УДК 004.413.4:004.738.52

Ю. Г. ДАНИК,
доктор технічних наук, професор,
О. О. ПИСАРЧУК,
доктор технічних наук, професор,
О. В. ЛАГОДНИЙ, *ад'юнкт*
(Житомирський військовий інститут ім. С. П. Корольова),
Г. С. ГАЙДАРЛИ,
старший науковий співробітник
(Національний університет оборони України ім. І. Черняховського, м. Київ)

Фасетна система класифікації інформаційних загроз визначеній цільовій аудиторії в кібернетичному просторі

Запропоновано фасетну систему класифікації інформаційних загроз цільовій аудиторії в кібернетичному просторі, що усуває недоліки ієрархічних систем класифікацій і дає можливість отримувати код інформаційної загрози для каталогізації, архівації та ідентифікації. Використання запропонованої фасетної класифікації зменшує час, необхідний для ідентифікації інформаційної загрози в інформаційних джерелах Інтернету.

Предложена фасетная система классификации информационных угроз целевой аудитории в кибернетическом пространстве, которая устраняет недостатки иерархических систем классификаций и дает возможность получать код информационной угрозы для каталогизации, архивации и идентификации. Использование предложенной фасетной классификации уменьшает время, необходимое для идентификации информационной угрозы в информационных источниках Интернета.

Враховуючи досвід проведення антитерористичної операції в окремих районах східної частини України, можна стверджувати, що в теперішній час стрімко розвивається "неконвенційна війна" (unconventional warfare), якій притаманні процеси всебічної інформатизації суспільства у формі неконвенційних дій (гібридних, асиметричних, мережоцентричних, високотехнологічних тощо) [1]. Характерною ознакою таких дій є застосування поряд з традиційним озброєнням і військовою технікою форм, методів і засобів деструктивного інформаційно-психологічного впливу (ІПсВ) на керівництво, особовий склад Збройних Сил, соціальні верстви населення держави-противника. Загалом неконвенційні дії спостерігаються в збройних конфліктах протягом останніх 10 років, наприклад, у Грузії, Україні, Сирії, Абхазії. Одною зі складових таких неконвенційних дій є ІПсВ, суть якого полягає в негативному впливі на визначену цільову аудиторію за допомогою інформації, що призводить до зміни думок, світоглядних установок та системи знань про навколишній світ, певних дій особистості. За допомогою використання методів і форм ведення ІПсВ інформаційне повідомлення трансформується в інформаційну загрозу (ІЗ), яка призводить до негативного впливу і поширюється через глобальну мережу Інтернет, а точніше через кібернетичний простір (КП). Під КП будемо розуміти систему, яка складається з елементів формування, передавання, зберігання інформації та взаємозв'язків між ними, у ньому готуються й відбуваються процеси управління, здійснюються управлінські відносини. Складовими КП є інформаційний, комунікаційний, віртуальний комп'ютерно-мережний та соціотехнічний простори [2]. Стрімкий розвиток КП надає цільовій аудиторії безмежний доступ до різноманітної інформації в Інтернеті.

Щодня здійснюється ІПсВ, ІЗ доставляються до цільової аудиторії через теле-, радіомовлення, друковані засоби тощо, у тому числі й через Інтернет. Визначена цільова аудиторія, на яку спрямований ІПсВ, сприймаючи різноманітну інформацію у вигляді повідомлень, тексту, аудіо-, відеороликів, не може в ній розрізнити ІЗ, яка має на меті переконати чи змусити особистість до певної дії, що може призвести до виникнення кризових явищ у суспільстві [3]. Для протидії ІПсВ першочерговим завданням є своєчасне виявлення, прогноз подальшого розвитку ІЗ та вжиття відповідних заходів щодо їх стримування, нейтралізації. Для того щоб виявляти ІЗ, потрібно мати їх класифікацію за певними індикаторами. Тому **актуальним завданням є** розроблення системи класифікації ІЗ для своєчасного їх виявлення в КП за певними, більш дієвими, індикаторами (фасетами).

