УДК 004.738.5:004.056.5(045)

Молодецька-Гринчук Катерина Валеріївна
Кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій і моделювання систем, *orcid.org/0000-0001-9864-2463*
Житомирський національний агроекологічний університет, Житомир

АНАЛІЗ ВПЛИВУ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ НА СФЕРИ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ

Анотація. *Соціальні інтернет-сервіси (СІС) перетворилися на ефективний інструмент взаємодії учасників віртуальних спільнот – акторів. Серед основних комунікаційних переваг СІС виділяють наявність засобів обміну контентом і координації взаємодії акторів, тому їх використовують у процесах самоорганізації громадянського суспільства. У випадку поширення неповного, недостовірного або викривленого контенту СІС перетворюються на джерело загроз інформаційній безпеці держави. Стратегічні дії для забезпечення національної безпеки у інформаційній сфері сформульовані в Доктрині інформаційної безпеки України. Однак, практичні рекомендації для реалізації сформульованих у Доктрині вимог, їх уточнення, координація додатково не задекларовані. Це призводить до відсутності дієвих методик протидії загрозам у СІС. У статті проведено аналіз загроз інформаційній безпеці держави і визначено життєво важливі інтереси особистості, суспільства, держави у СІС. Визначено наслідки реалізації загроз у СІС в розрізі сфер суспільної діяльності, що дозволило сформулювати концептуальний базис протидії. Запропоновано здійснювати взаємодію держави з громадськими організаціями у галузі інформаційної безпеки для координації протидії загрозам та подальшої побудови ефективної системи забезпечення інформаційної безпеки держави у СІС.*

Ключові слова: соціальні інтернет-сервіси; загрози; доктрина; інформаційна безпека держави; сфери суспільної діяльності

Вступ

Наслідком впровадження інформаційних технологій у всі галузі людської діяльності стала трансформація суспільних відносин, зокрема, у галузі комунікацій [1]. Особистість одночасно перетворилася на об'єкт і суб'єкт соціальних комунікацій, а масштабний доступ до інформаційних ресурсів, наявність інструментів генерації нового контенту, транскордонність процесів взаємодії призвели до глобалізації інформаційного простору [2]. Результатом таких процесів стала поява негативних наслідків, які пов'язані з інформаційною безпекою держави [2; 3]: перенесення конфліктів між провідними державами світу в інформаційний простір; розв'язування інформаційного протиборства; виникнення нового виду катастроф у зв'язку з помилками або втручанням у функціонування інформаційно-телекомунікаційних систем та мереж; розвиток кіберзлочинності; вплив на засоби масової комунікації (ЗМК) та маніпуляція суспільною думкою.

У свою чергу, суттєва роль у ході трансформації інформаційного простору відводиться соціальним інтернет-сервісам (СІС) завдяки ефективній реалізації соціальних комунікацій їх користувачів – акторів, наявності засобів самоорганізації громадянського суспільства для впливу на політичні й суспільні процеси у державі тощо. Однак, контент, який поширюється у СІС може мати недостовірний, неповний або упереджений характер і становити загрозу інформаційній безпеці особистості, суспільства, держави. З огляду на зростання кількості нових загроз інформаційній безпеці держави у СІС виникає проблема розподілу і координації функцій захисту в інформаційній сфері між органами влади та силовими структурами для побудови ефективної системи забезпечення інформаційної безпеки держави [4]. Тому встановлення особливостей впливу загроз інформаційній безпеці у СІС на окремі сфери суспільної діяльності як підґрунтя для їх подальшої оцінки і протидії є актуальним теоретико-прикладним завданням на шляху вирішення проблеми розроблення ефективної системи забезпечення інформаційної безпеки держави.

Аналіз останніх досліджень і публікацій показав, що сьогодні в Україні створено законодавче підґрунтя для регулювання інформаційного середовища держави, його розвитку і захисту від деструктивних інформаційних впливів [1-6]. Однак, залишаються неврегульованими ряд проблем у інформаційній галузі, зокрема питання

інформаційної взаємодії у СІС, недостатній рівень врахування у нормативно-правовому забезпеченні сучасних загроз і викликів інформаційній безпеці держави [6]. Фундаментальне значення для протидії сучасним інформаційним загрозам має затвердження Доктрини інформаційної безпеки України указом Президента України №47/2017 від 25 лютого 2017 року. Метою даної законодавчої ініціативи є «уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни» [7]. Даний нормативно-правовий документ окреслює стратегічні дії для забезпечення національної безпеки у інформаційній сфері. Однак, вироблення практичних рекомендацій для реалізації сформульованих у ньому вимог, їх уточнення, координація мають бути задекларовані додатково [4]. Отже, виникає об'єктивне протиріччя між сучасним рівнем загроз інформаційній безпеці держави і науковим базисом протидії для створення й ефективного функціонування системи забезпечення інформаційної безпеки у СІС, що додатково актуалізує обраний напрям досліджень.

