DOI:**10.33099/2311-7249/2019-36-3-165-170**

УДК 004.02:004.056

Леонід Михайлович Артюшин *(доктор технічних наук, професор)*[1]
Олександр Васильович Лагодний *(кандидат технічних наук)*[2]

[1]***Державний науково-дослідний інститут авіації, Київ, Україна***
[2]***Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна***

ІНДИКАТОРИ ВИЯВЛЕННЯ НЕГАТИВНОГО ПСИХОЛОГІЧНОГО ВПЛИВУ ПІД ЧАС МОНІТОРИНГУ ЕЛЕКТРОННИХ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Подання спрямованої інформації у вигляді текстових повідомлень дозволяє здійснювати психологічний вплив на визначені цільові аудиторії з метою формування передбачуваних наслідків, в тому числі і корисних противнику. Проаналізовано існуючі підходи до практики моніторингу мережі Інтернет щодо виявлення негативного психологічного впливу та встановлено їх недоліки. У статті запропоновано індикатори виявлення негативного психологічного впливу на особовий склад Збройних Сил України під час моніторингу електронних засобів масової інформації. Система наведених індикаторів дозволяє кількісно оцінювати рівень негативного психологічного впливу під час проведення противником в інтернет-мережі спеціальних дій. Це дає можливість прогнозувати розвиток подій та своєчасно вживати заходи інформаційної протидії. Кількісні показники негативного психологічного впливу в текстових повідомленнях електронних засобів масової інформації дозволяють об'єктивно оцінювати рівень небезпеки визначеній цільовій аудиторії та мінімізувати рівень суб'єктивізму під час моніторингу інтернет-ресурсів. Індикатори поєднують комплексний підхід до виявлення негативного психологічного впливу за рахунок семантичних та статистичних методів. Результати даної роботи можуть бути реалізовані у вигляді модуля спеціалізованого програмного забезпечення в підсистемі виявлення негативного психологічного впливу особовому складу Збройних Сил України.

Ключові слова: *мережа Інтернет; психологічний вплив; індикатори.*

Вступ

Характер сучасних воєн показав істотне зростання значущості такої сфери протиборства, як інформаційна. Нова реальність військових конфліктів та війн сучасності полягає в перенесенні військових дій саме в цю сферу [1]. При цьому інформаційні технології стають, по суті, одним із найперспективніших видів зброї, яка з кожним роком удосконалюється і розширює свої можливості, що призвело до більшого масштабу її застосування. Суттєве збільшення загроз інформаційно-технічного й інформаційно-психологічного впливу (ПсВ) зумовило створення спеціальних підрозділів, які використовують системи виявлення та оцінювання рівня загроз для вжиття адекватних заходів інформаційної протидії [2]. Проте для виявлення таких загроз мають бути розроблені відповідні індикатори (показники), що й спричинило виникнення актуального наукового завдання в даній сфері дослідження.

Постановка проблеми. П'ятий рік збройного конфлікту на сході України з Російською Федерацією (РФ) показує, що противник продовжує застосовувати гібридні дії в інформаційному просторі, у тому числі мережі Інтернет, які відзначаються низкою інформаційно-психологічних акцій проти особового складу Збройних Сил (ЗС) України. Під час інформаційно-психологічних акцій противник вживає заходи щодо дискредитації керівництва ЗС України, погіршення морально-психологічного стану особового складу, який виконує завдання в районі проведення Операції об'єднаних сил тощо. В інформаційному просторі нашої держави поширюються інформаційні приводи у вигляді текстових повідомлень в мережі Інтернет, які своїм змістом спонукають особистість до певних дій [3]. Протидія такому негативному ПсВ є важливою складовою у сфері забезпечення національної безпеки, що визначено Доктриною інформаційної безпеки України [4].

Практика виявлення такого негативного ПсВ показала, що під час моніторингу електронних засобів масової інформації (е-ЗМІ) особовий склад стикається з низкою проблем:

1. Завдання щодо моніторингу мережі Інтернет здійснюється в режимі ручного пошуку, що впливає на якість та ефективність виявлення ПсВ.

2. Спеціалізоване програмне забезпечення (СПЗ), яке дозволяє автоматизувати процес моніторингу (наприклад, Semantic Force), є комерційним і високовартісним. Крім того, воно не адаптоване для виконання специфічних завдань і дозволяє тільки збирати масив даних. При цьому одним із розробників СПЗ є компанія з РФ, яка в

умовах збройної агресії може використовувати його у своїх цілях для збору необхідної розвідувальної інформації.

