УДК 004.056:004.738.5(045) **Р.В. Грищук, К.В. Молодецька-Гринчук**

ПОСТАНОВКА ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

На сучасному етапі розвитку інформаційного суспільства соціальні інтернет-сервіси перетворилися не тільки на ефективний засіб комунікації, але й представляють собою дієвий інструмент впливу на суспільні й політичні процеси у державі. В умовах глобалізації інформаційного простору і гібридизації воєнних конфліктів соціальні інтернет-сервіси є джерелом загроз інформаційній безпеці держави. Тому підвищення рівня інформаційної безпеки України при використанні її громадянами СІС залишається однією із нагальних проблем, що потребують свого вирішення. В статті виконано формалізацію проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах і визначено перспективні напрямки досліджень. Отримані результати можуть використовуватися для розв'язку частинних задач у рамках вирішення проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах.

Ключові слова: Соціальний інтернет-сервіс, актор, інформаційна безпека держави, загрози, методологія.

Постановка проблеми

Наслідками інтенсивного розвитку інформаційних технологій у світі та Україні є поглиблення інформатизації сучасного суспільства та активізація глобалізаційних процесів [1]. Такі трансформації знайшли своє відображення й в системі стратегічних комунікацій суспільства, провідне місце в якій сьогодні відводиться соціальним інтернет-сервісам (СІС). СІС надають користувачам, яких називають акторами, засоби для обміну контентом різного типу, встановлення взаємозв'язків з іншими акторами і віртуальними спільнотами, інструменти для самовираження тощо [2].

У результаті інтенсивного зростання популярності СІС в сучасному інформаційному суспільстві, вони поєднали всі сфери людської діяльності. В умовах сьогодення СІС перетворилися на засіб залучення грошових, інформаційних, людських та інших ресурсів у національну економіку для забезпечення її сталого зростання [3]. Так, СІС використовуються для професійних комунікацій і фахового розвитку акторів, реалізації бізнес-проектів, покращення результатів економічної діяльності тощо [2]. З іншого боку, СІС представляють собою дієвий інструмент для розвитку громадянського суспільства. Таким чином, СІС є невід'ємною частиною національного інформаційного простору держави [4, 5], забезпечує створення контенту у мережі Інтернет, його зберігання, поширення та інформаційну взаємодію акторів з метою задоволення їх інформаційних потреб і впливає на ефективність суспільної діяльності.

В світлі останніх подій, СІС перетворилися на джерело загроз інформаційній безпеці держави (ІБД) [6, 7], оскільки поширення у СІС недостовірного, неповного чи упередженого контенту у поєднанні з технологіями інформаційно-психологічного впливу на індивідуальну, колективну і масову свідомість може мати наслідком прояв у суспільстві соціальної напруженості, міжнаціональної ворожнечі, протестних настроїв, незадоволення існуючою системою управління в державі тощо. Досвід збройної агресії Російської Федерації проти України вперше продемонстрував, що СІС є одним з ефективних інструментів ведення нової форми протистояння – гібридної війни. Отже, комплексний характер загроз ІБД у СІС потребує розроблення нових ефективних підходів до протидії, що є актуальним теоретико-прикладним завданням.

Аналіз останніх досліджень і публікацій показав, що незважаючи на постійно зростаючу кількість публікацій, присвячених віртуальним спільнотам, проблема забезпечення ІБД у СІС залишається невирішеною. У свою чергу, з цією проблемою пов'язані питання [8, 9] щодо виявлення і оцінювання загроз життєво важливим інтересам особистості, суспільства та держави у СІС; розроблення нових підходів і комплексу заходів із протидії загрозам у СІС; розроблення цілісної методології побудови системи забезпечення інформаційної безпеки держави у СІС тощо.

Публікації [10–13] продемонстрували, що загрози у СІС носять комплексний характер, а їх кількість постійно збільшується. Встановлено, що загрози ІБД у СІС відрізняються за

масштабністю, способом впливу на акторів, частотою повторюваності тощо [5, 9]. Тому сучасні загрози є складноформалізованими сутностями, характеризуються різними ознаками прояву як в окремих, так і у різних видах СІС. Внаслідок відсутності узагальнених ознак загроз інформаційній безпеці держави у СІС, розвитку технологій прихованого впливу на акторів, ускладнюються й процеси їх детектування. Тому ***виявлення і оцінювання ознак загроз*** є проблемою на шляху побудови дієвої системи забезпечення ІБД у СІС. Поряд з тим з праць [14, 15] відомо, що СІС належать до класу складних нелінійних динамічних систем. Однією з властивостей таких соціотехнічних систем є перехід до хаотичної динаміки у результаті дії на них збурень. Отже, наслідком реалізації загроз ІБД у СІС може бути перехід віртуальних спільнот акторів до некерованого стану і непередбачуваність їх поведінки в реальному житті. Тому нині особливо гостро стоїть проблема розроблення комплексу заходів для завчасної та ефективної ***протидії загрозам інформаційній безпеці держави у СІС***.

