УДК 004.02:004.056

DOI: 10.18372/2310-5461.38.12835

Р. В. Грищук, д-р техн. наук, старш. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0001-9985-8477
e-mail: Dr.Hry@i.ua;

Н. В. Лукова-Чуйко, канд. фіз.-мат. наук, доц.
Київський національний університет імені Тараса Шевченко
orcid.org/0000-0003-3224-4061
e-mail: lukova@ukr.net

О. В. Лагодний, ад'юнкт
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0002-0812-939X
e-mail: lov.82@ukr.net;

Г. Д. Носова**,** наук. співроб.
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0003-3573-9828
e-mail: nunya_13@i.ua

АВТОМАТИЗАЦІЯ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ У МЕРЕЖІ ІНТЕРНЕТ

Вступ

Особливості доступу до будь-якої інформації на сьогодні пов'язані зі стрімким розвитком інформаційно-комунікаційних технологій. Всесвітня мережа стає все більш потужним інструментом для формування громадської думки, підготовки до прийняття політичних, економічних і військових рішень. Сама інформація вже давно стала не тільки засобом розвитку, товаром та «валютою», а й способом впливу на різні галузі життєдіяльності суспільства, потужною зброєю масового ураження XXI ст. в руках обізнаних гравців.

Цілеспрямоване використання тієї чи іншої інформації у певних формах подання дозволяє здійснювати психологічний вплив (ПсВ) на об'єкти з метою формування бажаних ефектів з високим ступенем прихованості таких впливів. Мережа Інтернет стала ідеальним засобом доставки інформаційних загроз у форматі текстових, аудіо- або відео- повідомлень до будь-якого об'єкту впливу або цільової аудиторії. Самі інформаційні загрози, зазвичай визначаються як наміри, дії або явища, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її структурних органів). На рівні цільової аудиторії або об'єкту впливу (ОВ) метою таких дій є примушення робити те, про що вчора ще не задумувались. Наслідками такого впливу може стати виникнення кризових явищ у суспільстві.

Аналіз останніх досліджень і публікацій

Сьогодні стало очевидним істотне зростання ролі негативного інформаційного впливу у ході досягнення економічних, політичних, військових цілей. Водночас, активний розвиток інформаційних технологій привів до якісного розуміння ролі і місця ПсВ в системі забезпечення інформаційної та кібернетичної безпеки держави.

Узагальнивши результати досліджень [1–8] можна зробити висновки, що питання інформаційного протиборства, розроблення методів виявлення загроз та протидія їм залишається відкритим та актуальним.

Постановка завдання

Розвиток інформаційних технологій сприяє зростанню обсягу електронного документообігу, так за даними фахівців компанії International Data Corporation, яка спеціалізується в галузі інформаційних технологій, лише 2011 року обсяг світової інформації, розміщеної в мережі Інтернет склав понад 1,8 зетабайт (1,8 трлн Гб).

Щорічно ця цифра збільшується майже у два рази. За прогнозами на кінець 2020 року цей обсяг становитиме близько 42 зетабайтів рис. 1.

Така тенденція свідчить про зростання ресурсів, користувачів мережі Інтернет; розширення спектру їх можливостей щодо обміну інформацією, створення різнотипних зв'язків, що саме собою не містить негативних факторів, проте при-

зводить до зниження рівня захисту як самої інформації, яка циркулює у мережі, так і особистих даних користувачів, перетворюючи їх на об'єкти інформаційного впливу. Причому можливості здійснення такого впливу зростають майже пропорційно з можливостями самої мережі.

