**Ключові слова:** еліптична крива, крива Едвардса, порядок кривої, порядок точці, символ Лежандра, квадратичний лишок, квадратичний не лишок, криві кручення.

## CORRELATION OF BIG ORDER POINTS SETS OF THE EDWARDS CURVES OVER PRIME FIELD

Modification of the addition law of an Edwards curve points over a prime field is offered. It ensures traditional horizontal symmetry of inverse points of an elliptic curve. 2 theorems of properties of points co-ordinates of the big order points are proved. These properties generated by point halving, inverse of point doubling. On their basis it is possible to calculate of points order with only two operations in the field without group operations. The theorem 3 about degenerate pair of twisted curves with order $N_E = p+1$ is proved, if $p \equiv 3 \bmod 4$ and $p \equiv \pm 3 \bmod 8$, $d = 2$ or $d' = 2^{-1}$. The statement 1 about a non-existence of point halving for points of a maximum order and points of 4th order is proved. The statement 2 is proved that at among 8 points of a set of the points lying on one circle, 2 points have an order $n$, 2 points - an order $2n$ and 4 points - a maximum order $4n$. The algorithm of reconstruction without evaluations of all unknown points $kP$ of a of Edwards curve is offered, if only at 1/8 parts of points is known.

**Index terms**: elliptic curve, Edwards curve, curve order, points order, Legendre symbol, square, non-square, twisted curves.

**Бессалов Анатолий Владимирович**, доктор технических наук, профессор, профессор кафедры математических методов защиты информации ФТИ НТУУ «КПИ».
E-mail: bessalov@ukr.net.
**Бессалов Анатолій Володимирович**, доктор технічних наук, професор, професор кафедри математичних методів захисту інформації ФТІ НТУУ «КПИ».
**Anatoliy Bessalov**, Dr eng (information security), professor NTUU «KPI» (Kyiv,Ukraine).

**Цыганкова Оксана Валентиновна**, аспирант кафедры математических методов защиты информации ФТИ НТУУ «КПИ».
E-mail: cig@pti.kpi.ua
**Цыганкова Оксана Валентинівна**, аспірант кафедри математичних методів захисту інформації ФТІ НТУУ «КПІ».
**Oksana Tsygankova** aspirant PTI NTUU «KPI» (Kyiv,Ukraine).

**УДК 004 : 316.6**

# ТЕХНОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА НА СУЧАСНОМУ ЕТАПІ

**Руслан Грищук, Іван Канкін, Володимир Охрімчук**

*У статті систематизовано відомі методи та способи інформаційного протиборства на сучасному етапі та встановлено його основні технологічні аспекти. Показано, що основним інструментом інформаційного протиборства сьогодні виступають соціальні інтернет сервіси. Доведено, що соціальні інтернет сервіси, поряд з класичними засобами інформаційного протиборства, використовуються суб'єктами інформаційної боротьби для ведення пропаганди та контрпропаганди.*

***Ключові слова:*** *інформаційне протиборство, технологія, класифікація, соціальний інтернет сервіс.*

**Вступ.** Високотехнологічний розвиток сучасного суспільства не в останню чергу обумовлений повсюдним застосуванням новітніх досягнень ІТ-індустрії в різних галузях його діяльності. Не становить виняток і військова сфера яка, як показує досвід [1, 2], стає рушійною силою процесів різноманітної природи.

Останні інновації в сфері комунікацій – засоби масової комунікації (ЗМК) такі, як е-ЗМІ, блогосфера, соціальні мережі та інші соціальні інтернет сервіси (СІС) сьогодні дуже часто використовуються як інструмент інформаційного протиборства. Ефективність їх застосування в першу чергу обумовлена масовою доступністю до них усіх без винятку верст населення, що суттєво спрощує досягнення суб'єктами інформаційного протиборства політичних, економічних, фінансових та інших цілей. Тому питання, які пов'язані з дослідженням ролі й місця інформаційного протиборства в світових глобалізованих процесах тільки актуалізуються.

Сьогодні в науковій літературі приділяється значна увага дослідженню питань розробки методів та способів ведення інформаційного протиборства. У роботах [2-5] авторів розглядаються питання дослідження видів та сфер ведення ін-

формаційного протиборства. Визначається його мета та основні напрямки. При цьому в [3] не наведено класифікацію методів та способів його ведення, що суттєво ускладнює виявлення його технологічних аспектів. Приведена у [5, 6] класифікація має суб'єктивний характер. Вона не дозволяє врахувати роль традиційних друкованих ЗМІ та телебачення в інформаційному протиборстві. Матеріали вітчизняних авторів таких як [7, 8] більше спрямовані на встановлення тенденцій створення та розвитку інтернет-спільнот та способів розповсюдження інформації визначеного контенту.

