УДК 004.056:004.738.5(045)

К.В. МОЛОДЕЦЬКА

Національний агроекологічний університет, м. Житомир

УЗАГАЛЬНЕНА КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ В СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Вступ. На сучасному етапі постійно зростає роль соціальних інтернет-сервісів (СІС) у комунікативному просторі [1, 2]. Переваги використання СІС досягаються завдяки особливостям взаємодії акторів, які є учасниками взаємодії в СІС і віртуальних спільнотах, а саме: ідентифікація шляхом самостійного наповнення профілю; формування і відслідковування зв'язків з іншими акторами й об'єктами; підтримка комунікації та формування об'єднань тощо. Тому СІС використовуються акторами не тільки для спілкування, поширення і обміну контентом різного типу, але й поступово перетворюються в ефективний інструментарій суспільних перетворень, створення об'єднань громадян тощо [1-4]. Однак, позитивні комунікаційні властивості СІС можуть бути використані зловмисниками для реалізації власних інтересів шляхом поширення у віртуальних спільнотах недостовірного, неповного чи упередженого контенту [5-7]. Наслідком таких дій може бути виникнення передумов маніпулюванню індивідуальною або масовою свідомістю громадян з метою поширення у суспільстві соціальної напруженості, міжнаціональної ворожнечі, протестних настроїв, незадоволення існуючою системою управління в державі. Відомо, що організація ефективної протидії поширенню деструктивних інформаційних посилів у СІС пов'язана з їх оперативним виявленням, оцінюванням і прогнозуванням можливих наслідків в результаті контент-аналізу повідомлень [8, 9]. Однак, недостатній рівень теоретичного розроблення класифікації видів загроз у СІС ускладнює процедури реалізації дієвої протидії, тому є актуальним теоретико-прикладним завданням для вирішення проблеми забезпечення інформаційної безпеки людини, суспільства, держави.

Аналіз останніх досліджень і публікацій показав, що загальні положення законодавчого регулювання інформаційного простору закріплені в ЗУ «Про інформацію» [10] в чинній редакції від 21.05.2015 р. Одним з основних недоліків цієї законодавчої ініціативи є відсутність дефініції категорії «інформаційна безпека», що призводить до низької ефективності нормативно-правового захисту українського

інформаційного простору і, як наслідок, протидії інформаційній агресії [11, 12]. Також питання інформаційної безпеки держави відображене у оновленому Проекті Доктрини інформаційної безпеки України, що має на меті «створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету» [13]. Проведення наукових досліджень у обраному напрямку ускладнюється відсутністю прийнятого нормативно-правового забезпечення, що дозволило б розробити дієві механізми впливу на інформаційний простір СІС на державному рівні.

Аналіз академічної літератури [9, 11, 12, 14-18] за напрямком дослідження показав, що більшість публікацій пов'язані з аналізом і класифікацією загроз в аспекті технічного захисту інформації, безпеки інформаційно-комунікаційних систем, кібербезпеки. Ряд публікацій присвячений організаційно-правовому напрямку забезпечення інформаційної безпеки в СІС [11, 18-20]. З огляду на вищесказане і відносно новий феномен взаємодії акторів віртуальних спільнот СІС зокрема, класифікація загроз інформаційній безпеці держави в СІС є особливо актуальною і потребує подальшого дослідження.

Метою статті є аналіз загроз інформаційній безпеці держави в СІС і розробка узагальненої класифікації для реалізації ефективного їх виявлення та протидії для забезпечення інформаційної безпеки людини, суспільства, держави.

Для досягнення поставленої мети необхідно розв'язати частинні задачі:

– аналіз існуючих наукових підходів до класифікації загроз інформаційній безпеці держави;

– визначення загроз інформаційній безпеці держави в СІС;

– розробка нового підходу до узагальненої класифікації загроз інформаційній безпеці держави в СІС і їх формалізація.

Основна частина. Сьогодні на завершальному етапі розробки знаходиться Проект Концепції інформаційної безпеки України, яка визначає загрози інформаційної безпеки держави як «наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері» [22]. Ефективне дослідження кожної із загроз неможливе без розробки відповідної класифікаційної системи, що враховує їх особливості.

Серед вітчизняних вчених найбільш повна класифікація загроз за ознаковим принципом належить професору О.Г. Корченку. До базових класифікаційних ознак загроз автор відносить наведені на рис. 1 [15].