Забезпечення визначеного (бажаного) стану інформаційної безпеки держави у віртуальних спільнотах, відповідно до чинної Доктрини інформаційної безпеки України [6] та проекту Концепції інформаційної безпеки України [5], вимагає створення системи захисту інформаційного простору в СІС. Дослідження [8, 16, 17] показали, що система забезпечення ІБД представляє собою складову системи забезпечення національної безпеки держави з одного боку і складається з відомчих підсистем для вирішення окремих завдань з іншого. Встановлено, що в умовах зростання рівня загроз у державі ***відсутня науково обґрунтована методологія побудови системи забезпечення ІБД у СІС***. Аналіз показав, що існуючі засоби і відомчі підсистеми недостатньо забезпечені інструментарієм виявлення загроз ІБД у СІС, а протидія здійснюється із затримкою [18]. Внаслідок недостатнього рівня захисту інформаційного простору СІС від загроз держава, її суспільство і окремі громадяни перетворилися на суб'єкти деструктивних зовнішніх та внутрішніх інформаційних впливів.

Таким чином, узагальнюючи проведений аналіз літературних джерел, можна зробити висновок, що проблема створення та впровадження системи забезпечення інформаційної безпеки держави у СІС є актуальною і потребує свого вирішення.

Мета статті полягає у формуванні необхідних і достатніх умов для створення принципово нової методології побудови системи забезпечення інформаційної безпеки держави у СІС для вчасної ефективної протидії внутрішнім і зовнішнім загрозам національним інтересам України в інформаційній сфері.

Для досягнення поставленої мети сформульовано наступні частинні завдання:

проаналізувати роль і місце СІС в процесі забезпечення ІБД;

визначити підходи до виявлення і оцінювання ознак загроз у СІС;

встановити перспективні напрямки протидії загрозам ІБД у СІС;

формалізувати вимоги до систем забезпечення ІБД у СІС.

Аналіз ролі і місця СІС в процесі забезпечення ІБД

Відомо [19], що в основу функціонування усіх СІС покладено феномен соціальної мережевої комунікації. При цьому актори в СІС є вузлами зв'язку, а відношення між ними – каналами передачі інформації. Таким чином, віртуальна спільнота акторів у СІС представляє собою систему вузлів, зв'язаних між собою каналами передачі інформації. Можна припустити, що зв'язки між акторами є горизонтальними, тому усі вузли СІС є рівноправними. Оскільки актори можуть встановлювати зв'язки з іншими акторами або віртуальними спільнотами, то можна стверджувати про розподілений характер зв'язків між вузлами. У загальному вигляді взаємодія акторів у СІС подана на рис. 1.

На рис. 1 актори позначені кружками, а відповідні взаємозв'язки між ними – лініями. У свою чергу, актори можуть об'єднуватися у віртуальні спільноти BC_i, $i=\overline{1,n}$. Аналіз принципів організації взаємодії акторів у СІС (див. рис. 1) дозволяє зробити такий висновок: актори, об'єднавшись у віртуальні спільноти в СІС суттєво пришвидшують обмін інформацією, яка після її сприйняття свідомістю акторів відображується у вигляді зміни їх поведінки у реальному житті.

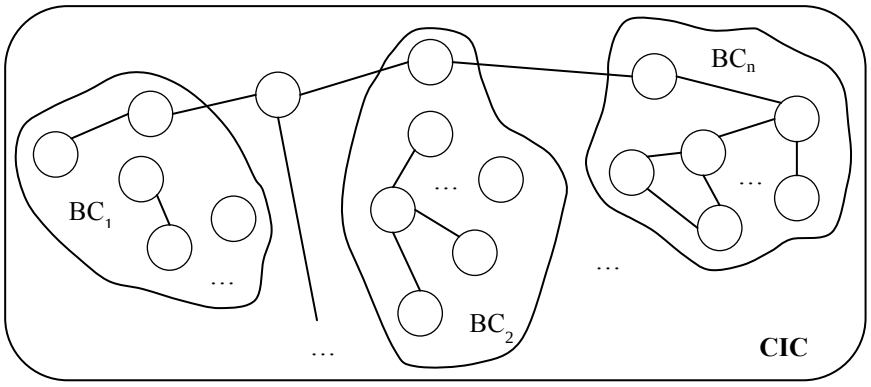


Рис. 1. Принцип організації взаємодії акторів у СІС

Світовий і вітчизняний досвід показали, що СІС пов'язані з появою нових викликів інформаційній безпеці людини, суспільства, держави. Перші згадки про використання СІС для впливу на владу пов'язані з протестами молоді проти результатів парламентських виборів у Молдові у квітні 2009 р. Суттєва відмінність даних соціальних опитувань від офіційно оголошених результатів виборів вивела на вулиці Кишиніва тисячі людей. Для поширення закликів до участі у мітингах використовувалися *Facebook* і *Twitter*, зокрема під геш-тегом *#pman* (Пяца Марій Адунерь Націонале – головна площа Кишиніва) у *Twitter* актори публікували новини про розвиток подій [11, 20, 21]. Таким чином, координація дій протестувальників виконувалася засобами СІС. Для цього публікувалися заклики до об'єднання опозиції, інформація про дії правоохоронних органів, стан і кількість постраждалих у сутичках з поліцією, дані про місця проведення акцій тощо. Після блокування владою стільникового зв'язку протестувальники використовували мобільний інтернет для взаємодії та публікації контенту в СІС. При цьому частина повідомлень публікувалася англійською мовою для широкого висвітлення в зарубіжних ЗМІ. Одночасно поширювалися відеозаписи подій в *YouTube* [20]. У результаті ці події отримали назву «*Twitter*-революція» за провідну роль мікроблогу в організації протестів.