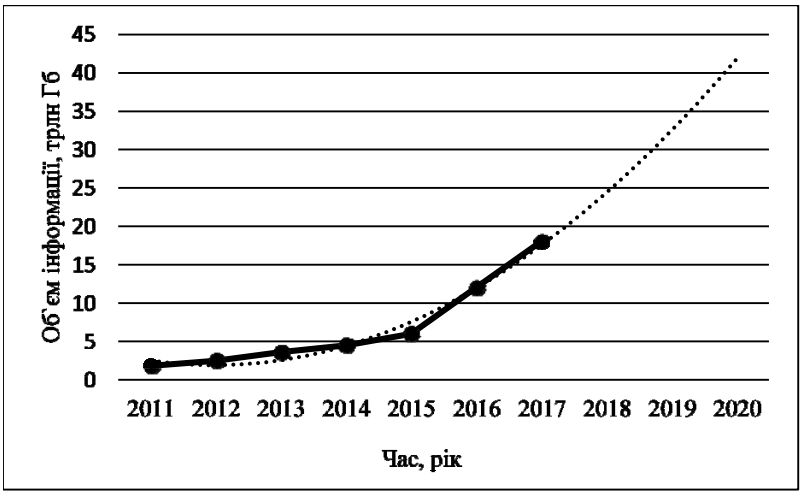

Рис. 1. Динаміка зростання розміщення світового обсягу інформації в мережі Інтернет

Виклад основного матеріалу

Об'єктом впливу може бути група осіб, а в окремих випадках і одна особа (керівник підприємства, держави), визначена для інформаційно-психологічного впливу.

Сам інформаційний вплив розглядається як організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан об'єктів впливу шляхом застосування інформаційних засобів і технологій [1; с. 13].

До того ж слід зауважити, що будь-яка особа, чи група осіб є потенційним джерелом інформаційних приводів, які, залежно від їх змісту, можуть знижувати стан національної безпеки держави: починаючи з дискредитації Міністерства оборони України і до витоку державної таємниці, що може провокувати виникнення конфліктних ситуацій як у середині країни, так і між країнами.

На прикладі соціальної мережі як нового типу соціальної структури суспільства можна дослідити загалом процес розповсюдження інформації через обмін повідомленнями, перш за все, між її користувачами, які вже мають встановлені зв'язки [7; с. 3], [9; с. 97], [10; с. 114].

Зв'язки в більшості соціальних мереж можна зобразити такими основними типами (рис. 2):

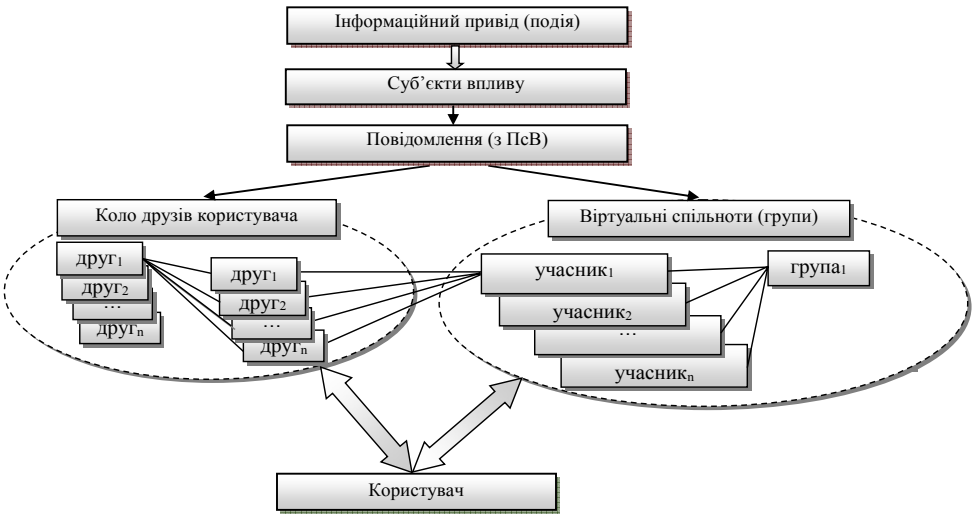

Рис. 2. Зв'язки у соціальних мережах

– безпосередні, набуті шляхом встановлення прямих контактів між користувачами мережі.