Рис. 1. Класифікація кібератак за О.Г. Корченком

Розглянута класифікація забезпечує широкий спектр охоплення загроз у інформаційно-комунікаційних системах. Вона описує загрози технологічного характеру, які пов'язані з функціонуванням інформаційно-комунікаційних систем і безпекою внутрішньодержавного інформаційного простору. Однак, така класифікація не може застосовуватися для опису загроз національним інтересам в інформаційному просторі СІС.

Професор В.А. Ліпкан запропонував власний підхід до визначення загроз інформаційній безпеці держави у розрізі загроз національній безпеці [12, 14]. Автор виділив групи класифікаційних ознак, наведених на рис. 2.

Рис. 2. Класифікація загроз інформаційній безпеці за В.А. Ліпканом

Перевагою даного підходу до класифікації загроз інформаційній безпеці є інтеграція з поняттями «інформаційна війна», «інформаційне протиборство», «інформаційний тероризм». Але така класифікація не враховує нових викликів інформаційній безпеці громадянина, суспільства, держави у СІС, пов'язаних з гібридною війною і агресією Російської Федерації.

Відповідно до рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» розроблено Проект Доктрини інформаційної безпеки України [13], який передбачає створення Проекту Концепції інформаційної безпеки України [22]. Запропонований Проект Концепції найбільш повно визначає актуальні загрози інформаційної безпеки України (рис. 3).

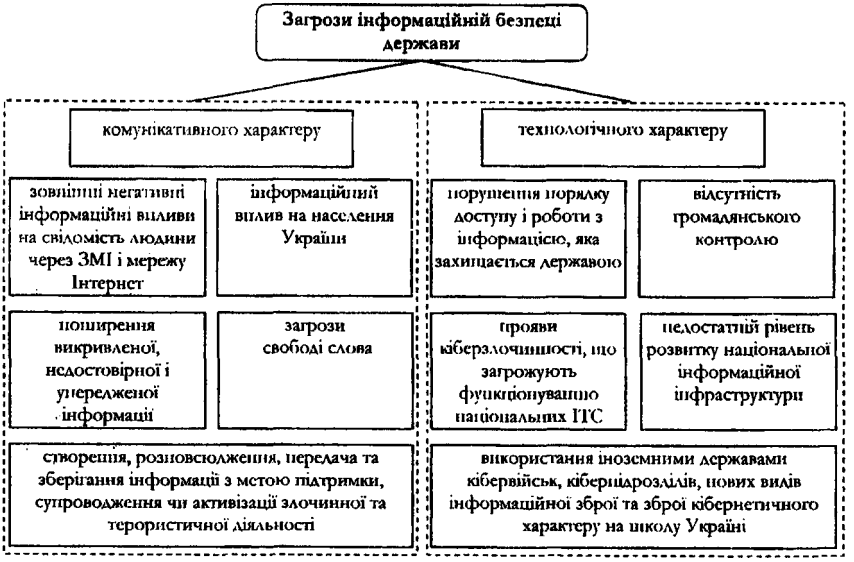

Рис. 3. Загрози інформаційній безпеці держави відповідно до Проекту Концепції інформаційної безпеки України

Визначені загрози інформаційній безпеці за сферою виникнення поділяються на комунікативні і технологічні. Загрози комунікативного характеру пов'язані з реалізацією потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження й розвитку національного стратегічного контенту та інформації [22]. Технологічні загрози проявляються в сфері

функціонування і захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору [22].

Отже, розглянуті різновиди класифікацій загроз інформаційній безпеці держави сформульовані у розрізі безпеки інформації, кібербезпеки, безпеки інформаційно-комунікаційних систем, однак не враховують особливості функціонування СІС і взаємодії акторів у віртуальних спільнотах.

Системний аналіз ролі СІС в інформаційному просторі держави і особливостей їх функціонування [1, 5, 6, 23, 24] показав, що вони є об'єктом реальних і потенційних загроз інформаційній безпеці людини й громадянина, суспільства та держави. Загальна структурна модель СІС як об'єкта загроз наведена на рис. 4.