Аналогічні події мали місце в Ірані у червні 2009 р. і пов'язані з протестами проти результатів президентських виборів. У відповідь на погроми і підпали протестуючими будівель державних установ у Тегерані влада ввела сурову інформаційну блокаду та проводила поліцейські рейди. Для цього було заблоковано стільниковий зв'язок, більшість СІС, зарубіжні радіостанції. При цьому державні ЗМІ висвітлювали виключно безлади на вулицях. Протестувальники використовували для комунікації мобільний інтернет і *Twitter*, за допомогою якого обмінювалися фото- та відеоматеріалами, інформацією про нові акції, списками заарештованих, даними про переміщення поліцейських тощо [11, 20]. З метою протидії представники влади Ірану під виглядом опозиціонерів публікували недостовірний контент у *Twitter*. У свою чергу, протестувальники поширювали рекомендації з виявлення таких агентів влади і приховування своїх персональних даних у СІС. Також у *Twitter* поширювали посилання на застосунок для організації *DDoS*-атак на державні інформаційні ресурси.

У грудні 2010 р. у Тунісі розгорнулися революційні події, пов'язані з незадоволенням громадян політикою президента. Особливістю цих революційних подій стало їх активне висвітлення у СІС *Facebook* і *Twitter* [21, 22]. Протестувальники ефективно використовували комунікаційні переваги СІС для координації своїх дій, обміну інформацією про протести в різних містах і безпечні напрямки пересування, публікації фото- й відеоматеріалів подій [22]. У результаті СІС перетворилися на незалежні ЗМІ для публікації новин і висвітлення інцидентів у Тунісі. Слід відмітити, що інформування світового співтовариства за умов ігнорування подій державними ЗМІ відбувалося також через СІС. Наслідком хвилі загальнонаціональних протестів стали відставка президента і зміна уряду.

Розглянуті події у Тунісі стали початком серії масових протестів громадян, революцій і внутрішніх військових конфліктів у країнах Північної Африки й Близького Сходу та отримали назву «арабська весна». Результатами протестного руху в Лівані, Йордані, Омані,

Єгипті, Ємені, Бахрейні, Лівії, Кувейті, Марокко, Сирії було повалення урядів або їх зміна, тривалі громадські заворушення тощо.

Узагальнивши хронологію подій «арабської весни» можна подати у вигляді часової діаграми на рис. 2.

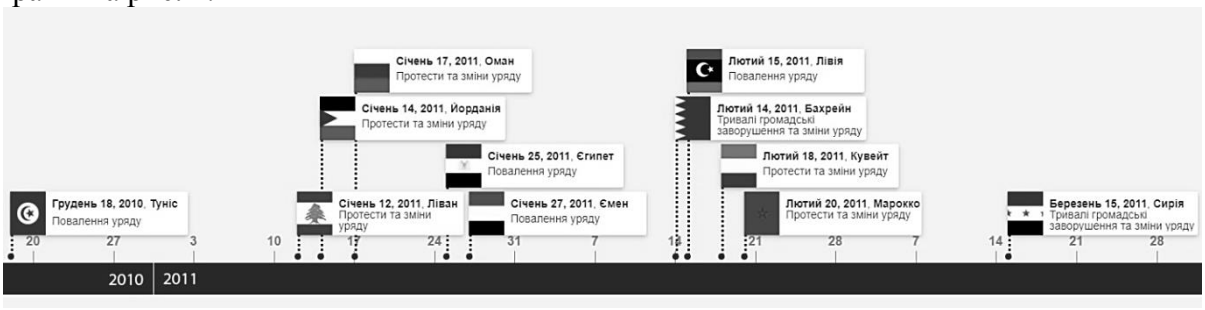


Рис. 2. Часова діаграма хронології подій «арабської весни»

Спільною рисою громадянських виступів проти влади було використання СІС для координації протестів, активізації суспільства, поширення протестних настроїв, оперативного висвітлення подій та інформування міжнародних ЗМІ. Слід зауважити, що комунікація учасників протестів відбувалася з використанням декількох СІС одночасно для ширшого охоплення цільової аудиторії завдяки поширенню мультимедійного контенту різного типу.

СІС активно використовувалися у громадянських протестах у Нью-Йорку під назвою «захопи Уолл-стріт» (вересень 2011 р.) [11]. Учасники демонстрацій ставили за мету захопити вулицю Уолл-стріт, на якій розміщується фінансовий центр міста, щоб привернути увагу до зростаючого впливу корпорацій на уряд США і закликати до структурних змін в економіці. Також марші протестів відбувалися й в інших містах США і тривали декілька місяців. Лозунги протестувальників вперше поширювалися у *Tumblr*, а для залучення нових учасників використовувалися *Twitter* та інші популярні СІС [21].

Сьогодні для протидії загрозам національній безпеці ряд країн обмежують доступ громадян до СІС. З 2003 р. в рамках проекту «Золотий щит» створено так званий «Великий китайський фаєрвол» для фільтрації контенту мережі Інтернет КНР [21]. На території КНР обмежено доступ до *Google, Flickr, Dropbox, Facebook, Twitter, YouTube* і частково до *Wikipedia*, тому громадяни користуються китайськими аналогами. Однак, спроби організації протестів громадян на фоні подій «арабської весни» показали, що зважаючи на постійне зростання кількості користувачів мережі Інтернет повний контроль інформаційних потоків на рівні держави є складним завданням. Практика постійного або тимчасового блокування СІС також використовується у Північній Кореї, Ірані, Пакистані, В'єтнамі, Саудівський Аравії, Єгипті, Туреччині та інших країнах.