3. Відсутність єдиної системи індикаторів для спеціальних підрозділів, за якими можливо виявляти негативний ПсВ, що ускладнює процес оцінювання рівня небезпеки особовому складу ЗС України та не дає своєчасно вживати заходи інформаційної протидії.

Аналіз останніх досліджень і публікацій. Завданням організації моніторингу інформаційного простору з метою виявлення негативних інформаційно-психологічних впливів на цільові аудиторії присвячено низку робіт як закордонних, так і вітчизняних дослідників [5–11]. Так, у [5] запропоновано методологічний підхід до створення підсистеми виявлення та оцінювання негативного інформаційно-психологічного впливу, який базується на трирівневій підсистемі моніторингу інформаційного простору. Автори робіт [6–9] пропонують кількісні показники оцінки негативного інформаційно-психологічного впливу під час організації моніторингу мережі Інтернет з метою протидії такому впливу. У публікаціях [10, 11] визначено впливи, які здійснюються РФ на цільові аудиторії, зокрема й України, та запропоновано індекси стійкості до них. Проведений аналіз показав, що на даний час до кінця не сформований єдиний підхід до виявлення та оцінювання негативного ПсВ за встановленою системою індикаторів (показників).

Тому **метою статті є** розроблення індикаторів виявлення негативного ПсВ на визначену цільову аудиторію, які є найбільш вагомими, на наш погляд, під час моніторингу мережі Інтернет.

Виклад основного матеріалу дослідження

Аналіз воєнно-політичної обстановки навколо України та суспільно-політичної в самій країні свідчить про те, що держава з дня своєї незалежності стала об'єктом російської пропаганди та напрямком зосередженого й потужного інформаційно-психологічного впливу [3]. В стані гібридних дій РФ проти України протягом останніх п'яти років актуальним залишається питання забезпечення інформаційної безпеки держави. Пріоритетним напрямком досліджень щодо забезпечення національних інтересів у воєнній сфері є захист особового складу ЗС України від негативного ПсВ РФ, що можливо забезпечити за рахунок створення системи і механізмів протидії спеціальним інформаційним (психологічним) операціям агресора [4].

Спеціальні підрозділи РФ широко використовують мережу Інтернет для поширення негативного інформаційно-психологічного впливу на військово-політичне керівництво держави, особовий склад ЗС України та населення [12]. З метою протидії такому негативному впливу виникає потреба у створенні нових і модернізації існуючих систем виявлення та оцінювання рівня негативного ПсВ на цільові аудиторії.

На сьогодні такі системи переважно базуються на семантичних методах із використанням якісних показників впливу. Оперативне виявлення такого впливу і прогнозування ситуації можуть реалізовуватися за рахунок введення кількісних індикаторів негативного ПсВ та розроблення методики динаміки відслідковування його поширення в мережі Інтернет. Виникає потреба в удосконаленні існуючих систем оперативного виявлення загроз національній безпеці на основі введення необхідних індикаторів негативного ПсВ у процесі моніторингу відкритої інформації глобальної мережі. Впровадження підходу на їх основі дасть змогу розробити відповідне СПЗ, що дозволить автоматизувати даний процес. До індикаторів, які вважатимуться критеріями для виявлення негативного ПсВ на особовий склад ЗС України, належать:

частота публікацій текстового повідомлення з негативним ПсВ за обраною тематикою C_i;

динаміка появи текстового повідомлення з негативним ПсВ за обраною тематикою D_i;

показник важливості е-ЗМІ (PageRang) у пошуковій системі Google $PR_i(A)$;

показник поширеності текстового повідомлення з негативним ПсВ за обраною тематикою M_i;

показник тональності текстового повідомлення $L_{п,н,нт}$.

Частота публікацій текстового повідомлення з негативним ПсВ за обраною тематикою C_i – це співвідношення кількості публікацій текстових повідомлень за досліджуваною тематикою y_i до загальної кількості публікацій $N_{пуб.}$ за усіма тематиками за визначений проміжок часу t_i спостереження в е-ЗМІ:

$$C_i = \frac{\sum_{i=1}^{k} y_i}{N_{пуб.} \cdot \sum_{i=1}^{k} t_i} \cdot 100\%, \qquad (1)$$

де k – дискрети, у які отримані текстові повідомлення.