Мета статті

Метою статті є аналіз впливу загроз на сфери суспільної діяльності для вироблення концептуального базису протидії та побудови ефективної системи забезпечення інформаційної безпеки держави у СІС.

Для досягнення поставленої мети необхідно розв'язати окремі задачі:

– визначити перелік актуальних загроз інформаційній безпеці держави;

– проаналізувати життєво важливі інтереси особистості, суспільства, держави у СІС;

– визначити наслідки реалізації загроз інформаційній безпеці держави у СІС в розрізі сфер суспільної діяльності;

– сформулювати концептуальний базис протидії загрозам інформаційній безпеці держави у СІС з урахуванням різних сфер суспільної діяльності.

Виклад основного матеріалу

У чинній Доктрині інформаційної безпеки України визначено, що актуальними загрозами національним інтересам та національній безпеці в інформаційній сфері є такі [7]:

– здійснення спеціальних інформаційних операцій, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури;

– неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Досвід показує, що для розповсюдження інформації використовуються засоби масової інформації (ЗМІ). Залежно від каналу поширення ЗМІ поділяють на друковані, аудіовізуальні та електронні. У сучасних умовах найбільш популярними є електронні ЗМІ, які інтегрують у собі характеристики друкованих та аудіовізуальних ЗМІ. У аналітичній записці Інституту стратегічних досліджень [8] встановлено, що нормативно-правовий статус і діяльність Інтернет-ЗМІ недостатньо регулюються на державному рівні. Такий стан інформаційного простору держави призводить до ускладнення процесів розвитку інформаційної сфери і створює умови для зростання числа загроз інформаційній безпеці держави.

Дослідження [1; 2; 9–13] показують, що одним із найбільш дієвих джерел загроз інформаційній безпеці держави є СІС, які являють собою платформу або веб-сайти, призначені для створення соціальних мереж або соціальних взаємозв'язків між людьми. СІС одночасно належать до ЗМК і ЗМІ як інструмент обміну й поширення контенту та звернення до масової аудиторії. Під час «Кольорових революцій», «Арабської весни», гібридної війни з Російською Федерацією на сході України та ряду протестних акцій СІС продемонстрували провідну роль в організації громадян, їх комунікації та управлінні взаємодією. Серед найбільш дієвих СІС, які використовуються зловмисниками для проведення спеціальних інформаційних операцій, зазначимо соціальні мережі, блоги і медіа-сховища [9]. Успішність застосування вказаних СІС для реалізації загроз інформаційній безпеці держави пов'язана із самостійною генерацією контенту актором для наповнення свого профілю, утворенням зв'язків з іншими акторами і віртуальними спільнотами,

використанням інструментів створення об'єднань акторів для втілення суспільних перетворень офлайн [10–13].

Визначені у [1; 7; 12; 13; 15–17] класи загроз національним інтересам і національній безпеці у СІС в інформаційній сфері спрямовуються проти особистості, суспільства й держави. З [7] відомо, що інтереси особистості у інформаційній сфері зводяться до реалізації конституційних прав на доступ до інформації, її законного використання у процесі діяльності й інтелектуального розвитку, забезпечення захисту інформації як складової особистої безпеки, а також захисту від руйнівних інформаційно-психологічних впливів. Реалізація загроз інформаційній безпеці особистості у СІС може призвести до впливу на психічний та емоційний стан акторів віртуальних спільнот, їх свободу вибору, маніпуляцій свідомістю, несанкціонованого накопичення і використання персональних даних акторів й інформації про їх особисте життя.

У свою чергу, до життєво важливих інтересів суспільства у [7] належить його захист від агресивної пропаганди, забезпечення доступу до об'єктивної і достовірної інформації, розвиток медіа-культури суспільства та соціально відповідального медіа-середовища, збереження духовних, культурних і моральних цінностей народу, розвиток й функціонування української мови та інші. Серед життєво важливих інтересів держави у інформаційній сфері [7] виділяють розвиток і захист національної інформаційної інфраструктури, формування ефективної системи захисту від деструктивних пропагандистських впливів, розвиток інформаційно-телекомунікаційних технологій та інформаційних ресурсів України, забезпечення взаємодії органів державної влади та інститутів громадянського суспільства тощо.