Підходи до класифікації ІЗ висвітлені в багатьох публікаціях вітчизняних і закордонних вчених. Найвідомішими серед них є В. А. Ліпкан, Ю. Г. Даник, В. Л. Бурячок, В. О. Хорошко, А. В. Манойло, В. Г. Крисько тощо [4–7]. Аналіз їх робіт за напрямом досліджень свідчить про те, що класифікація ІЗ визначеній цільовій аудиторії в КП потребує додаткового вивчення. Це пов'язано з тим, що дана класифікація повинна забезпечувати виконання таких завдань:

1) вона має обмежуватися визначеною цільовою аудиторією, активністю контенту, текстами повідомлень з інтернет-сайтів, що стосуються національної безпеки України;

2) розроблена класифікація повинна стати основою для процесів: моніторингу, виявлення, протидії, прогнозу;

3) вона має надати можливість для прогнозу біфуркаційного розвитку ІЗ;

4) значна динаміка зміни щільності потоку ІЗ повинна враховуватися при проведенні класифікації.

У цілому класифікація процесів і явищ передбачає розбиття об'єкта дослідження на класи і підкласи на основі загальних ознак. Результати таких класифікацій відображають у вигляді ієрархічних (деревоподібних) схем. При проведенні класифікації конфліктних чи загрозливих ситуацій їх поділяють на типи та види. Класифікація ризиків становить собою розподіл їх на окремі групи за визначеними ознаками для досягнення конкретної мети. Загрози в інфосфері класифікують за джерелом їх виникнення та об'єктом, на який вони націлені.

Більшість авторів у своїх публікаціях застосовували, як правило, ієрархічну систему класифікації, при якій послідовно деталізуються тільки якісні властивості об'єктів дослідження множин: клас, підклас, група, підгрупа, вид тощо. Дану систему широко використовують у різних галузях науки, але вона має такі недоліки: брак резервного обсягу; складність; необхідність ранжирування ознак класифікації; побудова громіздкого класифікаційного дерева. Усе це призводить до неможливості чіткої ідентифікації об'єктів класифікації. Проте існує інший метод – це фасетна система класифікації, що передбачає паралельний поділ множини об'єктів на незалежні класифікаційні угруповання, де множина об'єктів, що характеризується деяким набором однакових для всіх ознак (фасет), може поділятися багаторазово і незалежно [8]. Фасети – основні ознаки, індикатори, за якими потрібно розробити класифікацію ІЗ визначеній цільовій аудиторії в КП. Отже пропонуємо застосувати фасетну систему класифікації, що компенсує недоліки ієрархічної системи, є інноваційною в предметній області, більш зручною для інформаційно-пошукових

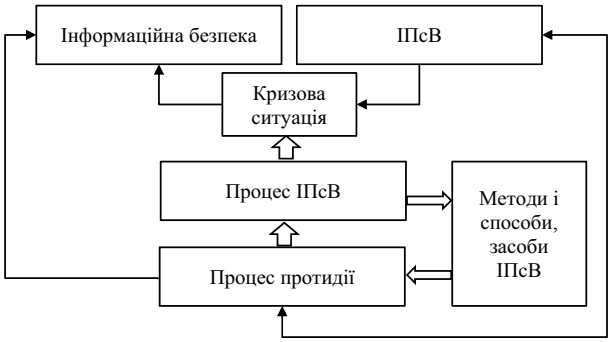

Рис. 1

систем і дозволяє систематизувати процес за необхідним набором ознак.

Метою статті є розроблення фасетної системи класифікації ІЗ визначеній цільовій аудиторії в КП.

Для досягнення мети дослідження в першу чергу необхідно сформулювати понятійний апарат, розкрити сутність і зміст ІЗ визначеній цільовій аудиторії, встановити основні складові системи реалізації ІЗ та процесу, який відбувається всередині неї. Загальна структурна схема ІЗ інформаційній безпеці, зображена на рис. 1, дає уявлення про взаємозв'язок елементів і процесів.

Під *інформаційною безпекою* будемо розуміти такий стан захищеності людини, суспільства і держави, при якому забезпечується адекватне світосприйняття особистістю інформації з різноманітних джерел, що досягається своєчасним виявленням та прогнозуванням розвитку ІЗ.

Загроза – явище, чинник (їх сукупність), що здатні реально створити умови або стати причиною повної або часткової неможливості реалізації будь-яких інтересів.

Інформаційна загроза – сукупність умов, випадкове поєднання обставин і подій або наміри об'єкта впливу щодо реалізації ймовірної небезпеки, яка несе деструктивний інформаційний вплив на особистість, суспільство, державу.

Для проведення фасетної системи класифікації будемо розглядати ІЗ, що присутні в інформаційному просторі та своїм деструктивним впливом на визначену цільову аудиторію можуть призвести до кризової ситуації.