Таким чином, аналіз останніх досліджень і публікацій за визначеною темою показав, що до сьогодні відсутня цілісна методологія ведення інформаційного протиборства. Тому актуальним залишається завдання щодо встановлення нових технологічних аспектів, з метою подальшого створення на їх базі єдиного підходу для ефективної протидії в інтересах забезпечення інформаційної безпеки держави.

**Основна частина.** Суб'єктами інформаційного протиборства є вище політичне і воєнне керівництво держави, органи державної та місцевого самоврядування, населення. Тому цілком очевидно заходи інформаційного протиборства спрямовані перш за все на створення та нагнітання конфліктної обстановки всередині держави, провокації політичної напруги та хаосу, дискредитації органів державної влади, ініціювання масових протестних акцій та заворушень, дестабілізації у відносинах між політичними партіями, розв'язання в державі громадянської війни тощо.

Зважаючи на [9] та інші фахові видання особливостями інформаційних дій, що становлять одну з основ інформаційного протиборства можна визначити такі, як детермінована природа поширення (відомі як канали поширення, так і суб'єкти впливу); селективна спрямованість (визначений суб'єкт) і цільова орієнтація (мета впливу); тривалий підготовчий період та тривала латентна фаза при досягненні визначеного результату; інформаційні дії є передвісником до підготовки та здійснення інших дій, у тому числі й силового характеру із застосуванням традиційних бойових дій.

Методи інформаційного протиборства, як правило ґрунтуються на уразливості людської психіки до сторонніх впливів. Враховуючи їх способи реалізації [10] подамо їх узагальнену ознакову класифікацію (рис. 1).

Згідно з прийнятою класифікацією (див. рис. 1) *за типом протиборства (ТС)* суб'єктами захисту (або впливу) при інформаційно-психологічному протиборстві є:

– системи прийняття політичних рішень;

– системи формування громадської думки;

– системи формування суспільної свідомості (книги, фільми, телевізійні програми, друковані ЗМІ);

– психологічний вплив на психіку осіб, що приймають рішення (дискредитація лідерів) тощо.

Об'єктами захисту при інформаційно-технічному протиборстві є:

– системи передачі даних;

– системи захисту інформації;

– радіоелектронна боротьба.

