційний аналіз і синергетика руйнування", Житомир, 2002.

192. І. Г. Грабар, "Прискорене прогнозування ресурсу конструкцій на стадії проектування та універсальна діаграма проф. Грабара", *Вісник ЖНАЕУ*, № 2(44), т. 4, ч. 2, 2014.

193. Л. М. Бойко, І. Г. Грабар, и С. М. Кульман, *Довговічність стружкових плит у конструкціях меблів*, Київ, 2013.

194. І. Г. Грабар, "Моделювання висоти і структури хаосу" на VII Всеукр. наук.-практ. конф., Полтава, 2016.

195. A. A. Shanyavskiy, T. P. Zakharova, and Yu. A. Potapenko, "Bifurcation transition from the meso- to nanocosm of fatigue of titanium alloy VT3-1 as a partially closed sysyem", *Физическая мезомеханика,* 12, 3, с. 33-44, 2009.

196. С. Н. Журков, "Проблема прочности твердых тел", *Вестн. АН СССР*, N11, с. 78, 1957.

197. В. Р. Регель, А. И. Слуцкер, и Э. Е. Томашевский, *Кинетическая природа прочности твердых тел*, М.: Наука, 1974.

198. Valery V. Gritsak-Groener, *A Theory of Finite Chaotic*, SLU, 1997.

199. В. К. Григорович, *Металлическая связь и структура металлов*, М.: Наука, 1988.

200. *Диаграммы состояния двойных металлических систем*, М.: Машиностроение, 1996–2000.

201. [Электронный ресурс]. Доступно: http://www.sifferkoll.se/sifferkoll/wp-content/uploads/2014/10/LuganoReportSubmit.pdf

202. [Электронный ресурс]. Доступно: http://www.whatisnuclear.com/physics/energy_density_of_nuclear.html.

203. Г. С. Ивасышин, "Научные открытия в микро- и нанотрибологии", *Трение и смазка в машинах и механизмах,* 4, с.24-27, 2008.

204. С. Глесстон, К. Лейдлер, и Г. Эйринг, *Теория абсолютных скоростей реакций*, М.: Изд-во иностр.лит., 1948.

205. С. Н. Журков, "К вопросу о физической основе прочности", *ФТТ*, Т. 22, N11, с. 3344, 1980.

206. В. И. Бетехтин. "Долговечность и структура кристаллических тел" в *Проблемы прочности и пластичности твердых тел*, Л.: Наука. Ленингр. отд-ние., с. 155, 1979.

207. Петров А.И., и В. И. Бетехтин, "Временные закономерности разрушения металлов при растяжении в условиях гидростатического давления", *Физика металлов и металловедение*, т. 34, N1, с. 39, 1972.

208. Ф. Горофало, *Законы ползучести и длительной прочности металлов*, М.: Металлургия, 1968.

209. А. Убеллоде, *Плавление и кристаллическая структура*, М.: Мир, 1969.

210. С. Н. Журков, В. И. Бетехтин, и А. И. Слуцкер, "Временная зависимость прочности двухфазных сплавов на основе алюминия", *Физика металлов и металловедение*, т. 17, N4, с. 564, 1964.

211. И. Г. Грабар, "Термоактивационный анализ разрушения ОЦК и ГЦК металлов", *Изв. АН СССР. Металлы*, N3, с. 119, 1989.

212. А. Г. Додонов, Д. В. Ландэ, В. В. Прищепа, та ін. *Конкурентная разведка в компьютерных сетях*, К. : ИПРИ НАН Украины, 2013.

213. В. Л. Рябічев, і А. О. Баклан, "Моблогінг як один із різновидів соціальних медіа", *Наукові записки Інституту журналістики*, т. 50, с. 159–161, 2013.

214. Р. В. Грищук, і Ю. Г. Даник, "Синергія інформаційних та кібернетичних дій", *Труди університету*, № 6 (127), с. 132–143, 2014.

215. C. Welt, "After the Color Revolutions: Political Change and Democracy Promotion in Eurasia". [Electronic resource]. Access: https://www.gwu.edu/~ieresgwu/assets/docs/PONARS_Eurasia_After_the_Color_Revolutions.pdf.

216. О. В. Матвєєва, "Віртуальні спільноти в контексті національної та міжнародної безпеки", *Вісник Маріупольського державного університету*, №6, с. 85–93, 2013.

217. К. О. Споришев, В. П. Грищенко, Є. Г. Башкатов, та ін. "Протидія мобільним засобам організації та координації масових безладь", *Честь і закон*, № 47, с. 66–67, 2013.