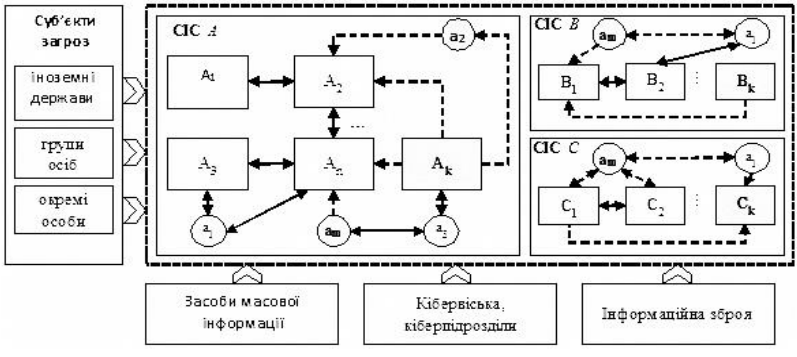

Рис. 4. СІС як об'єкт загроз інформаційній безпеці держави

Джерелами загроз в СІС можуть бути іноземні держави, групи або окремі особи, які намагаються шляхом деструктивного інформаційного впливу на масову свідомість акторів чи віртуальних спільнот змінити їх психологічний стан, розпалити ворожнечу за національною, етнічною або будь-якою іншою ознакою. Також джерелами загроз в СІС можуть поширюватися заклики до сепаратизму, незадоволення існуючою системою влади в державі тощо. Досягнення таких цілей реалізується створенням в СІС A, B, C окремих віртуальних спільнот A_k, B_k, C_k, які поряд з акторами a_m здійснюють поширення викривленої, недостовірної або упередженої інформації для дискредитації органів державної влади, дестабілізації суспільно-політичної ситуації,

підтримки злочинних угруповань чи терористичних організацій. На рис. 4 віртуальні спільноти і актори, які поширюють деструктивні інформаційні посили позначені кольором, а можливі напрямки їх поширення – штриховими лініями.

Значний вплив на інформаційний простір СІС мають засоби масової інформації, які несуть в собі загрози цілеспрямованого інформаційного впливу на акторів, і, як наслідок, маніпулювання свідомістю під впливом джерел загроз інформаційній безпеці держави. Окремо слід виділити вплив кібервійськ, кіберпідрозділів й інформаційної зброї інших держав на функціонування СІС і їх захищеність. Наслідком таких дій може бути інформаційна підтримка у СІС злочинної або терористичної діяльності, поширення деструктивних інформаційних впливів у віртуальних спільнотах, порушення порядку роботи з персональними даними акторів.

Узагальнюючи відомі підходи [11, 12, 14-16, 23, 25] до класифікації загроз інформаційній безпеці держави, особливості функціонування і взаємодії акторів віртуальних спільнот у СІС як об'єкта державного інформаційного простору, запропоновано авторський підхід до класифікації загроз інформаційній безпеці держави в СІС, що не суперечить матеріалам інших досліджень. Зважаючи на різноманітність загроз національній безпеці в інформаційній сфері доцільно використати фасетну систему класифікації за логічними ознаками [26], яка характеризується високою гнучкістю, можливістю необмеженого додавання числа фасетів і розбиття множини загроз за їх довільним сполученням. Встановлено такі основні ознаки класифікації загроз інформаційній безпеці в СІС, які наведені на рис. 5.

1. *По відношенню до акторів СІС* $Relatinon = \bigcup_j R_j$, $j = \overline{1,2}$ виділяють:

– внутрішні загрози R_1, які створюються компонентами СІС – акторами або віртуальними спільнотами;

– зовнішні загрози R_2, які з'являються від об'єктів, що взаємодіють з СІС, але не входять до їх функціональної структури, наприклад засоби масової інформації, спецслужби, неурядові організації, користувачі мережі Інтернет тощо.