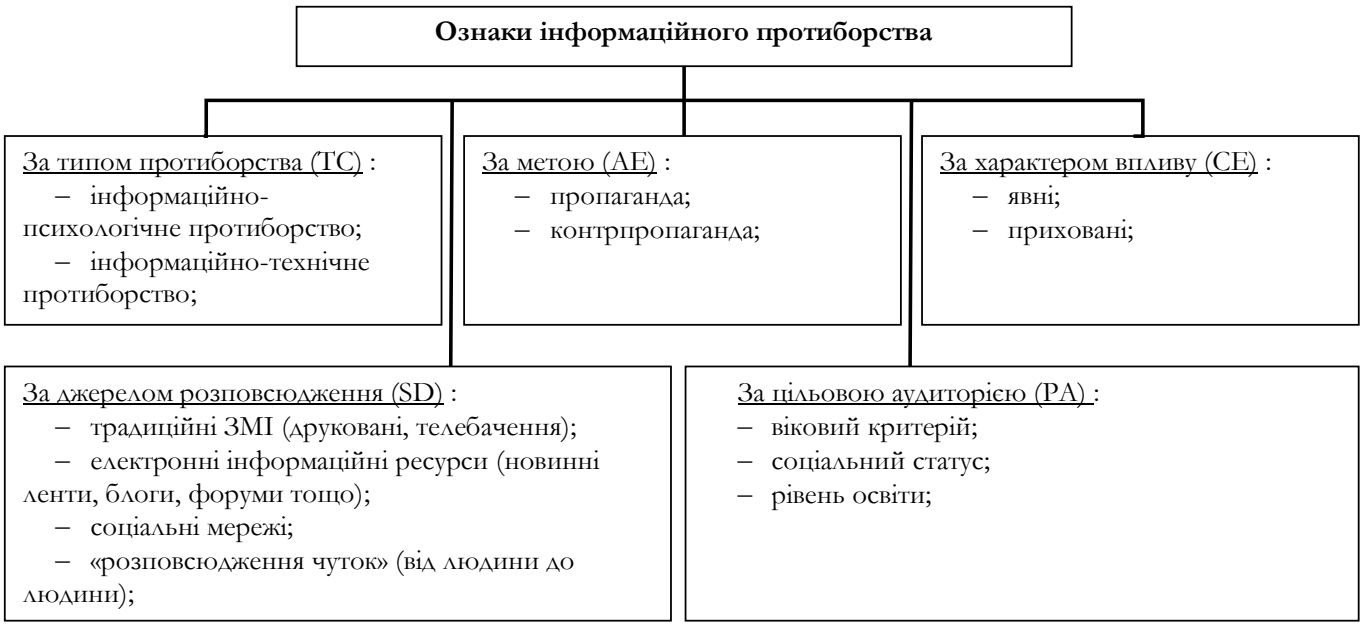


Рис. 1. Ознакова класифікація методів ведення інформаційного протиборства

Інформаційно-технічний вплив здійснюється переважно з метою порушення нормальних режимів роботи об'єктів та суб'єктів інформаційного протиборства та виведення з ладу їх телекомунікаційних систем, електронних інформаційних ресурсів та баз даних. З цією метою додатково для здійснення впливу на електронні інформаційні ресурси та бази даних використовуються програмні засоби деструктивного впливу (комп'ютерні віруси, троянські програми, «логічні бомби» тощо). Крім того ефективним та найбільш поширеним способом блокування таких ресурсів є здійснення кібератак класу DoS на відмову в обслуговуванні. Для порушення нормальної роботи телекомунікаційних систем, як правило, використовуються різноманітні засоби створення електромагнітних перешкод.

*За метою (AE)* розрізняють методи пропаганди та контрпропаганди [3]. Пропаганда спрямована на те, щоб донести до масової свідомості визначеної ідеї, тобто сформувати на визначеній ділянці інформаційного простору задане інформаційне підґрунтя.Контрпропаганда – це навпаки, комплекс заходів, що спрямовані на руйнування або придушення у заданому інформаційному просторі деструктивного інформаційного підґрунтя й недопущення його активізації в майбутньому.

Класифікація методів за цією ознакою із врахуванням *характеру їх впливу (CE)* на суб'єктів інформаційного протиборства подано на рис. 2.