218. Верник А. Г. "Социальная сеть YouTube как площадка для продвижения и монетизации контента мировых телеканалов", дис. канд. филос. наук, Челябинск, 2015.

219. П. Пишнамази, "Проблемы становления интернет-коммуникации в современном Иране", *Вестник РУДН*, № 3, с. 71–78, 2012.

220. Y. Theocharis, W. Lowe, J. W.van Deth, and G. García-Albacete, "Using Twitter to mobilize protest action: online mobilization patterns and action repertoires in the Occupy Wall Street, Indignados and Aganaktismenoi movements", *Information, Communication & Society*, №18(2), p. 202–220, 2015.

221. "Protest apps bring hi-tech flair to Thai rallies". [Electronic resource]. Available from: http://www.todayonline.com/tech/protest-apps-bring-hi-tech-flair-thai-rallies?singlepage=true.

222. Мобильная рация. [Электронный ресурс]. Режим доступа : http://zello.com.

223. И. Н. Панарин, *Информационная война и мировая политика*, М., 2006.

224. И. Н. Панарин, *СМИ, пропаганда и информационные войны*, М.: Поколение, 2012.

225. *Информационные войны в интернете*. [Електронний ресурс]. Доступно: http://emirr.ru/emirr_articles/232-informacionnye-vojny-v-internete.html

226. М.Григорьев, "Методы ведения информационных войн" – *Блог*. [Електронний ресурс]. Доступно: http://mcpt.narod.ru/pr_war.html#up

227. "Спосіб поширення інформації та запобігання поширення інформації в комп'ютерній мережі". [Електронний ресурс]. Доступно: http://findpatent.com.ua/patent/240/2408145.html

228. С. А. Зелинский, *Информационно-психологическое воздействие на массовое сознание. Средства массовой коммуникации, информации и пропаганды – как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс*, СПб.: СКИФИЯ, 2008.

229. Н. Н. Быченок, *Информационная безопасность государства в военной сфере : науч.-метод. Издание*, К. : НУОУ, 2012.

230. J. Xie, S. Sreenivasan, G.Korniss et al., "Social consensus through the influence of committed minorities", *Phys Rev E.*, vol. 84, No.1, P. 1–9, 2011.

231. "Агентство интернет маркетинга, услуги рекламы и PR в социальных сетях от компании Ingate". [Электронный ресурс]. Доступно: http://smm.ingate.ru/company.

232. "Магазин маркетинговых услуг в социальных сетях". [Электронный ресурс]. Доступно: http://www.market-smm.ru/main.html.

233. W. Wiersma, "Critical Mass in Collaborative Hypertext Environments". [Online]. Access: http://wybowiersma.net/pub/essays/Wiersma,Wybo,Critical_mass_in_collaborative_hypetext_environments.pdf.

234. "Как правильно раскручивать группу". [Электронный ресурс]. Доступно: http://putliker.com/blog/?id=3&razd=2.

235. А. Завялов, "Путь от 0 до критической массы пользователей в стартапах : как набрать критическую массу пользователей и не провалиться?". [Электронный ресурс]. Доступно: https://medium.com/@azavyalov/0-d563fd2f2bab.

236. Г. А. Остапенко, и др. *Информационные риски в социальных сетях*, Ред. Д. А. Новикова, Воронеж : ВГТУ, 2013.

237. P. J. Carrington, J. Scott, and S. Wasserman, *Models and Methods in Social Network Analysis*, New York: Cambridge University Press, 2005.

238. Д. Брайан, и Т. Сузан, *Основы воздействия СМИ*, М.: Изд. дом "Вильяме", 2004.

239. Ч. Лэм, *Hadoop в действии*, М.: ДМК Пресс, 2012.

240. А. Н. Тихонов, и В. Я. Арсенин, *Методы решения некорректных задач*, М. : Наука, 1986.

241. Э. Найман, "Расчет показателей Херста с целью выявления трендовости (персистентности) финансовых рынков и макроэкономических индикаторов", *Економіст*, №10, с. 18–28, 2009.

242. "R/S - анализ стабильности запаздывающего временного ряда". [Электронный ресурс]. Доступно: http://labfranep.com/r-s-analiz-stabilnosti-zapazdyvayushchego-vremennogo-ryada.

243. С. А.Зелинский, *Информационно-психологическое воздействие на массовое сознание. Средства массовой коммуникации, информации и пропаганды – как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс*, СПб.: СКИФИЯ, 2008.

244. П. С. Прибутько, та І. Б. Лук'янець, *Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах*, К. : Вид. ПАЛИВОДА А.В., 2007.

245. "ПРИЗМА: Управление репутацией". [Электронный ресурс]. Доступно: http://www.mlg.ru/pdf/prizma.pdf.