Вплив загроз інформаційній безпеці особистості, суспільства, держави у СІС безпосередньо проявляється не тільки у інформаційній, але й в усіх інших сферах суспільної діяльності. У монографії [1] досліджено тісний взаємозв'язок соціальної, економічної, політичної, воєнної та духовної сфер і вказано їх роль для функціонування та сталого розвитку суспільства й кібернетичної безпеки. Дія визначених у Доктрині інформаційної безпеки України загроз через СІС на інформаційну сферу призводить до змін у функціонуванні компонентів інших сфер діяльності й суспільства та держави в цілому. Реалізація розглянутих загроз проявляється такими наслідками у розрізі сфер суспільної діяльності [7; 13; 16]:

1) соціальної:

– поширення і підживлення панічних настроїв, загострення і дестабілізація суспільно–політичної ситуації;

– розпалювання міжетнічних конфліктів;

– невизначеність стратегічного наративу;

– недостатній рівень медіа–культури суспільства;

2) економічної:

– порушення порядку доступу, поводження та встановлених регламентів збирання, обробки, зберігання, поширення чи передачі інформації, яка захищається державою або роботи з інформаційними ресурсами;

– поширення соціально–економічної напруженості;

– недостатній рівень захищеності об'єктів критичної інфраструктури держави;

3) політичної:

– проведення спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– поширення закликів до сепаратизму, радикальних дій, повалення конституційного ладу чи порушення територіальної цілісності держави;

– поширення викривленої, недостовірної та упередженої інформації для дискредитації органів державної влади;

4) воєнної:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань;

– ведення розвідувальної діяльності;

5) духовної:

– поширення ідей моральної та духовної деградації суспільства;

– розпалювання міжконфесійних конфліктів.

У результаті аналізу нормативно–правових документів [7; 14; 16] встановлено, що виконання функцій координації діяльності державних органів з протидії загрозам інформаційній безпеці держави, зокрема у СІС, покладено на Раду національної безпеки і оборони. Реалізацію державної інформаційної політики і координацію міністерств та інших органів виконавчої влади виконує Кабінет Міністрів України. Ключовим органом виконавчої влади у сфері забезпечення інформаційного суверенітету України є Міністерство інформаційної політики України (МІПУ) [18].

Відповідно до Доктрини інформаційної безпеки держави [7], діяльність МІПУ у розрізі протидії загрозам у СІС зводиться до моніторингу з метою виявлення забороненого контенту та загроз національним інтересам і національній безпеці, урядові комунікації, кризові комунікації, імплементація стратегічного наративу. У свою чергу, Міністерство закордонних справ України (МЗСУ) із використанням СІС реалізує координацію інформаційної діяльності у зовнішньополітичній

сфері, донесення позиції України до широкої громадськості, просування її інтересів за кордоном.

Перед Міністерством оборони України (МОУ) поставлено завдання висвітлення, зокрема засобами СІС, ситуації у зоні проведення антитерористичної операції та завдань, які виконує МОУ, протидії інформаційним операціям проти військовослужбовців. Служба безпеки України (СБУ) проводить моніторинг СІС для виявлення загроз інформаційній безпеці держави, протидію для реалізації інформаційних операцій націлених на підрив конституційного ладу, порушення суверенітету, територіальної цілісності та поширення соціально-економічної й суспільно-політичної напруженості. Розвідувальні органи України реалізують протидію загрозам інформаційний безпеці держави, джерелами яких є іноземні держави, і сприяють захисту національних інтересів у СІС. Створення якісного контенту для поширення у СІС для реалізації протидії пропаганді та висвітлення боротьби з агресією Російської Федерації покладено на Міністерство культури України (МКУ), Державне агентство України з питань кіно, Національну раду України з питань телебачення і радіомовлення та Державний комітет телебачення і радіомовлення України.

Таким чином, в узагальненому вигляді концептуальний базис протидії загрозам інформаційній безпеці держави у СІС у різних сферах суспільної діяльності показано на рисунку.

Функції протидії загрозам інформаційній безпеці держави у СІС, які впливають на розглянуті сфери суспільної діяльності (рисунок), на законодавчому рівні розподілені між відповідними центральними державними органами та сектором безпеки і оборони.