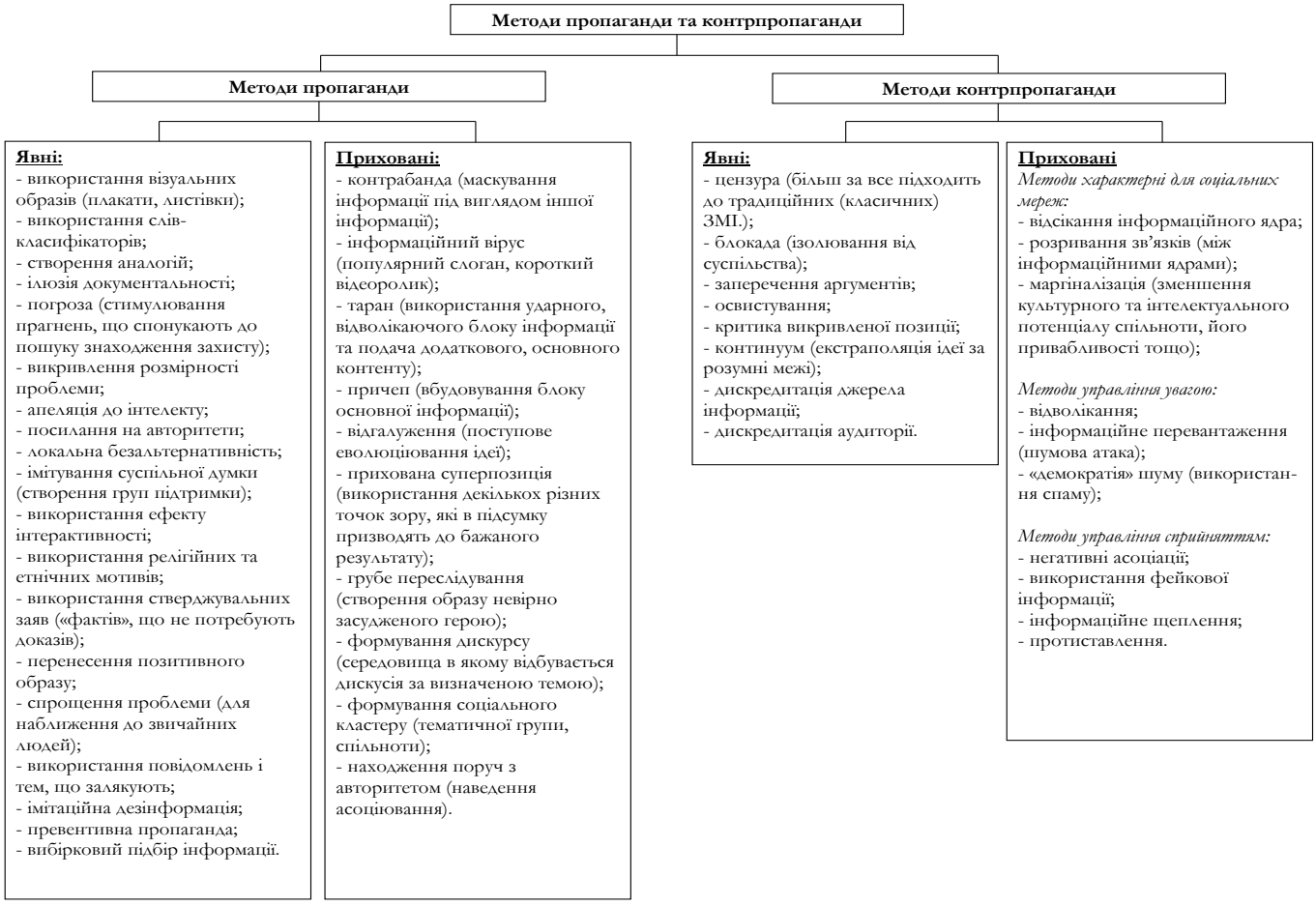


Рис. 2. Класифікація методів пропаганди та контрпропаганди за метою, залежно від характеру їх впливу на суб'єктів інформаційного протиборства

*За джерелами розповсюдження (SD)* різниця методів проявляється в способах їх реалізації. Провідна роль серед приведених вище методів (див. рис. 2) відводиться в першу чергу «класичним» засобам масової інформації (ЗМІ) – телерадіомовленню та друкованим виданням. Особливістю «класичних» ЗМІ є те, що по-перше, аудиторія центральних телевізійних каналів на порядок перевищує кількість аудиторії будь-якого інтернет-ресурсу та перекриває більший віковий діапазон. По-друге, телебачення сильніше у фоновому та наведеному інформаційному впливах.

Останнім часом спостерігається інтеграція «класичних» ЗМІ в електронне середовище – е-ЗМІ, які застосовуються як на підготовчому, основному, так і на завершальному періодах [4].

На підготовчому періоді на е-ЗМІ покладаються такі основні завдання щодо впливу на ма-

сову свідомість: формування стану «періодичної невдоволеності»; підготовка регіональної та світової точок зору на проблему; ведення агітації тощо. На основному – активізація масової свідомості; утримання суб'єктів впливу у «заданому» стані до «перемоги»; легітимізація інформаційних дій для внутрішньої та зовнішньої аудиторій; залякування протиборчої сторони з метою припинення аналогічних дій у відповідь тощо.

Основним завданням під час завершального періоду є легітимізація нових суб'єктів та об'єктів управління.

Визначальна роль е-ЗМІ обумовлено такими особливостями, як:

– відсутність обмежень на обсяги та зміст інформаційних повідомлень;

– можливість збереження анонімності;

– множина впливів (одна ідея може лавиноподібно розповсюджуватися за рахунок використання соціальних інтернет сервісів таких, як сайти спрямованого змісту, форуми, блоги, тощо);

– сильна кластеризація спільнот (розподіл груп за різними інтересами, темами);

– інтерактивність (надає суб'єктам впливу можливості живого спілкування);

– можливість використання неформальних лідерів;

– широкі можливості пошукових систем;

– використання довіри знайомих людей.

Наведені вище особливості характерні інформаційному протиборству, яке здійснюється з використанням соціальних мереж, для яких, окрім вказаного додаються власні властивості. Саме такі властивості створюють з них один з найпотужніших інструментів інформаційного протиборства.