Динаміка появи текстового повідомлення з негативним ПсВ за обраною тематикою D_i – це розподілення публікацій текстових повідомлень y_i на часовій шкалі Δt:

$$D_i = \frac{\sum_{i=1}^{k} y_i}{\Delta t}, \qquad (2)$$

де Δt – період (доба, тиждень, місяць…).

Показник важливості е-ЗМІ (PageRang) у пошуковій системі Google $PR_i(A)$ – це числова величина, яка визначає авторитетність інтернет-

ресурсу з урахуванням якісної характеристики посилань на них з інших сайтів [13]:

$$PR_i(A) = (1-d) + d\begin{pmatrix} PR(T1)/C(T1) + \dots \\ + PR(T_j)/C(T_j) \end{pmatrix}, \quad (3)$$

де $PR_i(A)$ – це вага PageRang сторінки сайта А, яку необхідно обрахувати;

d – сталий коефіцієнт затухання, який дорівнює 0,85;

$PR(T1)$ – це вага PageRang сторінки, яка вказує на сторінку сайта А;

$C(T1)$ – кількість посилань із цієї сторінки сайта;

$PR(T_j)/C(T_j)$ – обрахунок для кожної сторінки сайтів, які вказують на сторінку сайта А.

Показник поширеності текстового повідомлення з негативним ПсВ за обраною тематикою M_i – це відношення е-ЗМІ q, у яких виявлено текстове повідомлення з негативним ПсВ, до загальної кількості сайтів, які перебувають на моніторингу, Q:

$$M_i = \frac{q}{Q}. \quad (4)$$

Для визначення категорій рівня небезпеки поширеності текстових повідомлень із негативним ПсВ за обраною тематикою наведено трирівневу шкалу оцінювання, яку часто використовують у багатьох сферах сектора національної безпеки і оборони держави [14]. При цьому виділяють такі рівні небезпеки: високий, середній, низький (табл. 1).

Таблиця 1

Якісна шкала небезпеки рівнів поширеності текстових повідомлень із негативним ПсВ

Інтегральна оцінка, M_i	Категорія рівня небезпеки	Якісна характеристика
$0,71 \le M_i \le 1,0$	Високий	Проведення противником психологічної акції
$0,51 \le M_i \le 0,7$	Середній	Поширення противником текстових повідомлень із негативним ПсВ
$0,0 < M_i \le 0,5$	Низький	Розміщення противником текстових повідомлень із негативним ПсВ

На відміну від нормованої фундаментальної шкали, яка передбачає п'ять категорій оцінки, застосування трирівневої шкали забезпечує подання базових усталених рівнів небезпеки та уникання надлишкової деталізації.

Показник тональності текстового повідомлення $L_{п,н,нт}$ – це відношення кількості публікацій за тональністю ($l_{п,н,нт}$) до загальної кількості публікацій $N_{пуб.}$:

$$L_п = \frac{l_п}{N_{пуб.}} \cdot 100\%, L_н = \frac{l_н}{N_{пуб.}} \cdot 100\%, \quad L_{нт} = \frac{l_{нт}}{N_{пуб.}} \cdot 100\%. \quad (5)$$

Окрім базових показників, які характеризують негативний ПсВ та використовуються для обчислення узагальненого показника рівня негативного ПсВ, доцільним є оцінювання статистичних характеристик процесу розповсюдження ПсВ за кожним із напрямів реалізації впливу. Дане оцінювання дозволяє отримати обґрунтоване рішення щодо випадкового або невипадкового характеру виникнення текстових повідомлень із негативним ПсВ та їх розповсюдження.

Одним із підходів є застосування статистики, яка ґрунтується на показнику Херста (H) [15, 16]. Використання даного показника знайшло поширення під час аналізу часових рядів. Для калібрування часових вимірювань Херст ввів безрозмірний коефіцієнт шляхом ділення розмаху на стандартне відхилення спостережень. Цей метод називається методом нормованого розмаху (R/S – аналіз).