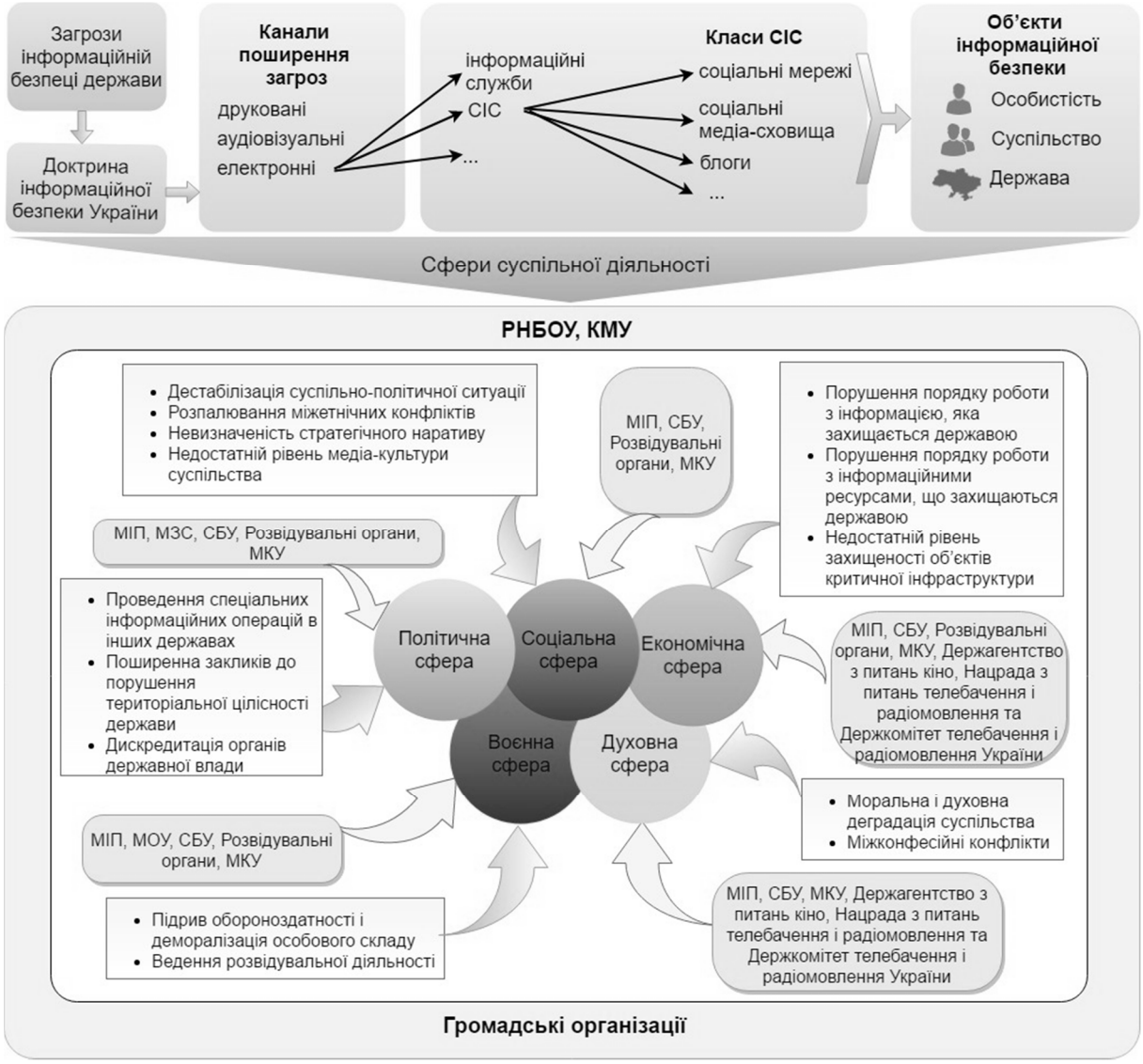

Рисунок – Концептуальний базис протидії загрозам інформаційній безпеці держави у СІС

Ключовою вимогою ефективності їх діяльності є гнучкість процесів взаємодії та координації суб'єктів інформаційної безпеки. Врахування цих принципів забезпечує оперативність процедур виявлення, оцінки і прийняття адекватних заходів протидії загрозам, ефективність перерозподілу ресурсів між державними органами за умови зміни або уточнення цілей системи забезпечення інформаційної безпеки держави у СІС. Однак, у Доктрині інформаційної безпеки України не вказано механізмів і засобів реалізації взаємодії центральних державних органів та сектору безпеки і оборони [4]. В умовах сьогодення ефективною виявилася модель взаємодії держави у галузі інформаційної безпеки з громадськими організаціями і волонтерськими проектами, наприклад «Інформнапалм», «СтопФейк», «Детектор медіа» та інші [4]. Тому нормативно–правове регулювання процедур залучення громадських організацій до діяльності державних органів у інформаційній сфері визначає напрям підвищення ефективності функціонування системи забезпечення інформаційної безпеки держави у СІС.