Відомо [11], що у мережі всі агенти є вузлами складного неорієнтованого графу, що з'єднані між собою за допомогою ребер з різною вагою. Соціальна мережа є складною нелінійною системою, для якої характерна висока швидкість та надійність розповсюдження заданого контенту. Такі переваги соціальних мереж, як швидкий пошук необхідної інформації та однодумців, широке коло користувальницької аудиторії, можливість обговорення актуальних тем, призвели до того, що ці соціальні структури стали важливим інструментом для управління громадською думкою, а разом і з тим і «класичними» ЗМІ, що є характерною технологією на сучасному етапі.

Розповсюдження чуток «з вуст в уста» також є технологією інформаційного протиборства, але її особливістю на сучасному етапі є суттєва залежність від первинних джерел – «класичних» ЗМІ, е-ЗМІ, соціальних інтернет сервісів тощо.

Живучість та сприйняття чуток соціумом в значний мірі визначається тим, що вони є легкодоступним способом задоволення інформаційних потреб людини, тобто потреб в інформації необхідній для соціальної орієнтації та організації своєї поведінки. Емоційно негативні переживання супроводжують людину якщо у неї відсутня інформація про події, що відбуваються, тобто коли вона знаходиться в стані своєрідного «інформаційного дефіциту». Даний «інформаційний дефіцит» і сприяє нейтралізації чуток. Таким чином, людина суб'єктивно відчуває себе інформованою, але в той же час її поведінка об'єктивно починає потрапляти, в певній мірі, в залежність від конкретних чуток.

*За цільовою аудиторією (РА)* при виборі методів, способів та прийомів інформаційного впливу обов'язково необхідно враховувати характер цільової аудиторії. В першу чергу обов'язково слід враховувати віковий критерій (наприклад, молодь або люди пенсійного віку), соціальний статус аудиторії (різні мотиваційні цінності) та рівень обізнаності аудиторії.

Враховуючи наведені вище особливості інформаційного протиборства на сучасному етапі його базові технологічні аспекти можна подати у вигляді схеми (рис. 3).

Таким чином, після формування задуму і постановки завдань на здійснення інформаційного протиборства, на етапі планування, здійснюється вибір відповідних методів та здійснюється розподіл сил і засобів, які будуть використовуватись в подальшому на етапі реалізації. При цьому враховуються як відомі способи психологічного впливу та характер цільової аудиторії так і нові технологічні аспекти, сутність яких описано в статті.

На заключному етапі здійснюється оцінювання результатів та відповідне корегування задач, методів та засобів для досягнення поставленої мети. Всі розглянуті заходи проводяться постійно і безперервно на протязі усього періоду протистояння, так і певний час після його припинення.

**Висновки**. Таким чином, інформаційне протиборство на сучасному етапі розвитку високотехнологічного суспільства, як показано в статті, виступає одним з дієвих інструментів регулювання відносин в інформаційній сфері.

Високотехнологічні новації вносять суттєві корективи в усталені роками механізми інформаційного протиборства, тому встановлення нових

технологічних аспектів сприяє виробленню ефективних механізмів протидії деструктивним впливам і, як наслідок, сприяє підвищенню рівня інформаційної безпеки держави.