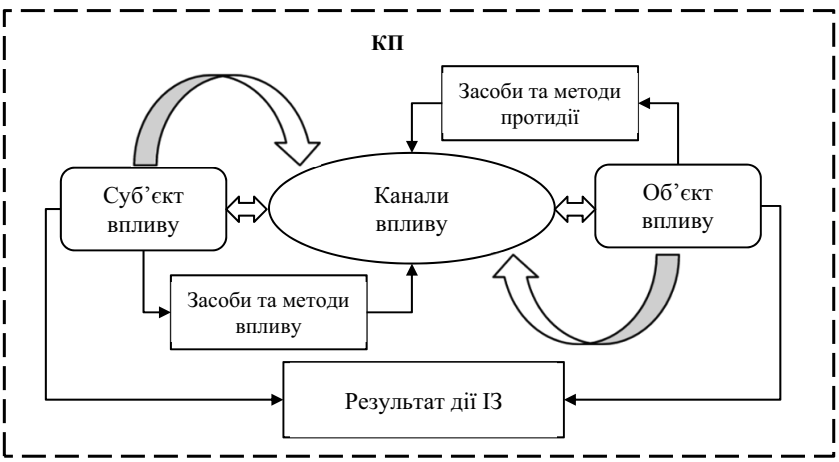

Рис. 2

ІЗ трансформується в інформацію у вигляді дезінформації, маніпулювання, навіювання, переконання та безпосередньо впливає на інформаційну безпеку держави.

Кризова ситуація – це такий стан системи, при якому контрольовані параметри виходять за межі допустимих значень, і, як наслідок, виникають біфуркаційні точки, що призводить до хаосу. Кожна ІЗ як елемент системи має свої кількісні та якісні характеристики. В інформаційному просторі до основних абстрактних характеристик ІЗ можна віднести: джерело її виникнення; частоту появи; об'єкт ІЗ; її контентне забарвлення; спосіб реалізації. Для проведення класифікації ІЗ цільовій аудиторії потрібно використовувати багатокритеріальний підхід, який дасть змогу врахувати більшість критеріїв (характеристик, індикаторів) ІЗ і підвищить адекватність прийняття остаточних рішень.

Реалізація ІЗ можлива за наявності таких основних складових системи (рис. 2): об'єкта й суб'єкта впливу, зв'язку між ними в КП, де відбувається даний процес.

Об'єкт впливу – це особистість, суспільство, держава, щодо яких можливе здійснення ІПсВ (у тому числі застосування інформаційної зброї), результатом якого буде модифікація властивостей свідомості як інформаційної системи. Об'єкт впливу є елементом сприйняття, аналізу та прийняття рішення (результат дії ІЗ).

Суб'єкт впливу – це особистість, суспільство, держава, група осіб, віртуальна соціальна спільнота, які здійснюють ІПсВ на визначений об'єкт відповідними засобами та методами. Суб'єкт впливу є елементом формування та розповсюдження ІЗ.

На рис. 3 зображено процес деструктивного впливу на соціум, який передбачає лавиноподібний перехід від одного етапу до іншого та містить в собі такі основні елементи логічного ланцюга: суб'єкт впливу (поява, джерело ІЗ) – загроза (дія, атака) – об'єкт впливу (сприйняття ІЗ) – результат дії (наслідок). При цьому ІЗ в цьому ланцюзі розвивається, модифікується і здатна до самоорганізації.

На рис. 3 введено такі позначення: X(t) – вхідна складова ІПсВ, Y(t) – прийняття рішення об'єктом (результат дії ІЗ), $k_i(t)$ – інформаційні загрози, t – час.

Суб'єкт впливу S як осередок виникнення ІЗ – середовище формування, передавання, обміну та зберігання інформації різного характеру, що служить для донесення до цільової аудиторії відповідна контенту негативного характеру.

Дія загрози N – це можлива небезпека (потенційна або та, що вже існує) вчинення будь-якої негативної дії, спрямованої на соціум. Її ефективність залежить від індивідуальних властивостей об'єкта впливу: освіченості, навколишнього середовища сприймання інформації, інформованості та часу перебування під ІПсВ.

Об'єкт впливу D – це соціум, який знаходиться під дією ІЗ і сприймає визначений контент у вигляді ІЗ завдяки проведенню інформаційних і кібернетичних дій над інформацією.