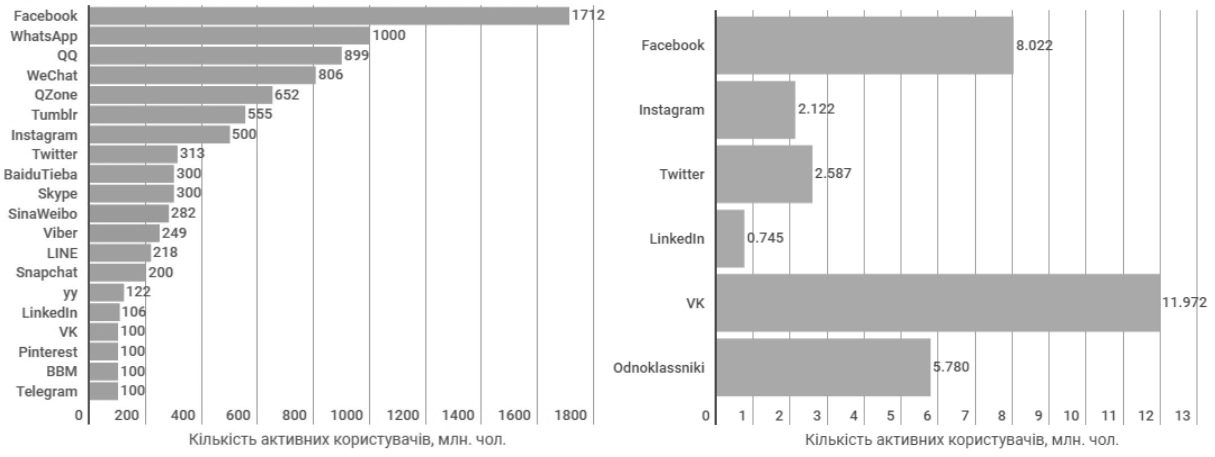
Події анексії Криму і збройної агресії Російської Федерації на сході України показали, що СІС активно використовувалися на етапах підготовки й безпосередньо під час їх ведення. Так, дослідження [23, 24] інформаційного супроводу анексії Криму у березні 2014 р. продемонстрували застосування СІС у інформаційно-пропагандистській діяльності Російської Федерації. За інформацією американського аналітика М. Голловея, опублікованою для військового видавництва США *Realcleardefense* [25], уряд Російської Федерації витратив 19 мільйонів доларів для фінансування діяльності 600 спеціально залучених акторів *Facebook, Vkontakte, Odnoklassniki*. Діяльність цих акторів полягала у публікації статей і коментарів до них з метою формування в українського та міжнародного суспільства враження про підтримку місцевим населенням анексії, дискредитації місцевої опозиції, поширення серед населення чуток, почуттів страху й ненависті. Перші публікації російських військ інформаційних операцій з'явилися у *Facebook*, однак найбільшу популярність їх публікації здобули у *Vkontakte*, причому швидкість поширення контенту складала 5 тисяч репостів за добу. Такий контент містив технології маніпулювання суспільною думкою для збільшення аудиторії впливу від старших поколінь до молоді,

поляризації суспільства. СІС використовувалися для легітимізації результатів псевдореферендуму про статус Криму. Також у Криму російськими військами інформаційних операцій створювався інформаційний вакуум шляхом блокування урядових сайтів, здійснення кібератак на сайти ЗМІ. Результатом таких дій стало отримання суттєвих переваг у інформаційному просторі для спрощення дій з анексії півострова. Таким чином, анексія Криму послужила дослідним майданчиком для проведення інформаційних операцій проти інформаційної безпеки держави і продемонструвала, що СІС є ефективним інструментом управління суспільством.

У квітні 2014 р. проросійські активісти розпочали захоплення адміністративних будівель Донбасу. Одночасно активізувалася діяльність спеціально створених віртуальних спільнот у СІС, передусім *Vkontakte*. Тематика таких віртуальних спільнот як *Антимайдан, Новороссия, Русская весна* і багатьох інших присвячувалась ідеям Антимайдану та полягала у створенні альтернативи громадянським протестам Революції Гідності. У даних віртуальних спільнотах поширювалася недостовірна інформація, широко використовувалися технології маніпуляції суспільною думкою, а їх діяльність цілеспрямовано нав'язувалася акторам СІС. Одними із завдань було поширення агітаційних матеріалів, символіки квазідержавного утворення для його легітимізації в суспільстві, регіональної ворожнечі та створення нової штучної національної ідентичності, відмінної від української. Метою інформаційних операцій проти інформаційної безпеки людини, суспільства, держави у СІС під час збройної агресії Російської Федерації на Сході України стали деструктивний інформаційний вплив на свідомість акторів, поширення заданих ідеологічних і соціальних установок, вироблення заданих стереотипів поведінки, бажані перетворення суспільних настроїв, почуттів, волі [23].

У праці *B. Perry* [24] проаналізовано інструменти, використані Росією під час гібридної війни з Україною, та визначено, що найбільш ефективними з них є інформаційні операції. Контроль над ескалацією ситуації досягався завдяки активній тривалій проросійській пропаганді серед населення Південно-Східних регіонів України. Наслідками таких дій стали сприйняття населенням відповідного наративу і формування проросійської ініціативної більшості, яка стала основою для консолідації сепаратистів та підтримки інтервенції збройних формувань.

Статистика використання СІС в Україні та світі станом на липень 2016 р. за даними компанії *Adpro* подана на рис. 3.