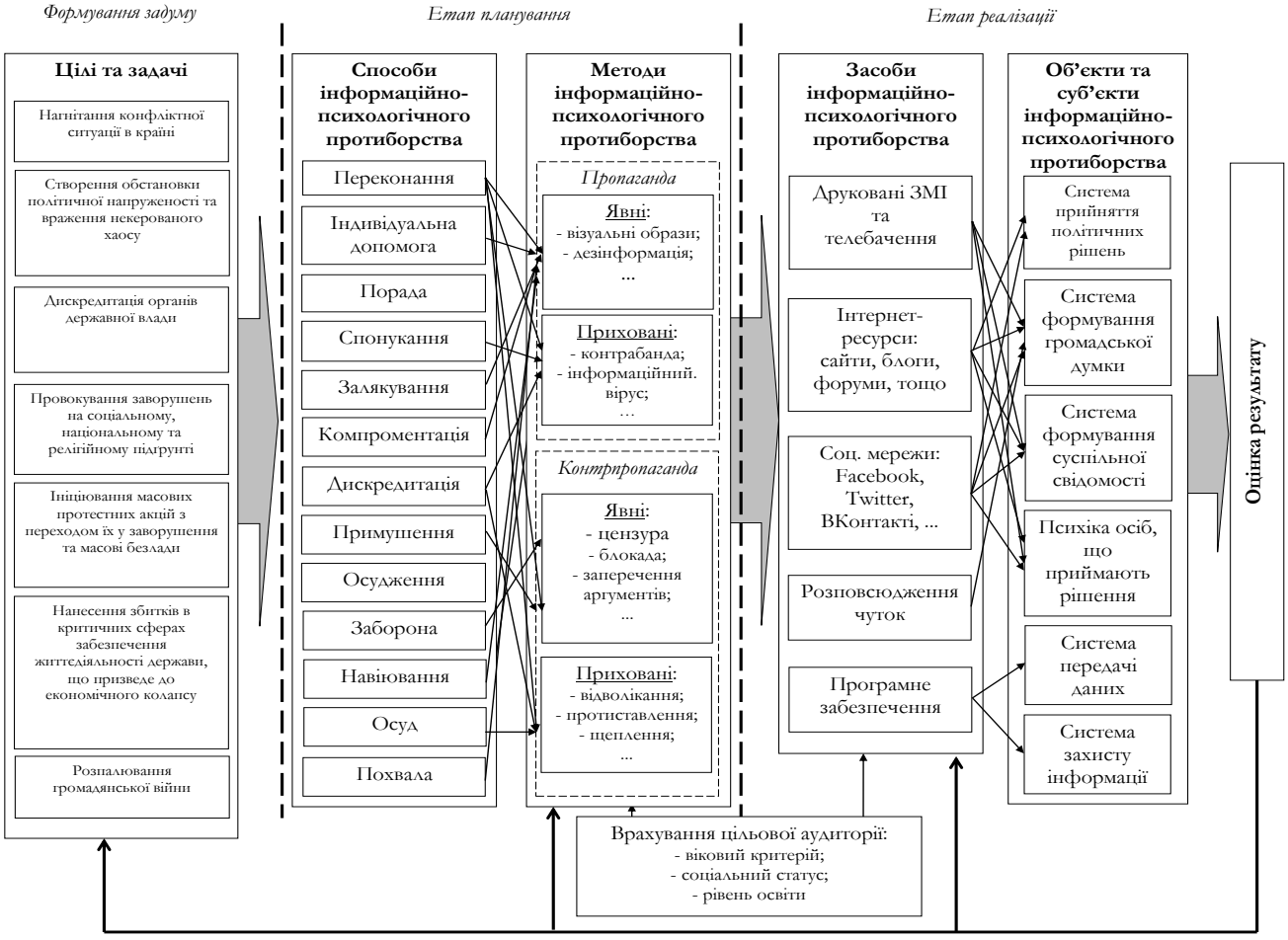


Рис. 3. Технологічні аспекти інформаційного протиборства на сучасному етапі

## ЛІТЕРАТУРА


[1]. Панарин И.Н. Информационная война и мировая политика / Панарин И.Н. – М., 2006. – 320 с.

[2]. Панарин И.Н. СМИ, пропаганда и информационные войны. / Панарин И.Н. – М.: Поколение, 2012 – 41 с.

[3]. Информационные войны в интернете. [Електронний ресурс] Режим доступу до статті: http://emirr.ru/emirr_articles/232-informacionnye-vojny-v-internete.html

[4]. Методы ведения информационных войн. [Електронний ресурс] / Григорьев М. – Режим доступу до статті: http://mcpt.narod.ru/pr_war.html#up

[5]. І. Гриненко, 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) вип., 2012 р.

[6]. Спосіб поширення інформації та запобігання поширення інформації в комп'ютерній мережі [Електронний ресурс] Режим доступу до статті: http://findpatent.com.ua/patent/240/2408145.html

[7]. Грищук Р.В. Синергія інформаційних та кібернетичних дій / Р.В.Грищук, Ю.Г. Даник // Труди університету. – К. : НУОУ, 2014. – № 6 (127). – С. 132–143.

[8]. Зелинский С. А. 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 / Зелинский С. А. – СПб.: СКИФИЯ, 2008. – 407 с.

[9]. Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства. / Д.А. Губанов, Д.А. Новіков, А.Г. Чхартишвили– М.: Физматлит, 2010. – 225 с.

[10]. Информационная безопасность государства в военной сфере : науч.-метод. Издание / [Быченок Н.Н., Дзюба Т.М., Рось А.А., Витковский В.В., Вищун В.В.]. – К.:НУОУ, 2012. – 264 с.

[11]. Welt C. After the Color Revolutions: Political Change and Democracy Promotion in Eurasia [Electronic resource] / [By ed. C. Welt, A. Schmemann]. – 2010. – Available from : https://www.gwu.edu/ ~ieresgwu/assets/docs/PONARS_Eurasia_After_the_Color_Revolutions.pdf.