Сервіси соціальних мереж постійно поширюють можливості спілкування у колі прямих контактів за рахунок масового одночасного розсилання повідомлень різного змісту, приватного обміну даними;

– опосередковані, зумовлені можливістю практично вільного доступу до прямих контактів користувачів мережі, з якими встановлені безпосередні контакти. У соціальній мережі створені умови для розширення кола своїх прямих контактів за рахунок опосередкованих, залежно від зацікавленості об'єктів впливу;

– зв'язки між учасниками групи, які можливі за рахунок реалізованих у соціальних мережах механізмів об'єднання користувачів у групи (віртуальні спільноти). Адміністратор групи створює профіль групи, аналогічний профілю окремого користувача, та встановлює правила обміну інформацією у ній.

Така модель обміну інформацією між учасниками віртуальних спільнот описує соціальну систему Т. Парсонса, що відображає притаманні більшості соціальних мереж властивості [2; с. 417], такі як:

– ідентифікація — особисті відомості про ОВ. Під особистими відомостями доцільно розуміти будь-які дані, особисте розміщення яких дозволене умовами користування даною соціальною мережею (анкетні дані, дані у вигляді фото- чи відеоматеріалів та ін.);

– репутація — можливість ОВ формувати репутацію інших користувачів (стіна відгуків, система репутації);

– присутність — відкритий доступ до інформації про наявність ОВ у мережі в конкретний момент часу;

– відносини — відкритий доступ до інформації про прямі контакти ОВ (коло спілкування з зазначенням рівнів доступу для кожного з прямих контактів, ступінь доступу інших користувачів);

– діалоги — можливість відкритого або закритого спілкування як між прямими контактами, так і з будь-яким іншим користувачем або спільнотою;

– рейтинг — ступінь впливу дій ОВ на інших користувачів (наприклад, оцінка дій інших користувачів через систему «подобається/поділитися»).

За наведеним прикладом легко побачити що, впровадження негативних процесів навіть в окремому сегменті мережі Інтернет, яким є соціальні мережі, може спричинити критичні наслідки як для окремої групи осіб, частини суспільства, так і для держави в цілому.

Запроваджена в Доктрині інформаційної безпеки України [3; с. 4] серед національних інтересів держави в інформаційній сфері визначає безпечне функціонування і розвиток інформаційного простору та створення системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів. Отже, здійснення механізмів забезпечення інформаційної безпеки є пріоритетним напрямом діяльності на державному рівні. Причому невпинне зростання можливостей здійснення негативного ПсВ потребує підвищення якості їх виявлення шляхом розробки нових або вдосконалення відомих методів.

Під інформаційною безпекою будемо розуміти такий стан захищеності людини, суспільства і держави, за якого забезпечується адекватне світосприйняття особистістю інформації з різноманітних джерел, що досягається своєчасним виявленням та прогнозуванням розвитку інформаційних загроз.

Загроза — явище, чинник (їх сукупність), що здатні реально створити умови або стати причиною повної або часткової неможливої 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.

Перед фахівцями з питань інформаційної безпеки постає складне завдання моніторингу мережі Інтернет в умовах неможливості фізично осягнути весь об'єм, що циркулює в ній, для пошуку загроз визначеним ОВ. Практично єдиним способом розв'язання цієї проблеми є застосування формальних методів опрацювання текстів, здатних автоматизувати частину необхідних виробничих операцій, наприклад пошуку та фільтрації певних текстових повідомлень. Проте машинна обробка текстової інформації супроводжується низкою специфічних труднощів, пов'язаних, у першу чергу з вирішенням семантико-залежних задач аналізу і синтезу природномовного контенту. Недостатній рівень розуміння природної мови в сучасних засобах комп'ютерної лінгвістики складає основну перепону для розпізнавання таких типів повідомлень, де зміст зазвичай передається інваріантними мовними структурами або навмисно завуальовується [4; с. 51].

Для фахівця виявлення прихованого змісту повідомлення не є надскладною задачею, проте модерація відповідальними особами потужного мовного потоку обмежена порівняно невеликою швидкістю сприйняття тексту.

Виявлення ознак інформаційних загроз об'єктам впливу

Особливістю ознак інформаційних загроз (ІЗ) є поява тенденції до багаторазового стійкого повторювання в джерелах загроз тестового повідомлення обраної тематики, яка направлена на дискредитацію визначених ОВ.