Розрахунок показника Херста

Популярність показника Херста викликана його високою стійкістю, можливістю класифікації досліджуваних часових вибірок і визначення їх випадкового чи невипадкового характеру. Його розрахунок ґрунтується на персистентності (схильності часових рядів до трендів). Кожне спостереження містить пам'ять про всі попередні події. Це не короткочасна пам'ять, яку часто називають "марківською", а інша – довготривала, теоретично вона зберігається назавжди. Нещодавні події мають більший вплив, ніж давно минулі, але їхній залишковий вплив завжди відчутний. Те, що відбувається сьогодні, впливає на майбутнє, і стан системи, у якому вона перебуває, визначається тим, якою вона була в минулому. Час виявляється важливим чинником. Показник Херста має таке значення:

1) $0 \le H < 0,5$ – антиперсистентний або ергодичний часовий ряд, постійно змінюється тенденція зростання і спадання. Чим ближче це значення до нуля, тим ряд більш непостійний, спостерігається броунівський рух і невизначеність. Такий тип поведінки називають "поверненням до середнього". Якщо для системи відбувається зростання певного показника в попередній період, то, швидше за все, в подальшому почнеться спад. І, навпаки, якщо йшло зниження, то ймовірний близький підйом;

2) $H = 0,5$ – часовий ряд абсолютно випадковий. Події випадкові і некорельовані, відсутня довготривала статистична залежність. Сьогодення не впливає на майбутнє. Функція щільності ймовірності може бути нормальною, проте це не обов'язкова умова. R/S – аналіз може ідентифікувати довільний ряд незалежно від типу функції розподілу, яка йому відповідає;

3) $0,5 < H \le 1,0$ – персистентний часовий ряд ("чорний шум"), спостерігається тренд, збереження тенденції до зростання чи спадання показника як у минулому, так і в майбутньому. Трендостійкість поведінки, або сила персистентності, збільшується в разі наближення H до 1 або 100% кореляції. Чим ближче H до 0,5, тим більше ряд зашумлений і тим менше виражений його тренд.

Показник Херста пов'язаний з такими коефіцієнтами, як R та S: R – різниця максимального і мінімального накопиченого відхилення від вимірюваного значення – "розмах"; S – стандартне відхилення від вимірювального значення [16, 17]. Показник Херста можна розрахувати за такою послідовністю: спочатку обчислюють середнє значення появи текстового повідомлення за n періодів (кількість разів, годин, днів, місяців тощо), протягом яких проводилося вимірювання:

$$y_{cp} = \frac{1}{n}\sum_{t=1}^{n} y_i(t). \qquad (6)$$

Потім розраховують накопичене відхилення членів ряду від середнього його значення за n періодів:

$$X_u = \sum_{i=1}^{u}\left(y_i(t) - y_{cp}\right), \qquad (7)$$

де u – конкретний елемент ряду.

Після цього визначають різницю максимального і мінімального накопиченого відхилення, яка і називається "розмахом":

$$R = \max_{1\le u\le n}(X_u) - \min_{1\le u\le n}(X_u). \qquad (8)$$

Стандартне відхилення числового ряду одиниці аналізу розраховують за таким виразом:

$$S = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y_i(t) - y_{cp}\right)}. \qquad (9)$$

Після знаходження наведених вище показників визначають показник Херста для часового ряду текстових повідомлень з негативним ПсВ:

$$H = \ln\frac{R}{S} \Big/ \ln\frac{n}{2}. \qquad (10)$$

Для проведення аналізу пропонується обирати тільки часові ряди текстових повідомлень, які характеризуються ознаками персистентності, а показник Херста знаходиться в межах $0,5 < H \le 1,0$.

Важливим є також оцінювання трендостійкості зміни ПсВ за період аналізованого часу та проведення статистичного аналізу активності тематичного контенту в мережі Інтернет [18].

Висновки і перспективи подальших досліджень

Таким чином, запропоновано індикатори виявлення негативного ПсВ у текстових повідомленнях під час моніторингу е-ЗМІ: частота публікацій текстового повідомлення з негативним ПсВ за обраною тематикою; динаміка появи текстового повідомлення з негативним ПсВ за обраною тематикою; показник важливості е-ЗМІ (PageRang) у пошуковій системі Google; показник поширеності текстового повідомлення з негативним ПсВ за обраною тематикою; показник тональності текстового повідомлення; показник Херста (ознака персистентності). Урахування запропонованих індикаторів дозволяє більш об'єктивно та всебічно оцінювати рівень ПсВ на обрану цільову аудиторію, що мінімізує його залежність від суб'єктивного фактора.