Результат дії загрози R – це можливі наслідки реалізації ІПсВ при дії джерела загрози в КП.

ІЗ може проявлятися в різних формах інформації, тому при проведенні фасетної класифікації слід враховувати методи і форми ІПсВ (рис. 4).

Протидія відомим формам і методам ІПсВ займає важливе місце в системі забезпечення інформаційної безпеки держави та включає в себе комплекс заходів щодо запобігання виникненню кризових ситуацій (рис. 5). Саме своєчасність виявлення і прогнозування подальшого розвитку ІЗ дозволить ефективно протидіяти цим методам і формам ІПсВ.

Для того щоб розробити фасетну класифікацію, потрібно виділити, за якими індикаторами (фасетами) її проводити та дотримуватися встановлених правил проведення класифікації. Відповідно до нової редакції

Рис. 3

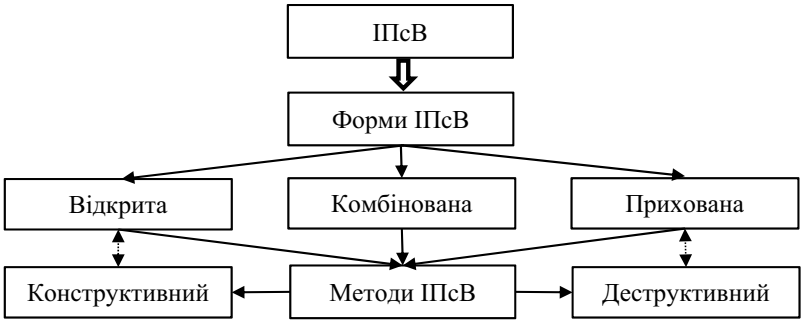

Рис. 4

Воєнної доктрини України 2015 року [9] основними реальними та потенційними загрозами інформаційній безпеці цільовій аудиторії України є:

зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

поширення негативного інформаційного впливу на свідомість людини (громадянина), здатного змінювати психічний стан, психологічні та фізіологічні характеристики, керувати свободою вибору;

деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України;

використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками.

Основними вимогами методу фасетної класифікації є:

1) наявність достатнього обсягу необхідної інформації, що гарантувала б охоплення всіх об'єктів класифікації;

2) забезпечення гнучкості й надмірності для можливого збільшення множини об'єктів, що класифікуються;

3) дотримання принципу взаємного виключення фасетів;

4) врахування істотних ознак, що забезпечують вирішення цільовго завдання;

5) лаконічність, чіткість і зрозумілість класифікаційних ознак.

Наведені вище індикатори відображають методи та способи реалізації ІПсВ, а вимоги методу фасетної класифікації – місце їх у фасетах: за інформаційним джерелом *S*; за контентним забарвленням інформаційного повідомлення *B*; за характером інформації *T*; за формою подання інформації *F*; за частотою появи в інформаційному джерелі *N*; за об'єктом впливу *D*; за способом ІПсВ *E*; за реакцією аудиторії на ІЗ *R*; за рівнем загрози системі управління держави G.

Визначенню фасетів ІЗ передував аналіз реального негативного інформаційного впливу в повідомленнях, розміщених у відкритих інформаційних джерелах інтернет-середовища. Об'єктом ІПсВ було обрано керівництво України як складну соціотехнічну систему.

Характеристика фасетів.

Фасет 1. Формування, зміна, трансформація і розповсюдження інформації відбувається в джерелі виникнення ІЗ. В Інтернеті ці процеси протікають швидше, ніж в засобах теле-, радіомовлення, тому *за інформаційне джерело S* доцільно розглядати соціальні мережі, інформаційні сайти, блоги і форуми [10].

Фасет 2. Інформація може мати позитивний, нейтральний і негативний характер, саме ці ознаки і застосуємо у фасеті *контентне забарвлення інформаційного повідомлення B*.

Фасет 3. *За характером інформації T* інформаційний привід може бути достовірним негативним, достовірним позитивним і неправдивим (фейковим).

Фасет 4. *За формою подання інформації F* слід розглядати приховану і відкриту форму відображення інформаційного повідомлення.