246. Танатар Н. В. "Интеллектуальные поисково-аналитические системы мониторинга СМИ", *Библиотеки национальных академий наук: проблемы функционирования, тенденции развития*, вип. 6, с. 205–219, 2008.

247. А. Федорчук, К. Лобузіна, та Н. Танатар, "Створення інформаційних ресурсів на основі моніторингу змісту публікацій ЗМІ", *Бібліотечний вісник*. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/j-pdf/bv_2011_2_4.pdf.

248. А. Г. Остапенко, М. П. Иванкин, и Г. А. Савенков, *Обнаружение и нейтрализация вторжений в распределенных информационных системах*, Воронеж: Воронежский гос. техн. ун-т, 2013.

249. *Обнаружение вторжений в компьютерные сети (сетевые аномалии)*, Ред. О. И. Шелухина, М. : Горячая линия–Телеком, 2013.

250. А. А. Малюк, *Информационная безопасность: концептуальные и методологические основы защиты информации*, М. : Горячая линия–Телеком, 2004.

251. "Computer Attacks: What They Are and How to Defend Against Them". [Електронний ресурс]. Доступно: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=151188.

252. "IBM Internet Security Systems corporate". [Електронний ресурс]. Доступно: http://www-03.ibm.com/security/xforce/resources.html#all.

253. О. Г. Корченко, *Системи захисту інформації: монографія*, К. : НАУ, 2004.

254. В. М. Мамарєв, "Метод побудови класифікатора кібератак на державні інформаційні ресурси", дис. канд. техн. наук, К.: ДУТ, 2015.

255. І. М. Павлов, С. В. Толюпа, та В. І. "Ніщенко Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем", *Сучасний захист інформації*, №4, с. 44–52, 2014.

256. Д. Ю. Гамаюнов, "Обнаружение компьютерных атак на основе анализа поведения сетевых объектов", дис. канд. физ.-мат. наук, М., 2007.

257. "The Bro Network Security Monitor". [Електронний ресурс]. Доступно: www.bro.org.

258. "Open Source Host-based Intrusion Detection System". [Електронний ресурс]. Доступно: http://www.ossec.net.

259. "NSTAT: A Model-based Real-time Network Intrusion Detection System". [Електронний ресурс]. Доступно: http://www.cs.ucsb.edu/research/tech-reports/1997-18.

260. "Prelude Universal Open-Source SIEM project". [Електронний ресурс]. Доступно: https://www.prelude-siem.org.

261. *Snort community*. [Електронний ресурс]. Доступно: www.snort.org.

262. *Autonomous agents for Intrusion Detection*. [Електронний ресурс]. Доступно: http://www.cs.perdue.edu/coast/project/autonomous-agents.html.

263. *Офіційний сайт McAfee for Consumer and Business*. [Електронний ресурс]. Доступно: http://www.mcafee.com.

264. *Офіційний сайт ACA Pacific*. [Електронний ресурс]. Доступно: www.acapacific.com.au.

265. *Офіційний сайт Juniper Networks*. [Електронний ресурс]. Доступно: http://www.juniper.net.

266. *Офіційний сайт CA Technologies*. [Електронний ресурс]. Доступно: http://www.ca.com.

267. D. Sáncheza, M. A. Vilaa, L. Cerdaa, and J. M. "Serranob Association rules applied to credit card fraud detection", *Expert Systems with Applications: An International Journal*, vol. 36, iss. 2, part 2, p. 3630–3640, 2009.

268. S. Y. Wua, and E. Y. Expert. "Data mining – based intrusion detectors", *Systems with Applications: An International Journal*, vol. 36, iss. 3, part 1, p. 5605–5612, 2009.

269. В. Сазанов, "Социальные сети: Анализ – Технологии – Перспективы. Обзор", *Сайт Лаборатории СВМ*. [Электронный ресурс]. Доступно: http://ntl-cbm.narod.ru/CBM-NET/net_rew.doc.

270. В. В. Мазуренко, та С. Д. Штовба, "Огляд моделей аналізу соціальних мереж", *Вісник Вінницького політехнічного інституту*, № 2, с. 62–74, 2015.

271. В. М. Томашевський, "Щодо моделювання соціальних мереж", на *Міжнар. наук.-практ. конф. Математичне та імітаційне моделювання систем*, Чернігів, 2013, с. 448–450.

272. А. М. Грушецький, "Агентне моделювання: основні ідеї і перспективи", *Наукові записки НаУКМА. Соціологічні науки*, т. 161, с. 21–27, 2014.

273. J. W. Forrester, *World Dynamics*, Portland, Oregon: Productivity Press, 1970.

274. M. Myrtveit, *The world model controversy*, The System Dynamics Group. Department of Geography: University of Bergen.