а) б)

Рис. 3. Статистика використання СІС: а) у світі; б) в Україні (без врахування тимчасово окупованих територій Луганської та Донецької областей та АР Крим)

Аналіз рис. 3 показав, що в Україні, на відміну від решти світу, суттєва частка ринку СІС належить російським сервісам. 15 травня 2017 р. Президентом України підписано Указ про введення в дію рішення Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Цей

документ забороняє інтернет-провайдерам здійснювати послуги з доступу до СІС *Одноклассники* і *Вконтакте* та деяких інших російських ресурсів. У зв'язку з цим відбувся істотний перерозподіл користувачів між іншими СІС, зокрема, за даними видання *Watcher*, аудиторія *Facebook* у серпні 2017 р. зросла до 9 млн. користувачів, а *Instagram* – до 6 млн.

Узагальнюючи, процеси проведення російських інформаційних операцій в Україні доцільно представити у вигляді паттернів (рис. 4).

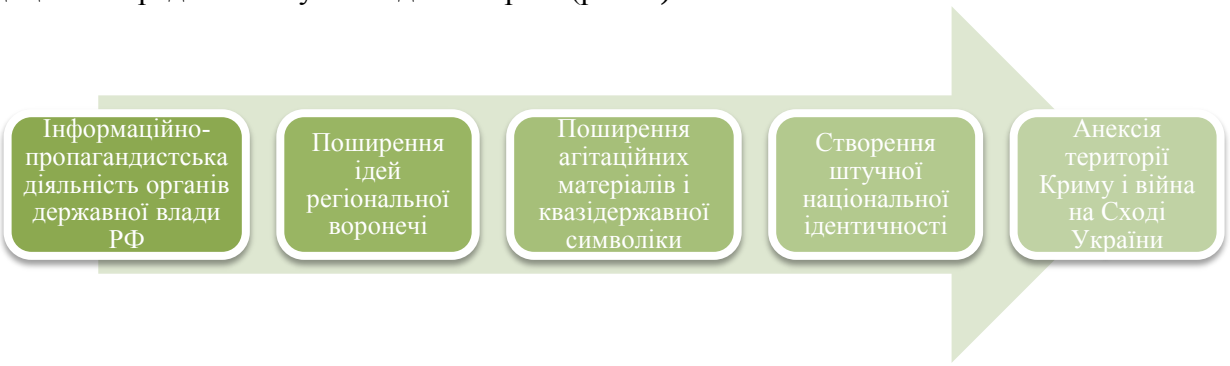


Рис. 4. Паттерни інформаційних операцій Російської Федерації на початкових етапах гібридної війни в Україні

Одним з результатів проведення інформаційних операцій в Україні стало створення суттєвих перешкод для прийняття управлінських рішень не тільки на регіональному, але і на державному рівні. Тому, можна зробити висновок, що СІС відігравали провідну роль для організації анексії Криму і розпалювання суспільної ворожнечі й ескалації насильства на Сході України.

Визначення підходів до виявлення і оцінювання ознак загроз у СІС

Забезпечення стійкого розвитку інформаційної сфери держави неможливе без своєчасного виявлення загроз ІБД у СІС. Узагальнення досвіду проведення інформаційних операцій проти України з використанням протиборчою стороною СІС показало, що для їх реалізації використовуються значні інформаційні ресурси, механізми таргетингу для впливу на цільову аудиторію, що забезпечує вибірковий характер інформаційного впливу [26].

Одним з найпоширеніших явищ у СІС є використання соціальних ботів для формування суспільної думки з актуальних питань, активного обговорення у віртуальних спільнотах другорядних подій, блокування акаунтів окремих акторів СІС тощо. Наприклад, дослідження компанії *TheRespo* разом зі спеціалістами *VoxUkaine* [27] офіційної сторінки президента П. Порошенка у *Facebook* за період з 07.06.2014 р. по 31.05.2017 р. показали, що тільки 2% коментарів публікацій належать соціальним ботами. При цьому соціальні боти найбільш продуктивно коментують дописи зі сторінки президента – їм належать 15% від усіх коментарів, тобто кожен шостий з них зроблений ботом. Позитивною тональністю характеризуються коментарі 27% ботів, негативною – 29% і нейтральною – 44%. Такі дані свідчать про залучення спеціального програмного забезпечення комунікаційними групами з протилежними цілями для створення у акторів СІС враження про підтримку чи несприйняття суспільством політики президента.

Результати аналізу текстового контенту, який поширювався ботами показали, що в ньому містилася дезінформація з елементами маніпулювання [28]. Такий контент, як правило, висвітлював актуальну тематику подій, яка загрожувала ІБД. Перевагами застосування маніпуляцій суспільною думкою акторів у СІС є нав'язування і спонукання до виконання визначених дій не тільки у віртуальних спільнотах, але й в реальному житті, проявів бажаних емоційних станів, обговорення недостовірного контенту тощо [29]. Також використовувалися суттєві відхилення від загальноприйнятої концепції використання лексем конкретної предметної області публікації, внаслідок чого здійснюється вплив на акторів СІС. Наприклад, вираз «влада держави цілеспрямовано знищує громадян пенсійного віку» вказує на свідоме знищення населення старшого віку і поширення такого контенту негативно

впливає на громадську думку. Таким чином завдяки латентному характеру впливу на акторів і високим темпам появи нових маніпулятивних технологій зловмисниками досягаються односторонні переваги в інформаційному просторі держави.