Перспективами подальшого дослідження є впровадження зазначених індикаторів виявлення негативного ПсВ у модуль СПЗ для підвищення ефективності застосування спеціальних підрозділів ЗС України в процесі проведення заходів інформаційного протиборства в мережі Інтернет.

Література

1. Почепцов Г. Сучасні інформаційні війни : монографія. Київ : Дім "Києво-Могилянська академія", 2015. 497 с. **2. Артюшин Л. М.,** Чернишук С. В. Шляхи підвищення ефективності системи виявлення та оцінювання інформаційних загроз // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2018. № 3. С. 99–106. **3. Горбулін В. П.** Світова гібридна війна: український фронт : монографія / За заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с. **4.** Про Доктрину інформаційної безпеки України : Указ Президента України від 25 лютого 2017 р. № 47/2017. URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення: 03.05.2019). **5.** Підсистема моніторингу інформаційного простору як необхідна складова протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / Сніцаренко П. М., Саричев Ю. О., Ткаченко В. А., Мотузяник О. А. // Наука і оборона. Київ : НУОУ, 2018. № 1. С. 29–33. **6. Левченко О. В.,** Косогов О. М., Сірик А. О. Методика оцінювання кількісних показників негативного інформаційного впливу // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2017. № 1. С. 31–35. **7. Грищук Р. В.,** Манько О. В., Орищук І. О. Особливості організації та ведення моніторингу електронних засобів масової комунікації // Інформаційна безпека. Луганськ : СНУ ім. В. Даля, 2014. № 3. С. 10–14. **8. Дзюба Т. М.,** Волошина Н. М., Пампуха І. В. Механізм інформаційно-психологічного впливу на психіку людини у гібридній війні // Зб. наук. праць Військ. ін-ту Київськ. нац. ун-ту ім. Тараса Шевченка. Київ : ВІКНУ, 2016. Вип. 51. С. 91–99. **9.** Інформаційно-

психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії / Пєвцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. // Наука і оборона. Київ : НУОУ, 2015. № 2. С. 28–32. **10.** Cyber and Information warfare in the Ukrainian conflict / Center for Security Studies (CSS), ETH Zurich. 2017. URL: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf (дата звернення: 21.05.2019). **11.** Disinformation Resilience in Central and Eastern Europe. URL: http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf (дата звернення: 21.05.2019). **12. Левченко О. В.** Класифікація інформаційної зброї за засобами ведення інформаційної боротьби // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2014. № 2 (20). С. 142–146. **13. Плеханова А. О.** Методы выбора и оценки эффективности информационных систем // Информационные технологии в управлении, образовании, науке и промышленности : монография / Под ред. В. С. Пономаренко. Харьков : Издатель Рожко С. Г., 2016. С. 491–505. **14. Горбулін В. П**., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с. **15. Федер Е.** Фракталы. Москва : Мир, 1991. 254 с. **16. Hurst H. E.** Long Term Storage Capacity of Reservoirs // Transactions of the American Society of Civil Engineers, 1951. № 116. P. 770–799. **17. Дербенцев В. Д.,** Сердюк О. А., Соловйов В. М., Шарапов О. Д. Синергетичні та еконофізичні методи дослідження динамічних та структурних характеристик економічних систем : монографія. Черкаси : Брама-Україна, 2010. 287 с. **18. Лагодний О. В.,** Писарчук О. О., Міхєєв Ю. І. Статистичний аналіз активності тематичного контенту в мережі Інтернет для прогнозування розвитку інформаційних загроз // Траекторія науки. Словаччина. 2017. Т. 3, № 8. С. 3011–3019.

ИНДИКАТОРЫ ВЫЯВЛЕНИЯ НЕГАТИВНОГО ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ ВО ВРЕМЯ МОНИТОРИНГА ЭЛЕКТРОННЫХ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ

Леонид Михайлович Артюшин *(доктор технических наук, профессор)*[1]
Александр Васильевич Лагодный *(кандидат технических наук)*[2]

[1]***Государственный научно-исследовательский институт авиации, Киев, Украина***
[2]***Житомирский военный институт имени С. П. Королева, Житомир, Украина***