275. S. P. Borgatti, and M. G. Everett, "Notions of Position in Social Network Analysis", *Sociological Methodology*, vol. 22, pp. 1–35, 1992.

276. R. S. Burt, "Some properties of structural equivalence measures derived from sociometric choice data", *Social Networks*, vol. 10, pp. 1–28, 1988.

277. H. C. White, A. S. Boorman, and R. L. Breiger, “Social structure from multiple networks. I. Blockmodels of roles and positions”, *American journal of sociology*, vol. 81, no. 4, pp. 730–780, 1976.

278. В. В. Бреер, “Стохастические модели социальных сетей”, *Управление большими системами*, № 27, с. 169–204, 2009.

279. A. Reka, “Statistical mechanics of complex networks”, *Reviews of Modern Physics*, no. 74, pp. 47–97, 2002.

280. L.-A. Barabasi, and A. Reka, “Emergence of scaling in random networks”, *Science*, 286 (5439), pp. 509–512, 1999.

281. Д. А. Губанов, Д. А. Новиков, и А. Г. Чхартишвили, “Модели информационного влияния и информационного управления в социальных сетях”, *Проблемы управления*, № 5, с. 28–35, 2009.

282. Д. А. Губанов, и Д. А. Новиков, “Модели распределенного контроля в социальных сетях”, *Системы управления и информационные технологии*, № 3.1(37), с. 124–129, 2009.

283. А. А. Шиян, *Моделі та методи інформаційної безпеки особи, соціальної групи, соціальної мережі та суспільства*. SSRN Electronic Journal, 2017. [Електронний ресурс]. Доступно: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078168. Дата звернення: Лист. 07, 2017.

284. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, та С. В. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект*, Київ: ДУТ, 2015.

285. C. Barrett, S. Eubank, and M. Marathe, “Modeling and simulation of large biological, information and socio-technical systems: an interaction based approach”, in *Interactive Computation*, Berlin: Springer Berlin Heidelberg, 2006, pp. 353–392.

286. К. В. Молодецька-Гринчук, “Адаптація методів теорії динамічного хаосу для забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах”, *Вісник Житомирського національного агроекологічного ун-ту*, № 2(61), т. 1, с. 180–187, 2017.

287. В. П. Горбулін, О. Г. Додонов, та Д. В. Ланде, *Інформаційні операції та безпека суспільства: загрози, протидія, моделювання*, К.: Інтертехнологія, 2009.

288. Л. Г. Раскин, *Анализ сложных систем и элементы теории оптимального управления*, М.: Сов. радио, 1976.

289. R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, New York: Addison-Wesley Publ. Co., 1993.

290. А. Лоскутов, *Математические основы хаотических динамических систем*. [Электронный ресурс]. Доступно: http://chaos.phys.msu.ru/loskutov/PDF/Lectures_math_found_of_chaot_dyn_syst.pdf. Дата обращения: Ноя. 10, 2017.

291. М. Є. Рогоза, С. К. Рамазанов, та Е. К. Мусаєва, *Нелінійні моделі та аналіз складних систем*, Полтава: РВВ ПУЕТ, 2011.

292. J.-M. Ginoux, *Differential Geometry Applied to Dynamical Systems*, World Scientific, 2009.

293. А. Ю. Лоскутов, и А. С. Михайлов, *Основы теории сложных систем*, Москва–Ижевск: РХД, 2007.

294. Ф. Хартман, *Обыкновенные дифференциальные уравнения*, М.: Мир, 1970.

295. В. Р. Андриевский, и А. Т. Фрадков, “Управление хаосом: методы и приложения. Ч. I: Методы”, *Автоматика и телемеханика*, № 5, с. 3–45, 2003.

296. Дж. Николис, *Динамика иерархических систем. Эволюционное представление*, М.: Мир, 1989.

297. М. Месарович, Д. Мако, и И. Тахакара, *Теория иерархических многоуровневых систем*, М.: Мир, 1973.

298. М. Табор, *Хаос и интегрируемость в нелинейной динамике*, М.: Эдиториал УРСС, 2001.

299. В. Б. Русин, “Моделювання методів управління динамічним хаосом та їх практичне застосування”, дис. канд. наук., Нац. ун-т “Львівська політехніка”, Львів, 2017.

300. Э. И. Владимирский, и Б. И. Исмайлов, *Синергетические методы управления хаотическими системами*, Баку: ELM, 2011.

301. E. Zeraoulia, *Models and Applications of Chaos Theory in Modern Sciences*, Taylor&Francis, 2012.

302. X. H. Yu, “Controlling chaos using input-output linearization approach”, *International Journal Bifurcation Chaos*, v. 7, pp. 1659–1664, 1997.