Основним джерелом контенту у СІС є актори, які використовують наявні засоби не тільки для публікації самостійно створеного контенту, але і для поширення контенту інших акторів чи віртуальних спільнот або зовнішніх до СІС ЗМІ. Аналіз і узагальнення інформації профілів акторів у СІС, їх зв'язків з іншими акторами й віртуальними спільнотами, особливостей поведінки онлайн дозволяють зробити висновок про їх участь в інформаційних акціях проти ІБД. Тому оцінювання профілів акторів СІС дає змогу виявити осіб, які залучені до інформаційних операцій у СІС. Таким чином, загрози інформаційній безпеці людини, суспільства, держави у СІС характеризуються різними ознаками, що визначають аспекти їх прояву. Окремі інформаційні операції можуть відрізнятися між собою не тільки змістом, але і використаними технологіями проведення, що додатково ускладнює процедури виявлення ознак проведення та оцінювання рівня загроз. Отже, узагальнюючи вищесказане, проблема виявлення ознак загроз ІБД у СІС і оцінювання їх рівня зводиться до розроблення нових методів і технологій виявлення складових ознак загроз та оцінювання їх рівня (рис. 5).

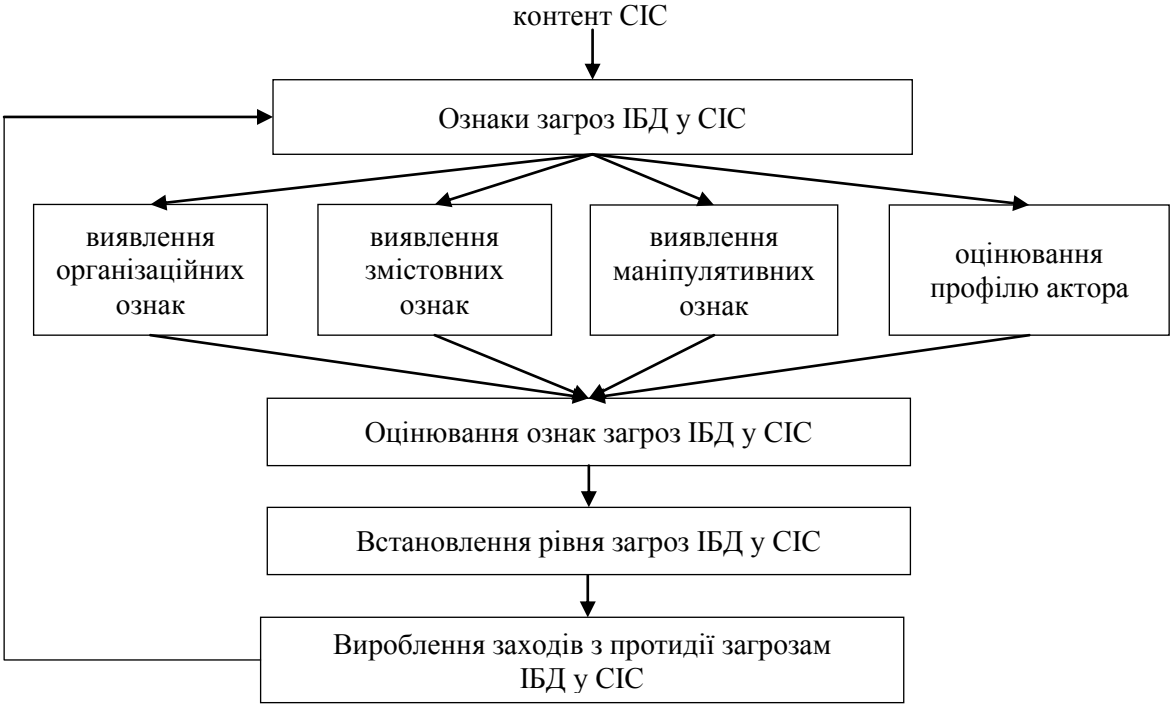


Рис. 5. Концептуальний базис виявлення і оцінювання ознак загроз ІБД у СІС

При цьому необхідно врахувати, що загрози ІБД у СІС не завжди проявляються всіма ознаками одночасно. На основі визначеного рівня ознак загроз у СІС проводяться заходи з їх нейтралізації та протидії відповідними відомствами й підрозділами.

Встановлення перспективних напрямків протидії загрозам ІБД у СІС

Із досліджень [14, 15, 30] відомо, що актори у СІС сумісно зі зв'язками з іншими акторами та віртуальними спільнотами утворюють складну нелінійну динамічну систему. СІС неперервно взаємодіють з національним та глобальним інформаційними просторами, які представляють собою зовнішнє середовище їх функціонування, і одночасно є його складовими підсистемами, тобто характеризуються еквіпотенційністю. Тому комунікація акторів у СІС характеризується відкритістю, нелінійністю, нерівноважністю і дисипативністю. При цьому актори здатні до самоорганізації за спільними інтересами шляхом утворення складних структур без зовнішнього управляючого впливу, що призводить до ускладнення організаційної структури і взаємозв'язків учасників віртуальних спільнот.

Наслідком високої чутливості СІС до зміни системних параметрів і дії збурень, зокрема деструктивних інформаційних впливів, є перехід до хаотичної динаміки віртуальних спільнот акторів. При цьому взаємодія акторів у СІС перетворюється на випадкову і непрогнозовану навіть за умови детермінованості моделей їх взаємодії. Таким чином, з метою протидії загрозам ІБД у СІС і управління процесами взаємодії акторів доцільно скористатися положеннями теорії хаосу.