Представление направленной информации в виде текстовых сообщений позволяет осуществлять психологическое влияние на определенные целевые аудитории с целью формирования предполагаемых последствий, в том числе и полезных противнику. Проанализированы существующие подходы к практике мониторинга сети Интернет по выявлению негативного психологического влияния и установлено их недостатки. В статье предложены индикаторы выявления негативного психологического влияния на личный состав Вооруженных Сил Украины во время мониторинга электронных средств массовой информации. Система приведенных индикаторов позволяет количественно оценивать уровень негативного психологического влияния при проведении противником в интернет-сети специальных действий. Это дает возможность прогнозировать развитие событий и своевременно принимать меры информационного противодействия. Количественные показатели негативного психологического влияния в текстовых сообщениях электронных средств массовой информации позволяют объективно оценивать уровень опасности определенной целевой аудитории и минимизировать уровень субъективизма при мониторинге интернет-ресурсов. Индикаторы объединяют комплексный подход к выявлению негативного психологического влияния за счет семантических и статистических методов. Результаты данной работы могут быть реализованы в виде модуля специализированного программного обеспечения в подсистеме обнаружения негативного психологического влияния личному составу Вооруженных Сил Украины.

Ключевые слова: *сеть Интернет; психологическое влияние; индикаторы.*

DETERMINATION INDICATORS OF NEGATIVE PSYCHOLOGICAL INFLUENCE UNDER MONITORING OF ELECTRONIC MASS MEDIA

Leonid Artushin *(Doctor of Technical Sciences, Professor)*[1]
Oleksandr Lahodnyi *(Candidate of Technical Sciences)*[2]

[1]***State Research Aviation Institute, Kyiv, Ukraine***
[2]***Koroljov Zhytomyr Military Institute, Zhytomyr, Ukraine***

The submission of directed information in the form of text messages allows to carry out psychological influence on certain target audiences in order to form the foreseeable consequences, including useful to the opponent. The existing approaches to monitoring the Internet for the detection of negative psychological influence, as well as their disadvantages are analyzed. Indicators of detection of negative psychological influence on the personnel of the Armed Forces of Ukraine during monitoring of electronic mass media were suggested. The system of the given indicators allows to quantify the level of negative psychological influence during the conduct of the enemy's special actions on the Internet. It allows to predict the development of events

and to timely take measures of information counteraction. Quantitative indicators of negative psychological impact in text messages of electronic mass media allow to objectively assess the level of danger to a specific target audience and to minimize the level of subjectivity during monitoring of Internet resources. Indicators combine a comprehensive approach to detecting negative psychological effects through semantic and statistical methods. The results of this work can be implemented as a module of specialized software in the subsystem of detecting negative psychological impact on the personnel of the Armed Forces of Ukraine.