303. E. Ott, C. Grebogi, and J. Yorke, "Controlling chaos", *Physical Review Letters*, v. 64(11), pp. 1196–1199, 1990.

304. А. Л. Фрадков, "Адаптивное управление нелинейными колебаниями", на *Междунар. конф. Алгоритмическое обеспечение процессов управления в механике и машиностроении*, Москва, 1994, с. 29–30.

305. O. Umut, "Controlling chaos in nuclear spin generator system using backstepping design", *Applied Sciences*, vol. 11, pp. 151–160, 2009.

306. И. В. Мирошник, В. О. Никифоров, и А. Л. Фрадков, *Нелинейное и адаптивное управление сложными динамическими системами*, СПб: Наука, 2000.

307. Y. Onozaka, and M. Nakagawa, "Back propagation learning with periodic chaos neurons", *Electronics and communications in Japan* (*Part III: Fundamental Electronic Science*), vol. 86, no. 3, pp. 11–19, 2003.

308. K. Y. Lian, P. Liu, and C. S. Chiu, "Fuzzy Chaotic Synchronization and Communication – Signal Masking and Encryption", in *Soft Computing in Communications. Studies in Fuzziness and Soft Computing*, Berlin Heidelberg: Springer, 2004, vol. 136, pp. 269–291.

309. I. F. Chung, C. J. Lin, and C. T. Lin, "A GA-based fuzzy adaptive learning control network", *Fuzzy sets and systems*, vol. 112, no. 1, pp. 65–84, 2000.

310. А. А. Колесников, *Синергетическая теория управления*, М.: Энергоатомиздат, 1994.

311. А. А. Колесников, *Синергетическое методы управления сложными системами: теория системного синтеза*, М.: Едиторал УРСС, 2005.

312. А. Г. Додонов, Д. В. Ландэ, и В. Г. Путятин, *Компьютерные сети и аналитические исследования*, К.: ИПРИ НАН Украины, 2014.

313. Е. М. Роджерс, *Дифузія інновацій*, Вид. дім "Києво-Могилянська академія", 2009.

314. M. Castells, and G. Cardoso, *The Network Society: From Knowledge to Policy*, Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005.

315. Р. В. Грищук, та В. В. Охрімчук, "Соціальні мережі як арена інформаційного протиборства", на *XX Всеукр. наук.-практ. конф. Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення*, Житомир, 2014, с. 168–169.

316. J. M. Epstein, *Generative Social Science: Studies in Agent-Based Computational Modeling*, Princeton: Princeton University Press, 2012.

317. И. Пригожин, и И. Стенгерс, *Порядок из хаоса: Новый диалог человека с природой*, В. И. Аршинова, Ю. Л. Климонтовича, и Ю. В. Сачкова, Общ. ред. М.: Наука, 1984.

318. Ю. В. Талагаев, и А. Ф. Тараканов, "Многопараметрический анализ на основе критерия Мельникова и оптимальное подавление хаоса в периодически возмущаемых динамически системах", *Известия высших учебных заведений. Прикладная нелинейная динамика*, т. 19, № 4, с. 77–90, 2011.

319. J. M. Epstein, *Nonlinear Dynamics, Mathematical Biology, and Social Science*, Massachusetts: Addison-Wesley Publishing Company, 1997.

320. Ю. О. Бєлов, А. С. Бичков, та О. І. Чулічков, *Математичні моделі, методи й алгоритми теоретичної та прикладної інформатики*, К.: "ФПФН", 2009.

321. Ю. Г. Даник, та Р. В. Грищук, "Синергетичні ефекти в площині інформаційного та кібернетичного протиборства", на *Наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2015, с. 235–237.

322. А. В. Сериков, "Эффективность хозяйственной деятельности: определение, измерение, синергетическое управление", *Економічний вісник Донбасу*, № 2(24), с. 212–219, 2011.

323. Е. С. Нестругина, Е. Ю. Ларина, и Н. И. Чичикало, "Концепция эволюции синтеза мультиагентной информационно-измерительной системы процесса реабилитации человека после травматизма", *Восточно-Европейский журнал передовых технологий*, № 2/10(62), с. 49–55, 2013.

324. Р. В. Грищук, та К. В. Молодецька, "Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах", *Безпека інформації*, т. 21, № 2, с. 123–130, 2015.

325. R. Hryshchuk, and K. Molodetska, "Synergetic Control of Social Networking Services Actors' Interactions", in *Recent Advances in Systems, Control and Information Technology. SCIT 2016. Advances in Intelligent Systems and Computing*, R. Szewczyk and M. Kaliczynska, Eds. Cham, Switzerland: Springer, 2017, vol. 543, pp. 34–42.