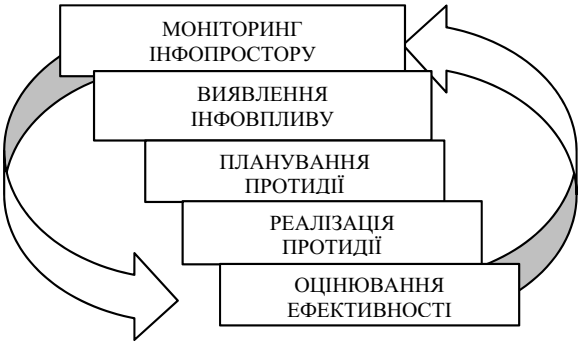

Рис. 5

Фасет 5. *Під частотою появи в інформаційному джерелі N* будемо розуміти появу певного інформаційного повідомлення, яке містить ІЗ, в дискретні проміжки часу: фонова публікація, фаза підготовки, інформаційна операція. Частота появи характеризує активність контенту.

Фасет 6. Інформаційна загроза може бути спрямована будь на кого незалежно від соціального статусу, віку, місця проживання тощо. *Серед об'єктів впливу D* визначено такі: Президент країни, влада, керівництво Збройних Сил України, особовий склад Збройних Сил України, соціальна група, окрема особистість.

Фасет 7. До більш негативних *способів ІПсВ E* на свідомість особистості належать навіювання, дезінформація, переконання, маніпулювання.

Фасет 8. *Реакція аудиторії на ІЗ R*, яка взаємозв'язана з частотою появи в інформаційному джерелі і викликає в особистості негативне ставлення до процесів, що відбуваються, може проявлятись в її незадоволенні владою, проведенні страйків, терористичних актів, революцій, збройних сутичок. Реальним доказом цього є анексія Криму Російською Федерацією та введення своїх військ для підтримки так званих ДНР і ЛНР.

Фасет 9. *Під рівнем загрози системі управління держави G* мається на увазі ієрархія управління, де відбувається прийняття рішення: вищого (стратегічного), середнього (оперативного), нижчого (оперативно-тактичного) рівнів.

Результати фасетної класифікації оформлено у вигляді спеціальної таблиці, стовпці якої визначають критерії класифікації (що для зручності користування в подальших наукових дослідженнях будуть нормовані), а рядки – можливі значення цих критеріїв.

Розроблену дев'ятикритеріальну фасетну класифікацію ІЗ визначеній цільовій аудиторії в КП наведено в табл. 1. У ній виокремлено 9 принципових підходів, кожен з яких характеризується 2–6 індикаторами. Зведений перелік критеріїв для фасетної класифікації формується в 9 паралельних незалежних фасетів. Конкретні значення критеріїв доповнюються характерними ознаками й у фасеті розміщуються у вигляді простого переліку.

Таблиця 1

Дев'ятикритеріальна фасетна класифікація ІЗ визначеній цільовій аудиторії в КП

№	Код фасета	Розділ фасета	Опис
1	S		**Класифікація ІЗ за інформаційним джерелом**
		1	Соціальні мережі
		2	Інформаційні сайти
		3	Блоги, форуми
2	B		**Класифікація ІЗ за контентним забарвленням інформаційного повідомлення**
		1	Негатив
		2	Нейтральна
		3	Позитив
3	T		**Класифікація ІЗ за характером інформації**
		1	Достовірний негатив
		2	Достовірний позитив
		3	Фейк
4	F		**Класифікація ІЗ за формою подання інформації**
		1	Прихована
		2	Відкрита
5	N		**Класифікація ІЗ за частотою появи в інформаційному джерелі**
		1	Фонова публікація
		2	Фаза підготовки
		3	Інформаційна операція
6	D		**Класифікація ІЗ за об'єктом впливу**
		1	Президент України
		2	Влада країни
		3	Керівництво ЗС України
		4	Особовий склад ЗС України
		5	Соціальна група
		6	Окрема особистість
7	E		**Класифікація ІЗ за способом впливу**
		1	Навіювання
		2	Дезінформація
		3	Переконання
		4	Маніпулювання
8	R		**Класифікація ІЗ за реакцією аудиторії на ІЗ**
		1	Невдоволення
		2	Страйк
		3	Революція
		4	Терористичний акт
		5	Збройний конфлікт
9	G		**Класифікація ІЗ за рівнем загрози системі управління держави**
		1	Вищий (стратегічний) рівень
		2	Середній (оперативний) рівень
		3	Нижчий (оперативно-тактичний) рівень

Практичний приклад застосування

Наприклад, назва одного з рівнів небезпеки інформаційної загрози описана фасетною класифікацією: код S.2–B.1–T.3– F.2–N.3–D.1–E.4–R.3–G.1. Розшифрування даного коду: проводиться інформаційна операція способом маніпулювання свідомістю населення через інформаційні сайти, розповсюджений негативний контент проти Президента України, який є відкритим фейком, може призвести до революції та загрожує стратегічному рівню управління державою.