Виявити ознаки загроз — це виявити наявність відповідних тенденцій, які пов'язані з їх формуванням, з метою попереджання виникнення кризових ситуацій у суспільстві.

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 багатокритерійний 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. 3): об'єкта й суб'єкта впливу, зв'язку між ними в кібернетичному просторі (КП), де відбувається даний процес.

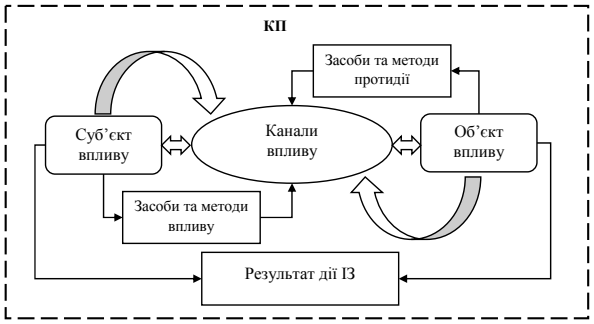

Рис. 3. Основні складові системи кібернетичного простору

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-мережевий та соціотехнічний простори [1; с. 10].

Тож метод виявлення ІЗ за даними з мережі Інтернет повинен враховувати ефективність джерела загрози щодо доцільності його моніторингу та ознаки загрози ОВ в текстовому повідомленні.

Інформаційна загроза може проявлятися в різних формах інформації, тому слід враховувати методи і форми ПсВ (рис. 4).

Протидія відомим формам і методам ПсВ займає важливе місце в системі забезпечення інформаційної безпеки держави та включає в себе комплекс заходів щодо запобігання виникненню кризових ситуацій (рис. 5).

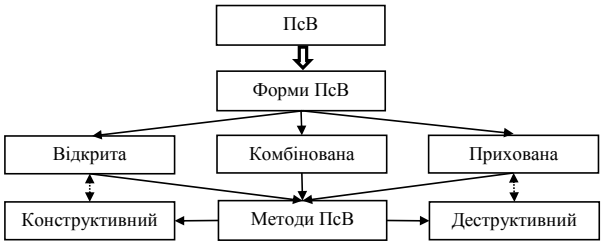

Рис. 4. Методи і форми ПсВ

Рис. 5. Порядок застосування протидії ІЗ

Саме своєчасність виявлення і прогнозування подальшого розвитку ІЗ дозволить ефективно протидіяти цим методам і формам ПсВ.

Автоматизація процесу застосування методів виявлення загроз

Розроблений метод виявлення ІЗ складається з таких кроків.

Крок 1. Вибір джерела загрози та визначення його ефективності. Для формалізації параметрів та визначення критеріїв оцінювання пропонується обирати інформаційні агентства відкритих джерел інформації мережі Інтернет, де за основний критерій ефективності джерела прийнято середню кількість публікацій кожного інформаційного агентства за добу. Наведені у табл. 1. джерела моніторингу відібрані з українського і російського сегменту з метою проведення аналізу та виявлення ознак загроз.

Крок 2. Оцінювання ефективності джерела моніторингу проводиться відповідно розробленої математичної моделі багатокритерійного оцінювання ефективності джерел загроз. Для формування параметрів обраних джерел моніторингу дані пропонується отримувати з таких сервісів мережі Інтернет: WebPagetest, Pingdom, Cy-Pr.com, Pr-Cy.ru. WebPagetest – сервісів зі схожими можливостями щодо аналізу швидкості завантаження сторінки, можливістю отримання даних про регіон, домен та рейтинг сайту, «індекс цитування», оцінювання продуктивності відповідно до Google PageSpeed вимог.

Після отримання даних для обраних джерел моніторингу проводиться розрахунок ефективності джерел загроз за допомогою розробленого програмного додатку SiteEvaluation_1.0 (рис. 6).