326. Р. В. Грищук, та К. В. Молодецька, “Синергетичний підхід до управління параметрами взаємодії агентів у соціальних інтернет-сервісах”, на *XII Міжнар. наук.-тех. конф. АВІА–2015*, Київ, 2015, с. 2.46–2.49.

327. Р. В. Грищук, “Концепція побудови диференціально-ігрових гарантовано захищених розподілених систем захисту інформації”, *Сучасний захист інформації*, № 1(6), с. 4–9, 2011.

328. К. В. Молодецька, “Методика вибору атрактора для управління динамікою процесів взаємодії акторів у соціальних інтернет-сервісах”, *Інформаційна безпека*, № 3(15), 4(16), с. 146–151, 2014.

329. К. В. Молодецька, “Спосіб вибору параметра порядку в задачах управління взаємодією акторів у соціальних інтернет-сервісах”, на *IV Міжнар. наук.-техн. конф. Актуальні задачі сучасних технологій*, Тернопіль, 2015, т. 2, с. 35–36.

330. К. В. Молодецька, “Вибір атрактора для синергетичного управління взаємодією акторів у соціальних інтернет-сервісах”, на *XXI Всеукр. наук.-практ. конф. Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення з урахуванням досвіду антитерористичної операції*, Житомир, 2016, с. 134–135.

331. А. В. Сєріков, та О. О. Зубова, “Маркетинг як необхідна умова синергетичного управління господарською діяльністю”, *Актуальні проблеми економіки*, № 5, с. 276–283, 2010.

332. Р. В. Грищук, “Диференціально-ігрові моделі та методи моделювання процесів кібернападу”, дис. д-ра техн. наук, Нац. авіац. ун-т, Київ, 2013.

333. Р. В. Грищук, та С. В. Чернишук, “Методика оцінювання рівня небезпеки кібернетичних загроз”, *Сучасний захист інформації*, спецвипуск, с. 23–28, 2013.

334. Р. В. Грищук, та К. В. Молодецька, “Спосіб синергетичного управління поведінкою акторів у соціальних інтернет-сервісах”, *Системи управління, навігації та зв’язку*, № 1(37), с. 66–70, 2016.

335. К. В. Молодецкая, “Модели аттракторов для синергетического управления взаимодействием акторов социальных интернет-сервисов”, в *Информационные технологии в управлении, образовании, науке и промышленности: монография*, В. С. Пономаренко, Ред. Харків, Україна: Рожко С. Г., 2016, с. 329–342.

336. S. Wasserman, and K. Faust, *Social network analysis: Methods and applications*, Cambridge: Cambridge university press, 1994.

337. К. В. Молодецька, “Управління попитом агентів на контент у соціальних інтернет-сервісах”, на *Міжнар. наук.-практ. інтернет-конф. молодих учених та студ. Актуальні проблеми автоматизації та управління*, Луцьк, 2015, вип. 3, с. 56–62.

338. Б. Я. Вахула, “Соціальні інтернет-мережі, їхні функції та роль у формуванні громадянського суспільства”, *Вісн. Львівського ун-ту*, вип. 6, с. 311–319, 2012.

339. Б. С. Калитин, *Качественная теория устойчивости движения динамических систем*, Мн.: БГУ, 2002.

340. К. В. Молодецька, “Синтез синергетичного управління попитом агентів на контент у соціальних інтернет-сервісах”, *Інформатика та математичні методи в моделюванні*, т. 5, № 4, с. 330–338, 2015.

341. К. В. Молодецька, “Прогнозування синергетичних ефектів взаємодії агентів у соціальних інтернет-сервісах”, на *Міжнар. наук.-практ. конф. Інформаційні технології, економіка та право: стан та перспективи розвитку*, Чернівці, 2015, с. 171–173.

342. К. В. Молодецька, “Спосіб підтримання заданого рівня попиту акторів соціальних інтернет-сервісів на контент”, *Радіоелектроніка, інформатика, управління*, № 4(35), с. 113–117, 2015.

343. А. М. Пелещишин, Ю. О. Сєров, О. Л. Березко, О. П. Пелещишин, О. Ю. Тимовчак-Максимець, та О. В. Марковець, *Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія*, Л.: Вид-во Львівської політехніки, 2012.

344. Р. В. Грищук, “Стартап віртуальних спільнот у соціальних мережах за принципом критичної маси”, *Захист інформації*, спец. вип., с. 19–25, 2015.