Проводився моніторинг відкритих джерел інформації в мережі Інтернет, у результаті якого були виявлені інформаційні приводи певного змісту. На основі фасетів (табл. 1) ІЗ були присвоєні коди. Результати дослідження відображено в таких фасетах: реальні події, які відбулися, і відомі наслідки, наприклад:

"14.09.2015 Порошенко відмовився обмінювати Савченко на російських спецназівців" – код S.2–B.1–T.1–F.2–N.1–D.1–E.3–R.1–G.1;

"15.09.2015 Соцопитування: українці категорично проти прем'єрства Тимошенко"– код S.1,3–B.2–T.3–F.1–N.1–D.6–E.2–G.3;

"*17.09.2015 Ляшко після арешту Мосійчука звинуватив Порошенка в шантажі"*– код S.2,3–B.1–T.1–F.2–N.1–D.1–E.1–R.2–G.1.

Тобто пряма або опосередкована ІЗ несе небезпеку системі в цілому або її складовим. Реакція аудиторії на дані ІЗ – економічна, політична, соціальна кризи.

Висновки. При проведенні дослідження було розроблено фасетну систему класифікації ІЗ визначеній цільовій аудиторії в КП. Вона побудована таким чином, щоб була можливість наповнення класифікатора новими фасетами, категоріями фасетів та підкатегоріями. Запропонована фасетна класифікація дає можливість отримувати код ІЗ, що зменшує час, необхідний для її виявлення. Вона не є остаточною, може змінюватися й розширятися відповідно до виконання поставлених завдань. Перспективою подальших досліджень є: нормування індикаторів (критеріїв) ІЗ; оцінювання рівня небезпеки інформаційної загрози цільовій аудиторії; проведення прогнозування подальшого розвитку ІЗ.

СПИСОК ЛІТЕРАТУРИ

1. Unconventional warfare [Електронний ресурс]. – Режим доступу: https://fas.org/irp/doddir/army/fm3-05-130.pdf.
2. Інформаційна та кібербезпека: соціотехнічний аспект [Текст] : підруч. / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – К. : ДУТ, 2015. – 288 с.
3. Даник, Ю. Г. Національна безпека: запобігання критичним ситуаціям [Текст]: моногр. / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін. – Житомир : Рута, 2006. – 388 с.
4. Грищук, Р. В. Диференціально-ігрові моделі та методи моделювання процесів кібернападу [Текст] : дис. … д-ра техн. наук : 21.05.01 / Р. В. Грищук. – К., 2013. – 411 с.
1. Даник, Ю. Г. Підхід до класифікації кібернетичних загроз [Текст] / Ю. Г. Даник, В. І. Шестаков, С. В. Чернишук // Збірник наук. праць Національної академії Державної прикордонної служби України. Сер. Військові та технічні науки. – 2014. – № 1. – С. 314–329.
5. Никитина, В. Л. О классификации информационных отношений и угроз в сети Інтернет [Электронный ресурс] / В. Л. Никитина // Безопасность информационных технологий. – 2011.– № 2.– С. 21–23 [Електронний ресурс]. – Режим доступа: http://pvti.ru/data/ file/bit/bit_2_2011_4.pdf.
6. Манойло, А. В. Государственная информационная политика в особых условиях [Текст] : моногр. / А. В. Манойло. – М. : МИФИ, 2003. – 388 с.
7. Ясенев, В. Н. Автоматизированные информационные системы в экономике [Текст] : учеб.-метод. пособ. / В. Н Ясенев. – Н. Новгород, 2007. – С. 80.
8. Нова редакція Воєнної доктрини України : затверджена Указом Президента України № 555/2015 від 24 вересня 2015 року [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/5552015-19443.
9. Новиков, Д. А. Социальные сети: модели информационного влияния, управления и противборства [Текст] / Д. А. Новиков, Д. А. Губанов, А. Г. Чхартишвили ; под. ред. Д. А. Новикова. – М. : Изд-во физ-мат. лите-ры, 2010. – 228 с.

Рецензент Р. В. Грищук, д-р техн. наук, старший наук. співробітник (Житомирський військовий інститут ім. С. П. Корольова)