Таблиця 1

Джерела моніторингу для виявлення ознак загроз

№ з/п	Назва інформаційного агентства, *m*	Електронна адреса інформаційного агентства	Середня кількість публікацій інформаційного агентства за день, *N*
1	Обозреватель	https://www.obozrevatel.com/	235
2	Інтерфакс-Україна	http://interfax.com.ua/	150
3	Сьогодні	https://www.segodnya.ua/	250
4	Головне	https://glavnoe.ua/	120
5	Укрінформ	https://www.ukrinform.ua/	145
6	Вести	https://vesti-ukr.com/	125
7	Цензор	https://censor.net.ua/	170
8	РБК-Україна	https://www.rbc.ua/	160
9	УНІАН	https://www.unian.net/	215
10	ТАСС	http://tass.ru/	100
11	Интерфакс-Россия	http://www.interfax-russia.ru/	130
12	Сегодня	http://www.segodnia.ru/	170
13	Московский комсомолец	http://www.mk.ru/	140
14	Вести	https://www.vesti.ru/	250
15	Ведомости	https://www.vedomosti.ru/	215
16	Коммерсант	https://www.kommersant.ru/	135
17	Первый канал	https://www.1tv.ru/	220
18	Лента	https://lenta.ru/	155
19	РИА	https://ria.ru/	650
20	Русская весна	http://rusvesna.su/	80

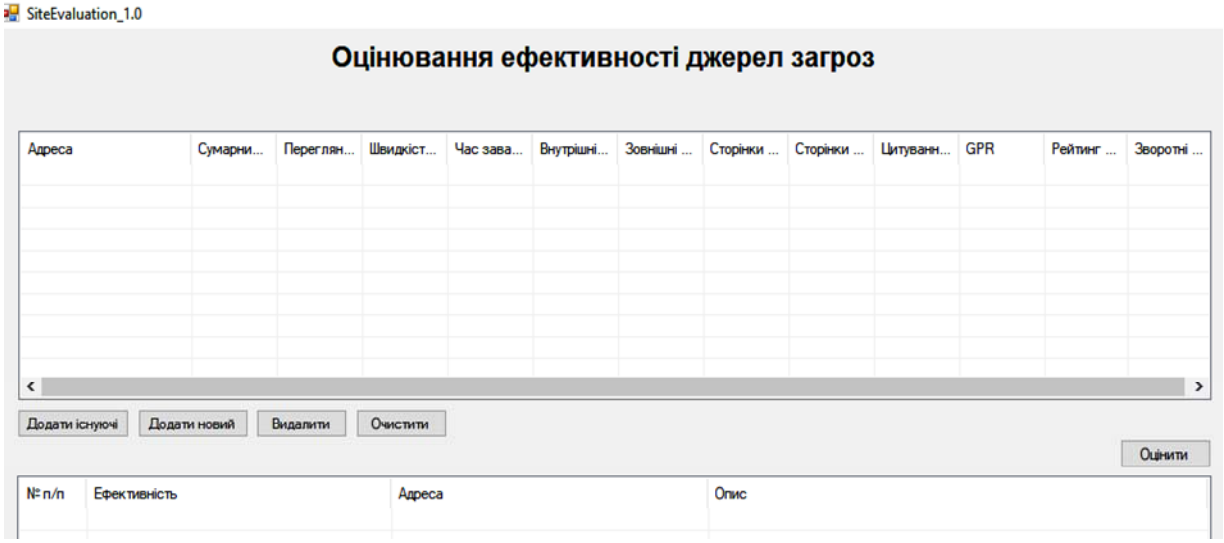

Рис. 6. Вигляд головного вікна програмного додатку SiteEvaluation_1.0

На наступному кроці здійснюється вибір теми новини для моніторингу, виходячи з попереднього аналізу визначених джерел та ОВ.

Сам моніторинг оціненого джерела загрози за тематичним контентом та збір статистичних даних виконується за допомогою розробленого програмного забезпечення Way_to_victory_1.0., призначеного для моніторингу блогів, форумів, сайтів соціальних мереж, інформаційні агентства відкритих джерел інформації мережі Інтернет, новинних сайтів з метою виявлення текстових повідомлень з ознаками загроз на визначені ОВ держави, що є вихідними даними для проведення статистичного аналізу з метою прогнозування їх подальшого розвитку [11; с. 3].