345. A. Tatnall, *Actor-Network Theory and Technology Innovation: Advancements and New Concepts. Information Science Reference*, New York, 2010.

346. К. В. Молодецька, “Підвищення інформаційної стійкості акторів соціальних інтернет-сервісів до контенту деструктивного змісту”, на *V Міжнар. наук.-практ. конф. Інфокомунікації – сучасність та майбутнє*, Одеса, 2015, ч. 3, с. 121–123.

347. K. Molodetska, "How to build up social networking service actors' tolerance for harmful content", на *II Міжнар. наук.-практ. конф. Інформаційні технології та взаємодії*, Київ, 2015, с. 166–167.

348. К. Молодецкая, "Валидация синергетического управления взаимодействием акторов в социальных интернет-сервисах", *Computer Science and Telecommunications: electronic journal*, № 2, pp. 18–26, 2016. [Электронный ресурс]. Доступно: http://gesj.networking-academy.org.ge/download.php?id=2735.pdf. Дата доступа: Дек. 30, 2017.

349. К. В. Молодецька, "Дослідження моделей синергетичного управління взаємодією акторів соціальних інтернет-сервісів", на *Наук.-техн. конф. Інформатика, математика, автоматика: ІМА–2016*, Суми, 2016, с. 129.

350. К. В. Молодецька, "Акредитація моделі синергетичного управління взаємодією акторів у соціальних інтернет-сервісах", на *Наук.-практ. конф. Проблеми та перспективи розвитку ІТ-індустрії*, Харків, 2016, с. 44.

351. В. М. Томашевський, *Моделювання систем*, Київ: Видавнича група BHV, 2005.

352. R. G. Sargent, "A New Statistical Procedure for Validation of Simulation and Stochastic Models", Department of Electrical Engineering and Computer Science, New York, Tech. Rep. SYR-EECS-2010-06, 2010.

353. О. В. Коваль, "Верифікація комп'ютерної моделі системи інформаційного управління", *Вісн. Нац. техн. ун-ту України "КПІ". Інформатика, управління та обчислювальна техніка*, № 61, с. 45–48, 2014.

354. D. A. Maevsky, E. J. Maevskaya, O. P. Jekov, and L. N. Shapa, "Verification of the software reliability models", *Reliability: theory & applications*, vol. 9, no. 3(34), pp. 14–23, 2014.

355. Р. В. Грищук, "Верифікація і дослідження спектральних P- та гібридних P-L-моделей процесу нападу на інформацію", *Вісн. ЖДТУ*, № II(49), с. 69–76, 2009.

356. "Ложь: распятие в эфире первого канала". *Stopfake.org*, 2014. [Электронный ресурс]. Доступно: https://www.stopfake.org/lozh-raspyatie-v-efire-pervogo-kanala/. Дата доступа: Дек. 30, 2017.

357. Р. В. Грищук, та К. В. Молодецька, "Спосіб синергетичного управління поведінкою акторів у соціальних інтернет-сервісах", *Системи управління, навігації та зв'язку*, № 1(37), с. 66–70, 2016.

358. "Берлін закликає Москву припинити пропаганду навколо "зґвалтованої мігрантами російської дівчини". *Euronews*, 2016. [Электронный ресурс]. Доступно: http://ua.euronews.com/2016/01/27/germany-warns-russia-against-using-teen-rape-case-as-propaganda. Дата доступа: Дек. 30, 2017.

359. О. В. Іванов, "Класичний контент-аналіз та аналіз тексту: термінологічні та методологічні відмінності", *Вісн. Харк. нац. ун-ту ім. В. Н. Каразіна. Сер. "Соціологічні дослідження сучасного суспільства: методологія, теорія, методи"*, № 1045, с. 69–74, 2013.

360. В. А. Хорошко, и М. Е. Шелест, *Информационно-аналитическое обеспечение безопасности*, К.: ВПВ "Задруга", 2016.

361. О. М. Колодчак, "Інтелектуальний аналіз даних", *Вісн. Нац. ун-ту "Львівська політехніка". Комп'ютерні системи та мережі*, № 773, с. 49–58, 2013.

362. Ф. Барсегян, М. Куприянов, В. Степаненко, и И. Холод, *Методы и модели анализа данных OLAP и DataMining*, СПб.: БХВ-Петербург, 2008.

363. С. Н. Голубев, "R/S-анализ стабильности запаздывающего временного ряда", *Лаборатория фрактального анализа, экологии, программирования*. [Электронный ресурс]. Доступно: http://labfranep.com/r-s-analiz-stabilnosti-zapazdyvayushchego-vremennogo-ryada. Дата обращения: Ноя. 30, 2017.