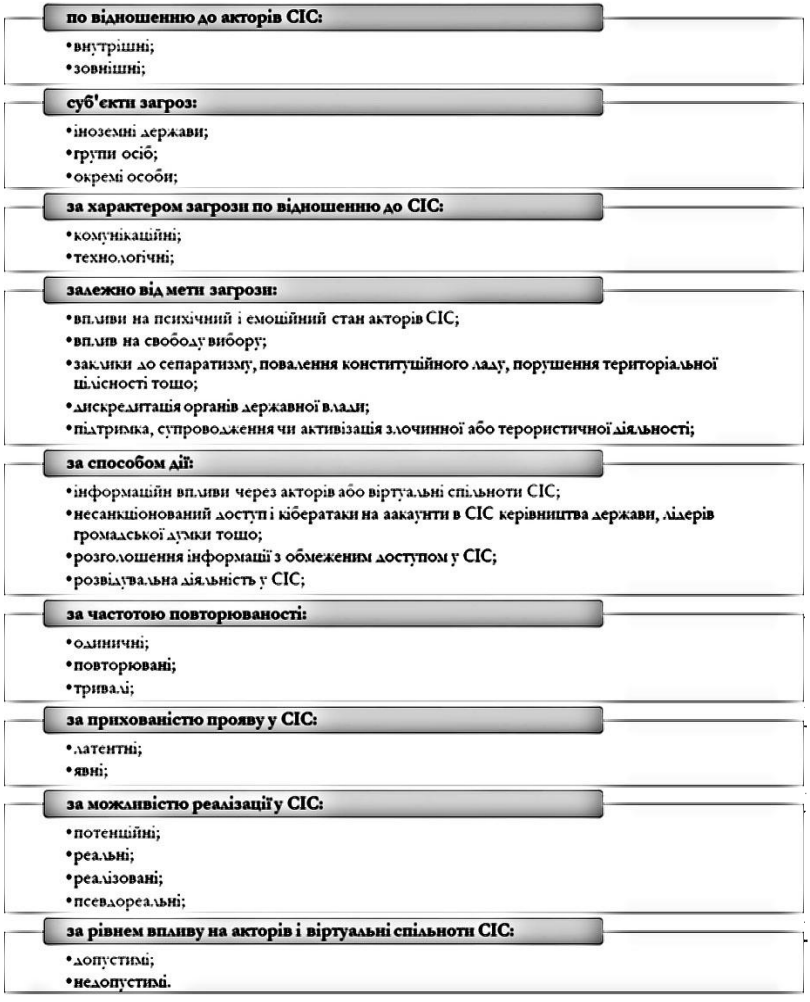

Рис. 5. Класифікація загроз інформаційній безпеці держави в СІС

2. *За видами суб'єктів загроз* $Subject = \bigcup_{l} S_l$, $l = \overline{1,3}$ розрізняють:

– іноземні держави S_1;

– групи осіб S_2;

– окремі особи S_3.

3. *За характером загрози по відношенню до СІС* $Character = \bigcup_b C_b$, $m = \overline{1,2}$ бувають:

– комунікаційні C_1, які проявляються в галузі реалізації потреб акторів у продукуванні, споживанні і розповсюдженні контенту;

– технологічні C_2, що полягають в порушенні функціонування і захищеності СІС, що є складовою національного інформаційного простору.

4. *Залежно від мети загрози* $Target = \bigcup_z T_z$, $n = \overline{1,5}$ розрізняють:

– вплив на психічний і емоційний стан акторів СІС T_1. Такий вплив може призводити до появи у акторів СІС заданого психічного стану (тривожності, ейфорії, задоволення або незадоволення) чи емоцій (стенічних, астенічних, позитивних, негативних) як реакції на поширюваний у СІС контент;

– вплив на свободу вибору акторів T_2 у прийнятті будь-яких рішень від зовнішніх факторів, наприклад зневажливого ставлення до людської або національної гідності, розпалювання ворожнечі чи ненависті на національному, етнічному, релігійному підґрунті, поширення ідей жорстокого ставлення чи ненависті.

– заклики до сепаратизму, повалення конституційного ладу, порушення територіальної цілісності T_3;

– дискредитація органів державної влади T_4, наслідком якої є ускладнення процесів прийняття політичних рішень, створення негативного іміджу держави, шкода національним інтересам;

– підтримка, супроводження чи активізація злочинної або терористичної діяльності T_5.

5. *За способом дії загрози у СІС* $Method = \bigcup_p M_p$, $p = \overline{1,5}$ поділяють на:

– інформаційні впливи через СІС M_1 – організований цілеспрямований вплив на акторів СІС для деструктивних змін свідомості, корекції їх поведінки або фізичного стану;

– несанкціонований доступ і кібератаки на аккаунти в СІС керівників держави, лідерів громадської думки M_2, внаслідок яких може поширюватися недостовірний, викривлений, упереджений контент або блокуватися їх діяльність у СІС;

– розголошення інформації з обмеженим доступом у СІС M_3 як одному з найбільш ефективних засобів комунікації і поширення контенту;

– розповсюдження шкідливого програмного забезпечення у СІС M_4, наприклад шляхом додавання гіперпосилань у коментарях на розміщений шкідливий програмний код зі сторонніх сайтів;

– розвідувальна діяльність у СІС M_5, що проявляється як встановлення противником державної належності та ідентифікації об'єктів, навігаційне забезпечення операцій тощо.