Такий підхід з комплексним застосуванням розробленого програмного забезпечення та покроковою обробкою виділеного обсягу інформації за рахунок автоматизації процесу дозволяє оперативно отримувати результат з максимально можливою повнотою охоплення текстових повідомлень, оприлюднених на обраних ресурсах мережі Інтернет за визначеною тематикою та ОВ (або тієї частини суспільства, моніторинг якої на

даний момент є першочерговим). Крім того, систематизація отриманих текстових повідомлень та структуризація результатів їх обробки дозволяє створити інструменти для їх сукупної обробки, що у свою чергу підвищує якість виявлення окремих текстових повідомлень з ознаками загроз визначеним ОВ.

Одна ітерація робочого циклу (однієї сесії пошуку) Way_to_victory_1.0 містить:

– завантаження першого джерела загроз для пошуку;

– пошук усіх посилань з цього джерела загроз на інші сторінки;

– завантаження сторінки для першого знайденого посилання;

– безпосередній пошук у завантаженій сторінці шуканих слів, словосполучень і акумулювання кількості знайдених фраз для кожної пошукової фрази; занесення даних до таблиці бази даних;

– повтор двох попередніх кроків для всіх інших знайдених посилань;

– після закінчення пошуку по всіх знайдених посиланнях завантаження наступного сайту і повторення кроків 2–5.

– виведення результатів для поточної сесії у журнал, нанесення результатів на графік, запис результатів у таблиці бази даних.

Початок наступної сесії відбувається автоматично через заданий інтервал часу.

Після здійснення процедури класифікації отриманих статистичних даних та визначення ознак загроз в текстових повідомленнях формуються коди текстових повідомлень з ознаками деструктивного ПсВ на визначені ОВ, що дозволяє спростити опис його змісту для проведення каталогізації та архівації інформації для більш зручного пошуку її в базі даних.

Приклад отриманого кількісного представлення текстових повідомлень наведено у табл. 2.

Таблиця 2

Кількісне представлення виявлених ознак загроз в текстових повідомленнях визначеній ЦА

КОД 1		КОД 2		КОД 3		КОД 4	
Дата, день *t*	Кількість, *y*	Дата, день *t*	Кількість, *t*	Дата, день *t*	Кількість, *t*	Дата, день *t*	Кількість, *t*
26.10.14	5	03.05.15	7	07.01.16	1	19.12.17	11
27.10.14	7	04.05.15	4	08.01.16	6	20.12.17	2
28.10.14	13	05.05.15	5	09.01.16	4	21.12.17	7
29.10.14	11	06.06.15	6	10.01.16	2	22.12.17	11
30.10.14	5	07.05.15	6	11.01.16	3	23.12.17	14
31.10.14	10	08.05.15	5	12.01.16	5	24.12.17	11
01.11.14	13	09.05.15	4	13.01.16	4	25.12.17	6
02.11.14	13	10.05.15	1	14.01.16	7	26.12.17	11
–	–	11.05.15	2	15.01.16	2	27.12.17	11
–	–	12.05.15	1	16.01.16	1	28.12.17	6
–	–	13.05.15	6	17.01.16	7	29.12.17	11
–	–	14.05.15	4	18.01.16	5	30.12.17	11
–	–	15.05.15	7	19.01.17	7	–	–
–	–	16.05.15	1	20.01.17	2	–	–
–	–	17.05.15	8	21.01.16	4	–	–
–	–	18.05.15	7	22.01.16	9	–	–
–	–	19.05.15	4	–	–	–	–
–	–	20.05.15	1	–	–	–	–
–	–	21.05.15	4	–	–	–	–
–	–	22.05.15	3	–	–	–	–

Отримані дані є вихідними для проведення необхідних математичних розрахунків.

Висновки

Запропонований підхід спрямований на реалізацію автоматизації процесу аналізу визначеного сегменту джерел інформації у мережі Інтернет, виявлення джерел інформаційних загроз, урахування ефективності джерела загрози щодо доцільності його моніторингу, оцінювання рівня деструктивного ПсВ на визначених користувачів мережі, що у свою чергу дозволить підвищити оперативність попереджання негативних впливів та запровадження протидії ним.