Відповідно до теоретичних положень теорії хаосу, досягнення бажаного стану СІС можливе за умови пригнічення хаотичної динаміки процесів взаємодії акторів. Серед класичних методів управління хаотичною динамікою систем виділяють програмні методи управління, метод лінеаризації відображення Пуанкаре, метод зворотного зв'язку, що запізнюється тощо. Загальним недоліком таких методів є складність виконання вимоги малості управління, нехтування якою створює хибне бачення простоти управління хаотичною динамікою системи [31]. Реалізація управління такими методами пов'язана з привнесенням суттєвих змін не тільки в динаміку системи, а й у її структуру вцілому, тому не може використовуватися у СІС.

Із публікацій [32–35] встановлено, що у складних динамічних системах, далеких від стану рівноваги, виникають процеси самоорганізації. Завдяки самоорганізації акторів у СІС виникає, відтворюється або удосконалюється організаційна структура віртуальних спільнот. Тому можна виділити невелику кількість змінних чи характеристик інформаційного середовища, варіювання якими призводить до бажаної зміни динаміки СІС. Такі змінні представляють собою параметри порядку системи і разом з теоретичними основами синергетики можуть бути покладені в основу ефективних методів протидії деструктивним інформаційним впливам на акторів СІС.

Отже, перспективним напрямком протидії загрозам ІБД у СІС є розроблення концепції синергетичного управління взаємодією акторів, при якому відбувається керована самоорганізація учасників віртуальних спільнот. До синтезованого управління висуваються вимоги узгодження природних закономірностей функціонування СІС із вимогами реалізованості управління, асимптотична стійкість керованої системи, її грубість, мінімізація за часом перехідних процесів тощо [35].

Узагальнений аналіз і формалізація проблеми розроблення методології побудови систем забезпечення ІБД у СІС

Системний аналіз ролі СІС в національному інформаційному просторі держави показав, що вони здатні суттєво впливати на політичні й суспільні процеси у державі, тому такі сервіси є об'єктом загроз ІБД (рис. 6).

Джерелами реальних і потенційних загроз можуть виступати актори a_m, b_m, c_m або їх віртуальні спільноти A_k, B_k, C_k, що представляють собою внутрішні джерела загроз ІБД у СІС. У свою чергу, усі СІС функціонують у зовнішньому середовищі, яке представлене міжнародним і національним інформаційним простором, зокрема ЗМІ. При цьому суб'єктами загроз виступають іноземні держави, окремі особи чи їх групи. Для реалізації поставлених цілей суб'єкти загроз ІБД у СІС залучають війська інформаційних операцій, а інколи й сили та засоби кіберпідрозділів. Використовуючи інформаційну зброю такі підрозділи здатні цілеспрямовано впливати на індивідуальну і групову свідомість акторів.

Застосування існуючих відокремлених компонентів системи інформаційної безпеки (СІБ) держави, відомчих підсистем забезпечення ІБД для протидії окремим видам загроз не дозволяє ефективно вирішити проблему захисту людини, суспільства, держави від зовнішніх і внутрішніх загроз у СІС.

Зважаючи на складність процесів управління соціотехнічними системами, інтенсивний розвиток інформаційних технологій впливу на суспільну думку, латентний характер загроз ІБД, особливої актуальності набуває необхідність розроблення методології побудови системи забезпечення ІБД у СІС.