Keywords: *Internet; psychological influence; indicators.*

References

1. Pochepcov Gh. (2015), Modern information wars: a monograph. [*Suchasni informacijni vijny: monoghrafija*], Kyiv, dim "Kyjevo-Moghyljansjka akademija", 497 p. **2. Artyushin L. M.,** Chernyshuk S. V. (2018), Approaches of improvement of effectiveness of information threats detection and estimation system. [*Shljakhy pidvyshhennja efektyvnosti systemy vyjavlennja ta ocinjuvannja informacijnykh zaghroz*], Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony, No. 3, pp. 99–106. **3. Ghorbulin V. P.** (2017), World hybrid war: Ukrainian front: monograph. [*Svitova ghibrydna vijna: ukrajinsjkyj front: monoghrafija za zagh. red. V. P. Ghorbulina*], NISS, Kyiv, 496 p. **4.** On the Doctrine of Information Security of Ukraine: Decree of the President of Ukraine dated February 25, 2017 No. 47. [*Pro Doktrynu informacijnoji bezpeky Ukrajiny: Ukaz Prezydenta Ukrajiny vid 25 ljutogho 2017 roku No 47/2017*], available at: http://www.president.gov.ua/documents/472017-21374 (posting date 03.05.2019). **5. Snicarenko P. M.,** Sarychev Ju. O., Tkachenko V. A., Motuzjanyk O. A. (2018), Subsystem of monitoring of the information space as an essential component of countering the negative informational and psychological impact on the personnel of the Armed Forces of Ukraine. [*Pidsystema monitorynghu informacijnogho prostoru jak neobkhidna skladova protydiji neghatyvnomu informacijno-psykhologhichnomu vplyvu na osobovyj sklad Zbrojnykh Syl Ukrajiny*], Nauka i oborona, No. 1, pp. 29–33. **6. Levchenko O. V.,** Kosoghov O. M., Siryk A. O. (2017), Method of estimation of quantitative indicators of negative informational influence. [*Metodyka ocinjuvannja kiljkisnykh pokaznykiv neghatyvnogho informacijnogho vplyvu*], Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony, No. 1, pp. 31–35. **7. Ghryshhuk R. V.,** Manjko O. V., Oryshhuk I. O. (2014), Features of organization and monitoring of electronic media of mass communication. [*Osoblyvosti orghanizaciji ta vedennja monitorynghu elektronnykh zasobiv masovoji komunikaciji*], Informacijna bezpeka, No. 3, pp. 10–14. **8. Dzjuba T. M.,** Voloshyna N. M., Pampukha I. V. (2016), Mechanism of informational and psychological influence on human psyche in hybrid warfare. *[Mekhanizm informacijno-psykhologhichnogho vplyvu na psykhiku ljudyny u ghibrydnij vijni*], zb. nauk. pracj. Vijsjkovogho instytutu Kyjivsjkogho nacionaljnogho universytetu imeni Tarasa Shevchenka, No. 51, pp. 91–99. **9. Pjevcov Gh. V.,** Zalkin S. V., Sidchenko S. O., Khudarkovsjkyj K. I. (2015), Information-psychological operations of the Russian Federation in Ukraine: models of influence and directions of counteraction. [*Informacijno-psykhologhichni operaciji Rosijsjkoji Federaciji v Ukrajini: modeli vplyvu ta naprjamy protydiji*], Nauka i oborona, No. 2, pp. 28–32. **10.** Cyber and Information Warfare in the Ukrainian Conflict (2017), [*Kiber ta informacijna vijna v ukrajinsjkomu konflikti*], Centr doslidzhenj bezpeky (CSB), available at: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf (posting date 21.05.2019). **11.** Disinformation Resilience in Central and Eastern Europe. [*Dezinformacijna stijkistj u Centraljnij ta Skhidnij Jevropi*], available at: http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf (posting date 21.05.2019). **12. Levchenko O. V.** (2014), Classification of information weapons by means of conducting an information struggle. [*Klasyfikacija informacijnoji zbroji za zasobamy vedennja informacijnoji borotjby*], Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony, No. 2, pp. 142– 146. **13. Plehanova A. O.** (2016), Methods of selection and evaluation of the effectiveness of information systems//Information technologies in management, education, science and industry: monograph/ed. V. S. Ponomarenko. [*Metodyi vyibora i otsenki effektivnosti informatsionnyih sistem//Informatsionnyie tehnologii v upravlenii, obrazovanii, nauke i promyishlennosti: monografiya/pod red. V. S. Ponomarenko*], Kharkov, Izdatel Rozhko S. G., pp. 491–505. **14. Ghorbulin V. P.,** Kachynsjkyj A. B. (2010), Strategic planning: solving problems of national security: monograph. [*Strateghichne planuvannja: vyrishennja problem nacionaljnoji bezpeky: monoghrafija*], Kyiv, NISD, 288 p. **15. Feder E.** (1991), Fractals. [Fraktalyi], Moscow, Mir, 254 p. **16. Kherst Kh. E.** (1951), Long Term Storage Capacity of Reservoirs. [*Dovghotryvala potuzhnistj vodoskhovyshh*], Operaciji Amerykansjkogho tovarystva cyviljnykh inzheneriv, pp. 770–799. **17. Derbencev V. D.,** Serdjuk O. A., Solovjov V. M., Sharapov O. D. (2010), Synergetic and econophysical methods of study of dynamic and structural characteristics of economic systems: monograph. [*Synerghetychni ta ekonofizychni metody doslidzhennja dynamichnykh ta strukturnykh kharakterystyk ekonomichnykh system: monoghrafija*], Cherkasy, Brama-Ukrajina, 287 p. **18. Lahodnyi O. V.,** Pysarchuk O. O., Mikhjejev Ju. I. (2017), Statistical Analysis of the Activity of the Thematic Content on the Internet forPredicting the Development of Information Threats. [*Statystychnyj analiz aktyvnosti tematychnogho kontentu v merezhi Internet dlja proghnozuvannja rozvytku informacijnykh zaghroz*], Traektorija nauky, Volume 3, No. 8, pp. 3011-3019.