Перспективи подальших досліджень мають бути спрямовані на оптимізацію практичної реалізації запропонованого підходу, більш гнучкого підходу до врахування кількісних та якісних характеристик окремих інформаційних приводів під час оцінювання рівня загроз.

ЛІТЕРАТУРА

1. ВСТУ 01.004.004 Видання 1. Воєнна політика безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення. Київ, 2014. 22 с. (Інформація та документація).

2. **Парсон Т. О.** социальных системах / под ред. В. Ф. Чесноковой и С. А. Белановского / Т. О. Парсон. — М., 2002. — 832 с.

3. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». — К., 2017. — 10 с. (Закони України).

4. **Расторгуев С. П.** Информационные операции в сети Интернет / под общ. ред. А. Б. Михайловского / С. П. Расторгуев, М. В. Литвиненко. — М., 2014. — 128 с.

5. **Грищук Р. В.** Диференціально-ігрові моделі та методи моделювання процесів кібернападу / Р. В. Грищук // дис. доктора техн. наук: 21.05.01. — К., 2013. — 411 с.

6. **Додонов В. О.** Інформаційні технології аналізу та виявлення інформаційного впливу в соціальних мережах на основі мультиагентних моделей розповсюдження інформації / В. О. Додонов // дис. канд. техн. наук: 05.13.06. Київ, 2017. — 143 с.

7. **Дзюндзюк В. Б.** Віртуальні співтовариства: потенційна загроза для національної безпеки. Київ, 2011, № 1. URL: http://nbuv.gov.ua/j-pdf/DeBu_2011_1_4.pdf.

8. **Грищук Р. В.** Основи кібернетичної безпеки / Р. В. Грищук, Ю. Г. Данник // монографія за заг. ред. проф. Ю. Г. Даника. Житомир, 2016. — 636 с.

9. **Горбулін В. П.** Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін та ін. — К., 2009. — 163 с.

10. **Губанов Д. А.** Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили. — М., 2010. — 228 с.

11. **Лагодний О. В.** Статистичний аналіз активності тематичного контенту в мережі Інтернет для прогнозування розвитку інформаційних загроз [Електронний ресурс] / О. В. Лагодний, О. О. Писарчук, Ю. І. Міхєєв // Traektoriâ Nauki = Path of Science. – 2017. – Vol. 3, No. 8. – P. 3011–3019. — Режим доступу. : http://pathofscience.org/index. php/ps/article/view/376. – ISSN 2413-9009, doi: 10.22178/pos.25-2.

Грищук Р. В., Лагодний О. В., Носова Г. Д., Лукова-Чуйко Н. В.

АВТОМАТИЗАЦІЯ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ У МЕРЕЖІ ІНТЕРНЕТ

У роботі розглянуто передумови необхідності виявлення інформаційних загроз у визначеному сегменті мережі Інтернет об'єктам впливу, проведено аналіз особливостей організації інформації у мережі, обґрунтовано необхідність активного впровадження автоматизації цих процесів у сучасних умовах. На сьогодні мережа Інтернет стала ідеальним засобом доставки інформаційних загроз у форматі текстових, аудіо- або відео повідомлень до будь-якого об'єкту впливу або цільової аудиторії. Використання інформації у певних формах подання дозволяє здійснювати психологічний вплив на об'єкти з метою формування бажаних ефектів з високим ступенем прихованості таких впливів. Для подальших досліджень проведено аналіз моделі обміну інформацією між користувачами мережі Інтернет на прикладі соціальних мереж. Обґрунтовано вразливість цього процесу до впровадження негативних впливів на об'єкти впливу. Запропоновано впровадження автоматизованого процесу аналізу відкритих джерел інформації з метою виявлення деструктивного психологічного впливу на визначені об'єкти. Виділено ключові проблеми вирішення питання моніторингу мережі Інтернет з метою виявлення негативних інформаційних впливів. На основі проведених досліджень запропоновано підхід до виявлення ознак інформаційних загроз об'єктам впливу. Визначено основні вимоги до розробленого методу їх виявлення за результатами моніторингу. Розроблено покроковий метод виявлення інформаційних загроз. У роботі подано стислий опис дій на кожному кроці виконання процесу виявлення негативних впливів на визначені об'єкти. Запропоновано підхід з комплексним застосуванням розробленого програмного забезпечення та покроковою обробкою виділеного обсягу інформації.