364. Р. М. Кроновер, *Фракталы и хаос в динамических системах. Основы теории*, М.: Постмаркет, 2000.

365. О. Ф. Гіда, "Соціальні мережі як засіб деструктивних впливів через інформаційний простір", *Боротьба з організованою злочинністю і корупцією (теорія і практика)*, № 3(31), с. 268–278, 2013.

366. Д. Халилов, *Маркетинг в социальных сетях*, М.: Манн, Иванов и Фербер, 2014.

367. П. Алексийчук, "Система слежки PRISM собирала персональные данные через лидеров IT-индустрии", *Проект WebScience.ru*. [Электронный ресурс]. Доступно: http://webscience.ru/news/sistema-slezhki-prism-sobirala-personalnye-dannye-cherez-liderov-it-industrii. Дата обращения: Ноя. 30, 2017.

368. Р. В. Грищук, та К. В. Молодецька, “Метод прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах”, *Системи управління, навігації та зв'язку*, № 4(36), с. 60–65, 2015.

369. Ю. Б. Бродський, та К. В. Молодецька, *Інформатика і системологія*, Житомир: ЖНАЕУ, 2014.

370. B. Toth, “Estonia Under Cyber Attack”. [Electronic resource]. Access: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

371. E. Tikk, K. Kaska, K. Rünnimeri et. al. *Cyber Attacks Against Georgia: Legal Lessons Identified*. [Electronic resource]. Access: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

372. *The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict.* [Electronic resource]. Access: http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

373. L. Milevski, “Stuxnet and Strategy: A Special Operation in Cyberspace?”. [Electronic resource]. Access: http://www.academia.edu/872101/Stuxnet_and_Strategy_-_A_Special_Operation _in_Cyberspace.

374. C. Welt, *After the Color Revolutions: Political Change and Democracy Promotion in Eurasia.* [Electronic resource]. Access: https://www.gwu.edu/~ieresgwu/assets/docs/PONARS_Eurasia_After_the_Color_Revolutions.pdf

375. Ураження шкідливими програмами регіонів України. [Електронний ресурс]. Доступно: http://cert.gov.ua/?p=1310.

376. *Snake Campaign & Cyber Espionage Toolkit : BAE Systems Applied Intelligence: Snake Rootkit Report, 2014*. [Electronic resource]. Access: http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf.

377. *Uroburos: Highly Complex Espionage Software With Russian Roots. G Data Discovers Alleged Intelligence Agency Software*. [Electronic resource]. Access: https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf.

378. Ю. Г. Даник, *Основні аспекти парадигми кібернетичної безпеки*. [Електронний ресурс]. Доступно: http://jrnl.nau.edu.ua/index.php/IMV/article/view/3171.

379. Р. В. Грищук, “Атаки на інформацію в інформаційно-комунікаційних системах”, *Сучасна спеціальна техніка*, К.: ДНДІ МВС України, №1(24), с. 61–66, 2011.

380. П. С. Прибутько, та І. Б. Лук’янець, *Інформаційні впливи: роль у суспільстві та сучасних военних конфліктах*, К. : Вид. ПАЛИВОДА А.В., 2007.

381. C. W. Stephen, *Revealed: Air Force ordered software to manage army of fake virtual people*. [Electronic resource]. – Access: http://www.rawstory.com/rs/2011/02/18/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people.

382. “Служба внешней разведки России создает ботов для социальных сетей за 30 млн. рублей”. [Электронный ресурс]. Доступно: http://habrahabr.ru/post/150269.

383. Ю. Г. Даник, Ю. І. Катков, та М. Ф. Пічугін, *Національна безпека: запобігання критичним ситуаціям: монографія*, К.: МО України; Житомир: Рута, 2006.

384. *Symantec Corporation Internet Security Threat Report 2014* : Volume 19. [Online]. Access: http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf.

385. *Kaspersky Security Bulletin 2013.* [Online]. Access*:* http://media.kaspersky.com/pdf/KSB_2013_RU.pdf.

Наукове видання

Грабар Іван Григорович,

Грищук Руслан Валентинович,

Молодецька Катерина Валеріївна

Безпекова синергетика:
кібернетичний та інформаційний аспекти

МОНОГРАФІЯ

Редагування *Р. В. Грищук*

Макетування та дизайн обкладинки *К. В. Молодецька*

Підписано до друку 8.02.19 р.
Формат 60х84/16. Гарнітура Bookman Old Style.
Умов.-друк.арк. 16,3.
Наклад 300 прим. Зам № 7

Свідоцтво суб'єкта про державну реєстрацію
ДК № 3402 від 23.02.2009 р.
Житомирський національний агроекологічний університет
10008, м. Житомир, бульвар Старий, 7