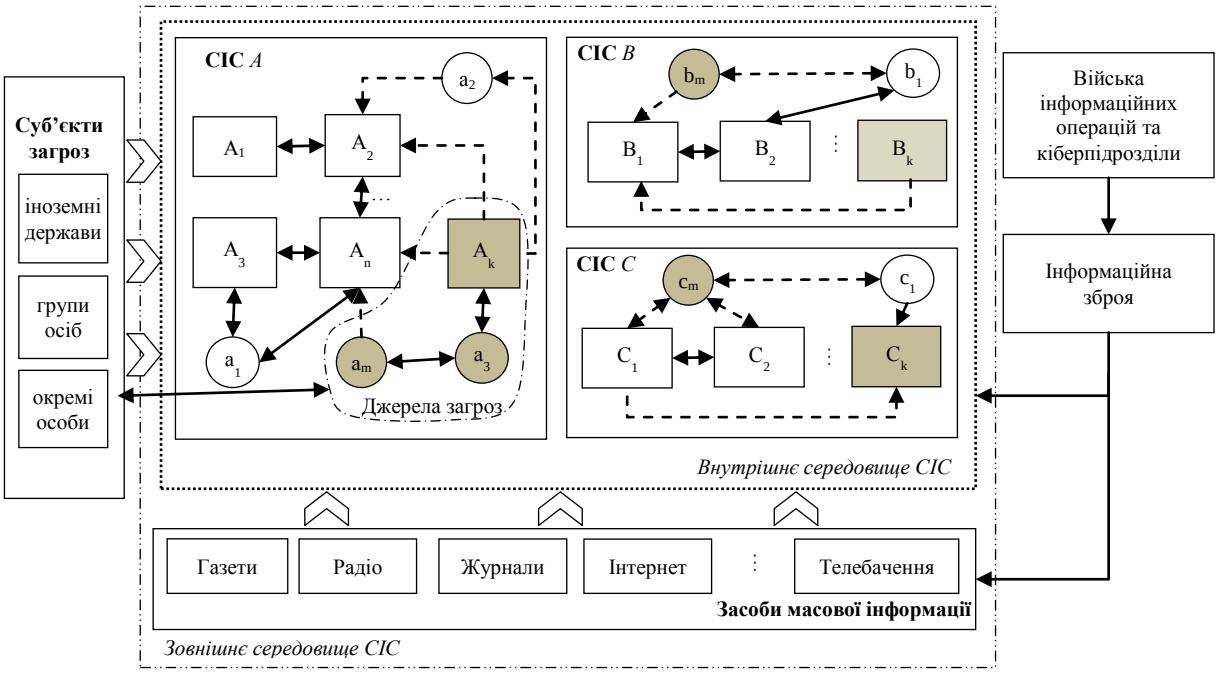


Рис. 6. СІС як об'єкт загроз інформаційній безпеці держави

Відсутність відповідної методології обумовлена проблемою практики, яка пов'язана з тим, що в умовах ведення інформаційного протиборства для будь-якої розвиненої держави світу й України зокрема, нагальною є потреба в підвищенні рівня власної інформаційної безпеки при використанні її громадянами СІС. З іншого боку, недосконаліть системи ІБД в цілому та, як наслідок, відсутність цілісної науково обґрунтованої методології побудови відповідної системи її забезпечення у СІС зокрема, що гарантує системність та комплексність у прийнятті рішень (рис. 7).

Рис. 7. Сутність наукової проблеми розроблення методології побудови системи забезпечення ІБД у СІС

Виходячи зі змісту наукової проблеми розроблення методології побудови системи забезпечення ІБД у СІС доцільно сформулювати її наступним чином. Нехай СІС перебуває в одному з w можливих станів, що визначає рівень її інформаційної безпеки S_{real}^{w} і характеризується вектором параметрів системи P. Тоді створена система забезпечення ІБД у СІС повинна синтезувати таку управляючу дію $U_j(P)$, $j=\overline{1,m}$ з множини можливих, щоб

тривалість перехідних процесів T_{PR} переходу віртуальної спільноти акторів до бажаного стану інформаційної безпеки S^{v}_{accept} була мінімальною

$$S^{w}_{real}(t) \xrightarrow[T_{PR}\to\min]{U_j(P)} S^{v}_{accept}(t+T_{PR}).$$

Необхідно розробити методологію побудови систем забезпечення ІБД у СІС, що забезпечить перехід до бажаного стану інформаційної безпеки за умови ресурсних обмежень.

Висновки

Встановлено, що СІС є дієвим інструментом впливу на суспільні й політичні процеси у державі. Тому забезпечення ІБД у СІС в умовах глобалізації інформаційного простору і гібридизації воєнних конфліктів залишається однією із нагальних проблем, які потребують свого вирішення. В статті у загальному вигляді формалізовано проблему забезпечення ІБД у СІС на основі критичного аналізу сучасних підходів і визначено перспективні напрямки досліджень. Встановлено, що виявлення загроз ІБД у СІС доцільно реалізувати за частинними ознаками їх прояву – організаційними, змістовними, маніпулятивними та на базі оцінювання профілів інформаційної безпеки акторів. Сформульовано гіпотезу про ефективність використання процесів самоорганізації в складних нелінійних системах для протидії загрозам ІБД у СІС. Перевагою такого підходу є використання природних особливостей функціонування складних систем для штучно керованого управління динамікою процесів взаємодії акторів у СІС. При цьому перехід віртуальної спільноти до бажаного стійкого стану інформаційної безпеки відбувається за умови реалізованості синтезованого синергетичного управління і мінімальної тривалості перехідних процесів. Визначені підходи до виявлення ознак і протидії загрозам пропонується використовувати для побудови системи забезпечення ІБД у СІС, що дозволить суттєво підвищити рівень ІБД у СІС. Отримані результати можуть використовуватися для розв'язку частинних задач у рамках проблеми забезпечення ІБД у СІС.

Список використаної літератури

1. Проблеми суспільної безпеки в процесі розвитку соціальних мереж : [монографія] / [В. Попик (кер. проекту), В. Горовий, О. Онищенко та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – Київ, 2015. – 202 с.

2. Соціальні мережі як чинник розвитку громадянського суспільства : [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.

3. Информационные риски в социальных сетях / Г. А. Остапенко, Л. В. Паринова, В. И. Белоножкин, И. Л. Батаронов, К. В. Симонов / Под ред. член-корр. РАН Д.А. Новикова. 2013. 161с.

4. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання : аналіт. доп. / В. К. Конах. – К. : НІСД, 2014. – 76 с.

5. Проект Концепції інформаційної безпеки України : [Електронний ресурс] / Офіційний сайт Міністерства інформаційної політики України. – Режим доступу: http://mip.gov.ua/documents/30.html (дата звернення 30.08.2017). – Назва з екрану.

6. Доктрина інформаційної безпеки України (затверджена указом Президента України №47/2017 від 25 лютого 2017 року) : [Електронний ресурс] / Офіційне представництво Президента України. – Режим доступу : http://www.president.gov.ua/documents/472017-21374 (дата звернення 30.08.2017). – Назва з екрану.

7. Ознаковий принцип формування класифікацій кібератак / О. Г Корченко, С. В. Казмірчук, Є. В. Паціра, С. О. Гнатюк, В. М. Кінзерявий // Вісник СНУ ім. В. Даля. – 2010. – №4, т. 1. – С. 184–193.

8. Юдін О. К. Інформаційна безпека держави : навч. посіб. / О. К. Юдін , В. М. Богуш. – Харків: Консум, 2004. – 508 с.

9. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.

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

11. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник; під заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

12. Молодецька К. В. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави / К. В. Молодецька // Information technology and security. – 2016. – Vol. 4, Iss. 1(6). – С. 13–20.