Ключові слова: об'єкт впливу; інформаційні загрози; психологічний вплив; відкриті джерела.

Hryshchuk R. V., Lahodniy O. V., Nosova H. D., Lukova-Chuiko N. V.

AUTOMATION IDENTIFY AND COUNTER THREATS TO INFORMATION ON THE INTERNET

Pre-conditions of necessity of exposure of informative threats are in-process considered in the certain segment of network the Internet the objects of influence, the analysis of features of organization of information is conducted in a network, grounded necessity of active introduction of automation of these processes for modern terms. For today network the Internet became the ideal mean of delivery of informative threats in the format of phototypograph audio- or video of reports to any object of influence or having a special purpose audience. the use of information in the certain forms of presentation allows to carry out psychological influence on objects with the purpose of forming of the desired effects with the high degree to reserve of such influences. The analysis of model of exchange information is conducted between the users of network the Internet on the example of social networks for subsequent researches. Grounded im-

pressionability of this process is to introduction of negative influences on the objects of influence. Introduction of the automated process of analysis of the opened information generators is offered with the purpose of exposure of destructive psychological influence on certain objects. There are selected the key problems of decision of question of monitoring of the Internet with the purpose of exposure of negative informative influences On the basis of the conducted researches offered approach to the exposure of signs of informative threats the objects of influence. Certainly the basic requirements are to the developed method of their exposure as a result of monitoring. The step-by-step method of exposure of informative threats is developed. The compressed description of actions at every step of implementation of process of exposure of negative influences is in-process given on certain objects. Offered approach with complex application of the developed software and step-by-step treatment of the selected volume of information.

Keywords: object of influence, information threats, psychological influence, open sources of information.

Грыщук Р. В., Лагодный А. В., Носова А. Д., Лукова-Чуйко Н. В.

АВТОМАТИЗАЦИЯ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ УГРОЗАМ В СЕТИ ИНТЕРНЕТ

В работе рассмотрены предпосылки необходимости выявления информационных угроз в определенном сегменте сети Интернет объектам воздействия, проведен анализ особенностей организации информации в сети, обоснована необходимость активного внедрения автоматизации этих процессов в современных условиях. На сегодня сеть Интернет стала идеальным средством доставки информационных угроз в формате текстовых, аудио- или видео сообщений к любому объекту воздействия или целевой аудитории. Использование информации в определенных формах представления позволяет осуществлять психологическое воздействие на объекты с целью формирования желаемых эффектов с высокой степенью скрытности таких воздействий. Для дальнейших исследований проведен анализ модели обмена информацией между пользователями сети Интернет на примере социальных сетей. Обоснованно уязвимость этого процесса к внедрению негативных воздействий на объекты воздействия. Предложено внедрение автоматизированного процесса анализа открытых источников информации с целью выявления деструктивного психологического воздействия на определенные объекты. Выделены ключевые проблемы решения вопроса мониторинга сети Интернет с целью выявления негативных информационных воздействий. На основе проведенных исследований предложен подход к выявлению признаков информационных угроз объектам воздействия. Определены основные требования к разработанного метода их выявления по результатам мониторинга. Разработан пошаговый метод выявления информационных угроз. В работе представлены краткое описание действий на каждом шагу выполнения процесса выявления негативных воздействий на определенные объекты. Предложен подход с комплексным применением разработанного программного обеспечения пошаговой обработкой выделенного объема информации.

Ключевые слова: объект влияния; информационные угрозы; психологическое воздействие; открытые источники.

Стаття надійшла до редакції 21.05.2018 р.
Прийнято до друку 04.06.2018 р.
Рецензент — д-р техн. наук, доц. Заїка В. Ф.