[12]. Khondker H. H. Role of the New Media in the Arab Spring / H. H. Khondker // Globalizations. – 2011. – Vol. 8, No. 5. – Pp. 675 – 679.

## REFERENCES


[1]. Panarin I.N. Information War and World Politics, M., 2006., 320 p.

[2]. Panarin I.N. Media, propaganda and information war., M .: Generation, 2012, 41 p.

[3]. Information in the Internet wars. [Electron resource] mode to access ARTICLES: http://emirr.ru/emirr_articles/232-informacionnye-vojny-v-internete.html

[4]. Methods of information warfare. [Electron resource] / M. Grigoriev - Mode of access to articles: http://mcpt.narod.ru/pr_war.html#up

[5]. I. Grynenko, D. Prokofiev-Yanchylenko. The impact of virtual communities of information security: current situation and trends. The legal, regulatory and metrological support information security system in Ukraine, 1 (23) grad., 2012.

[6]. The method of the spread preventing of information and dissemination of information in a computer network [electronic resource] Access article: http://findpatent.com.ua/patent/240/2408145.html

[7]. Hryshchuk R.V. Synergy of information and cyber actions, Proceedings of the university., K: NUOU, 2014., № 6 (127)., P. 132-143.

[8]. Zelinsky SA Information and psychological impact on the public consciousness. The media of communication, information and Propaganda - as conductor of manipulative techniques impact on the subconscious and modeling behavior of the individual and the mass, Zelinsky SA - SPb .: Scythians, 2008., 407 p.

[9]. Gubanov DA Social Networks: Models of informational influence, management and confrontation., Gubanov DA, Novikov DA, Chkhartishvili AG, M.: FIZMATLIT, 2010., 225 p.

[10]. Information security of the state in the military sphere: scientific method. Edition, Bychenok NN, Dziuba TM, Ros AA, Witkowski VV, VV Vischun., K.: NUOU, 2012., 264 p.

[11]. Welt C. After the Color Revolutions: Political Change and Democracy Promotion in Eurasia [Electronic resource], [By ed. C. Welt, A. Schmemann]., 2010., Available from : https://www.gwu.edu/~ieresgwu/assets/docs/PONARS_Eurasia_After_the_Color_Revolutions.pdf.

[12]. Khondker H. H. Role of the New Media in the Arab Spring, Globalizations., 2011., Vol. 8, No. 5. PP. 675 – 679.


## ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОГО ПРОТИВОСТОЯНИЯ НА СОВРЕМЕННОМ ЭТАПЕ


В статье систематизированы известные методы и способы информационного противостояния на современном этапе и установлено его основные технологические аспекты. Показано, что основным инструментом информационного противостояния сегодня выступают социальные интернет сервисы. Доказано, что социальные интернет сервисы, наряду с классическими средствами информационного противостояния, используются субъектами информационной борьбы для ведения пропаганды и контрпропаганды.



**Ключевые слова:** информационное противоборство, технология, классификация, социальный интернет сервис.


## TECHNOLOGICAL ASPECTS OF INFORMATION WARFARE AT THE PRESENT STAGE


Known methods and techniques of information warfare at the present stage have been systematized and its main technological aspects have been established in the article. It has been shown that the main instrument of information warfare today are the social Internet services. It has been proved that the social Internet services, along with the classical means of information warfare, are used by agents of information struggle for conducting propaganda and counter-propaganda.



**Index terms**: information warfare, technology, classification, social Internet service.



**Грищук Руслан Валентинович**, доктор технічних наук, старший науковий співробітник, начальник науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П Корольова.
E-mail: Dr.Hry@i.ua

**Грищук Руслан Валентинович**, доктор технических наук, старший научный сотрудник, начальник научно-исследовательского отдела информационной и кибернетической безопасности научного центра Житомирского военного института имени С. П Королёва.

**Ruslan Hryshchuk,** Dr. of Techn. Sci., Senior Researcher, Chief of Scientific Research Department Information and Cybersecurity of Scientific Center of Zhytomyr Military Institute after S. P. Korolyov.

**Канкін Іван Олегович,** кандидат технічних наук, провідний науковий співробітник науково-дослідної лабораторії проблем забезпечення кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П Корольова.
E-mail: I_Kankin@ukr.net

**Канкин Иван Олегович**, кандидат технических наук, ведущий научный сотрудник научно-исследовательской лаборатории проблем кибернетической безопасности научного центра Житомирского военного института имени С. П Королёва.