6. *За частотою повторюваності* $Frequency = \bigcup_d F_d$, $d = \overline{1,3}$ мають місце такі загрози в СІС:

– одноразові F_1, які не мають повторень у інформаційному полі СІС;

– повторювані F_2, які вже виникали на попередніх етапах комунікації акторів у СІС;

– продовжувані F_3 – це неодноразові подібні загрози, які підпорядковані конкретній поставленій меті.

7. *За прихованістю прояву* $Secrecy = \bigcup_w Sr_w$, $w = \overline{1,2}$ бувають:

– латентні Sr_1 – це приховані, ретельно замасковані загрози;

– явні Sr_2 – об'єктивно існуючі, видимі загрози.

8. *За можливістю реалізації у СІС* $Possibility = \bigcup_i P_i$, $i = \overline{1,4}$ виділяють загрози:

– потенційні P_1 – активізація загрози виконується при створенні заданих умов у суспільній, політичній, економічній або інших сферах державної діяльності;

– реальні P_2 – поява загрози є невідворотною, не обмежена в часі і просторі;

– реалізовані P_3 – загрози, які здійснені в інформаційному просторі СІС;

– псевдореальні P_4 – поява у СІС ознак загроз, яких насправді немає.

9. *За рівнем впливу на акторів і віртуальних спільноти СІС* $Impact = \bigcup_q I_q$, $q = \overline{1,2}$ розрізняють:

– допустимі I_1 загрози, які не несуть деструктивних наслідків для інформаційної безпеки людини, суспільства, держави;

– недопустимі I_2 – причиняють критичні деструктивні наслідки в інформаційному середовищі, дестабілізують державні процеси, призводять до істотних змін у суспільній свідомості.

Розроблена класифікація загроз інформаційній безпеці держави у СІС демонструє широке різноманіття небезпек, які виникають у віртуальних спільнотах, а їх кількість постійно зростає. Отже, відповідно до запропонованого підходу класифікації загрози інформаційній безпеці держави у СІС формалізують у вигляді кортежа $D=\langle R,S,C,T,M,F,Sr,P,I\rangle$. Своєчасне детектування таких загроз забезпечить ефективність функціонування систем забезпечення інформаційної безпеки держави і розробку дієвих методів протидії загрозам у СІС.

Висновки. Запропонована класифікація загроз інформаційній безпеці держави у СІС дозволяє формалізувати процеси їх виявлення у СІС, підвищити швидкодію і ефективність систем забезпечення інформаційної безпеки держави. Перевагами розглянутого підходу до класифікації загроз є врахування особливостей процесів функціонування СІС і взаємодії акторів у віртуальних спільнотах, актуальність сучасним викликам інформаційній безпеці держави, можливість подальшого розширення залежно від досліджуваного виду СІС чи необхідної глибини класифікації. Напрямок подальших досліджень полягає в розробленні методики оцінювання ступеня загроз інформаційній безпеці держави в СІС.

Література

1. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства: [монографія] / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.]. – К.: НАН України, Нац. б-ка України ім. В.І. Вернадського, 2014. – 260 с.

2. Earl J. Digitally Enabled Social Change: Activism in the Internet Age / J. Earl, K. Kimport. – Cambridge: MIT, 2011. – 170 p.

3. Tufekci Z. Social media and the decision to participate in political protest: observations from Tahrir Square / Z. Tufekci, C. Wilson. // J. Commun. – 2012. – №62(2). – PP.363-379.

4. González-Bailón S. Networked discontent: The anatomy of protest campaigns in social media / S. González-Bailón, N. Wang // Social Networks. – 2016. – №44. – PP.95-104.

5. Соціальні мережі як чинник інформаційної безпеки. Інформаційно-аналітичний бюлетень: [електронний ресурс] / Центр досліджень соціальних комунікацій. – Режим доступу: http://nbuviap.gov.ua/index.php?option=com_content&view=category&layout=blog&id=26&Itemid=187 (дата звернення: 07.03.16). – Назва з екрану.

6. Гриненко І. Вплив віртуальних спільнот на інформаційну безпеку: сучасний стан та тенденції розвитку / І. Гриненко, Д. Прокоф'єва-Янчиленко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – №1(23). – С.18-23.

7. Соціокультурні механізми формування ментального імунітету проти зовнішніх маніпуляцій свідомістю населення України : [монографія] / [В. Горовий, О. Онищенко, В. Попик та ін.]. – К.: НАН України, Нац. б-ка України ім. В.І. Вернадського, 2015. – 228 с.

8. Грищук Р.В. Прогнозування динаміки поширення контенту й запитів на нього, за даними контент-аналізу повідомлень у соціальних інтернет-сервісах / Р.В. Грищук, К.В. Молодецька // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: II міжнар. наук.-практ. конф., 24-27 лют. 2016 р. – К.: Вид-во Європейського ун-ту, 2016. – С.58-59.

9. Бурячок В.Л. Політика інформаційної безпеки: підручник / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко, під заг. ред. проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

10. Закон України «Про інформацію»: [Електронний ресурс] / Офіційний портал Верховної ради України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2657-12 (дата доступу: 07.03.16). – Назва з екрану.

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

12. 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.

13. Проект Указу Президента «Про Доктрину інформаційної безпеки України»: [Електронний ресурс] / Сайт державного комітету телебачення і радіомовлення України. - Режим доступу: ИіІр://comin.ктu.£оУ.ua/conIгoI/ик/puЬИMагIicIe?агI i(1-113319&caі_id~61025 (дата звернення: 07.03.16). - Назва з екрану.

14. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення: [монографія] / В.А. Ліпкан. - К.: Текст, 2003. - 180 с.

15. Ознаковий принцип формування класифікацій кібератак / О.Г Корченко, С.В. Казмірчук, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий//Вісн. СНУ ім. В. Даля. - 2010. - М 4 , Т.1. - С.184-193.

16. Пелещишин А.М. Загрози інформаційної безпеки держави в соціальних мережах / А.М. Пелещишин, Р.В. Гумінськмй // Наука і техніка Повітряних Сил Збройних Сил України. - 2013. -М 2 . - С. 192-199.

17. Протидія інформаційним війнам: інформація як щит і меч / Уклад.: Г. Буркацька, А. Саприкін; підред.: С. Чачко, В. Кучерявої, Н. Лінкевич. - К : «Держ. б-ка України для юнацтва». 2014. - 54 с.

18. Грищук Р.В. Диференціально-ігрові моделі та методи моделювання процесів кібернападу: дис. ... д-ра техн. наук: 21.05.01 / Грищук Руслан Валентинович: Нац. авіац. ун-т. - Київ, 2013. - 441 с.

19. Марущак А.І. Пріоритети розвитку інформаційного права України / А.І. Марущак / / Інформація і право. - 2011. - М І. - С.20-24.

20. Пилипчук В.Г. Системні проблеми розвитку правової науки в інформаційній сфері / В.Г. Пилипчук // Вісник Академії правових наук України. - 2011. - М3. - С. 16-27.

21. Широкова-Мурараш О.Г. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-правовий аспект / О.Г. Широкова-Мурараш, Ю.Р. Акчурін //Інформація і право. - 2011. -М І. - С. 76-82.

22. Проект Концепції інформаційної безпеки України: [електронний ресурс] / Офіційний сайт Міністерства інформаційної політики України. - Режим доступу: Ніір://mip.£oy.ua/<1ocumen1$/30.кіт1 (дата звернення: 07.03.2016). - Назва з екрану.

23. Кухарська Н.П. Вплив соціальних мереж на корпоративну інформаційну та економічну безпеку / Н.П. Кухарська, В.М. Кухарський / / Вісн. Нац. ун-ту «Львів, політехніка». - 2012. - Т. 741. - С.214-217.

24. Грищук Р.В. Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах / Р.В. Грищук, К.В. Молодецька // Безпека інформації. - 2015. - Т.21, Ч.ІІ. – С.123-130.

25. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева, Є.Д. Скулиш, О.Д. Бойко, В.В. Остроухов]; за заг. ред. С.Д. Скулиша. -- К.: ЗАТ "ВІПОЛ", 2011. - 248 с.

26. Основи побудови автоматизованих систем управління: навч. посіб. / І.А. Пількевич, К.В. Молодецька, І.І. Сугоняк, Н.М. Лобанчикова. – Житомир : ЖДУ ім. І. Франка, 2014. - 174 с.