**Ivan Kankin**, Ph.D., leading researcher of scientific research laboratory issues of information security of scientific center of Zhytomyr military institute after S. P. Korolyov.

**Охрімчук Володимир Васильович**, науковий співробітник науково-дослідної лабораторії проблем забезпечення кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П Корольова.
E-mail: Okhrimchuk84@ukr.net

**Охримчук Владимир Васильевич**, научный сотрудник научно-исследовательской лаборатории проблем кибернетической безопасности научного центра Житомирского военного института имени С. П Королёва.
**Vladimir Okhrimchuk**, research scientist of scientific research laboratory issues of cybersecurity of scientific center of Zhytomyr military institute after S. P. Korolyov.

**УДК 004.056.53:004.492.3 (045)**

# МЕТОД ОЦІНКИ РІВНЯ КРИТИЧНОСТІ ДЛЯ СИСТЕМ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ

***Анна Корченко, Валерій Козачок, Андрій Гізун***

*Вплив кризових ситуацій на стан захищеності державних інформаційних ресурсів, різноманітних установ, підприємств, організацій та державу в цілому є досить значним. Так, кризові ситуації здатні не лише загальмувати розвиток системи, що підпадає під її вплив, а й зруйнувати її взагалі. Для запобігання такого впливу необхідним є прийняття адекватних рівню загрози заходів та застосування засобів захисту, що визначає важливість оцінки критичності поточної ситуації. На даний час не існує загальноприйнятих універсальних критеріїв та інтегрованого показника оцінки рівня критичності. Тому визначення рівня критичності інциденту, що може спричиняти КС, є актуальною та важливою науковою задачею. В дослідженні введена множина параметрів оцінки рівня критичності ситуації, запропонований метод визначення рівня критичності з використання експертних підходів та методів нечіткої логіки, які не вимагають збирання та обробку статистичних даних, та описана процедура дефазифікації значення параметрів, на основі якої будується індикатор відображення рівня критичності.*

***Ключові слова:*** *кризова ситуація, інцидент, рівень критичності кризової ситуації, індикатор, множина критеріїв, оцінка рівня критичності, збитки, клас критичності, експертні методи, теорія нечітких множин.*

Захист державних інформаційних ресурсів (ДІР) від впливу кризових ситуацій (КС) та їх наслідків на даний час є чи не найбільш актуальною задачею у всій сфері інформаційної безпеки. Будь-які інциденти інформаційної безпеки мають свої причини, тобто дестабілізуючі чинники, що їх спричиняють і завжди створюють негативний вплив на процеси управління інформаційними ресурсами організації чи ДІР. Так, чисельні інциденти за умови відсутності контролю за їх протіканням та відповідної реакції можуть мати критичні наслідки. Відповідно до визначення КС, наведеного в [1], вона характеризується великими збитками, серйозними перериванням бізнес-процесів, що ставлять під сумнів можливість подальшого функціонування організації, руйнуванням структури окремого підприємства чи цілої галузі, потенційними загрозами життю та здоров'ю людей. Таким чином КС не тільки може порушити характеристики безпеки ДІР (конфіденційність, цілісність та доступність), а й порушити процеси управління ними, призвести до їх втрати. При цьому чим більший рівень критичності КС, тим тяжчі наслідки вона може мати і, зрозуміло, більш ефективними мають бути антикризові засоби та заходи. Тому для прийняття ефективних контрзаходів, максимальної ліквідації наслідків необхідним є визначення рівня критичності КС, породженої інцидентом-потенційною кризовою ситуацією (ІПКС), враховуючи динаміку її розвитку.

Процеси захисту інформаційних ресурсів в умовах впливу КС регламентуються концепцією управління безперервністю бізнесу (КУББ). Вона передбачає в собі моніторинг поточної ситуації, прогнозування КС, оцінку рівня критичності ситуації, прийняття контрзаходів та ліквідацію їх наслідків і в цілому відповідає етапам циклу Шухарта-Демінга або PDCA. Кожен з цих процесів має свої особливості і різну ступінь реалізації на практиці.

На даний момент питання визначення поняття КС, їх класифікації були розглянуті в роботах [1, 2], описані та розроблені методи та системи для прогнозування, ідентифікації аномального стану в інформаційно-комунікаційних системах та мережах (ІКСМ) [3, 4], діяльності порушників [5-9], комп'ютерних атак [10]. Питанням іденти-