Висновки

У статті визначено наслідки реалізації загроз інформаційній безпеці держави в розрізі їх впливу на різні сфери суспільної діяльності, сформульовано концептуальний базис протидії загрозам інформаційній безпеці особистості, суспільства, держави у СІС. Встановлено, що ефективним інструментом є модель взаємодії держави у галузі інформаційної безпеки з громадськими організаціями і волонтерськими проектами для координації протидії загрозам у СІС.

Напрям подальших досліджень полягає в розробці моделей оцінки впливу загроз на окремі сфери суспільної діяльності для реалізації їх своєчасного виявлення і нейтралізації засобами системи забезпечення інформаційної безпеки держави у СІС.

Список літератури

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

2. Технології розвитку і захисту національного інформаційного простору : [монографія] / [О. Онищенко, В. Горовий, В. Попик та ін.] ; НАН України, Нац. б–ка України ім. В. І. Вернадського. – К., 2015. – 296 с.

3. Леонов А. П. Актуальные проблемы информационной безопасности в контексте глобализации [Электронный ресурс] / А. П. Леонов. – Режим доступа: http://www.itsec.ru/doc/leonov.doc. – Загл. с экрана.

4. Попова Т. Що означає «Доктрина інформаційної безпеки України»? : [Електронний ресурс] / Офіційний сайт «Радіо свобода». – Режим доступу : http://www.radiosvoboda.org/a/28337376.html. – Назва з екрану.

5. Гурковський В. І. Організаційно–правові засади забезпечення інформаційно–психологічної безпеки в контексті дослідження функціонування традиційних і конвергентних медіа / В. І. Гурковський // Ефективність державного управління. – 2014. – Вип. 40. – С. 116–125.

6. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання : аналітична доповідь // В. К. Конах ; Нац. ін–т стратег. дослідж. – К., 2013. – 49 с.

7. 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. – Назва з екрану.

8. Конах В. К. Інтернет–ЗМІ в Україні: проблеми визначення нормативно–правового статусу та врегулювання : [Електронний ресурс] / В. К. Конах. – Сайт офіційного представництва інституту стратегічних досліджень. – Режим доступу: http://www.niss.gov.ua/articles/1085/#_ftn2. – Назва з екрану.

9. 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.

10. Федушко С. С. Розроблення алгоритму визначення адекватності даних інформаційного образу учасника віртуальних спільнот / С. С. Федушко, Д. В. Мельник // Управління розвитком складних систем. – 2016. – № 27. – С. 132 – 138.

11. Єгорченков О. В. Оптимізація управління інформацією в продуктових системах управління проектами / О. В. Єгорченков, О. Б. Лисищін, Д. С. Катаев // Управління розвитком складних систем. – 2013.– №13. – С. 28–31.

12. Гумінський Р. В. Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж : дис. … канд. техн. наук : 21.05.01 / Гумінський Руслан Вікторович. – Київ, 2016. – 157 с.

13. Молодецька К. В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет–сервісах / К. В. Молодецька // Защита информации. – 2016. – Вып. 23. – С. 75–87.

14. Закон України «Про основи національної безпеки України» (редакція від 07.08.2015) : [Електронний ресурс] / Офіційний портал Верховної Ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/964–15. – Назва з екрану.

15. 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.

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

17. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – Київ : МК–Прес, 2005. – 432 с.

18. Офіційний сайт Міністерства інформаційної політики України. – Режим доступу: http://mip.gov.ua. – Назва з екрану.

Стаття надійшла до редколегії 11.04.2017

Рецензент: д–р техн. наук, професор І. Г. Грабар, Житомирський національний агроекологічний університет, Житомир.

Молодецкая–Гринчук Катерина Валерьевна
Кандидат технических наук, доцент, доцент кафедры компьютерных технологий и моделирования систем, orcid.org/0000–0001–9864–2463
Житомирский национальный агроэкологический университет, Житомир

АНАЛИЗ ВЛИЯНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ НА СФЕРЫ ОБЩЕСТВЕННОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. *Социальные интернет–сервисы (СИС) превратились в эффективный инструмент взаимодействия участников виртуальных сообществ – актёров. Среди основных коммуникационных преимуществ СИС выделяют наличие средств обмена контентом и координацию взаимодействия актёров, поэтому их используют в процессах самоорганизации гражданского общества. В случае распространения неполного, недостоверного или искаженного контента СИС превращаются в источник угроз информационной безопасности государства. Стратегические действия для обеспечения национальной безопасности в информационной сфере сформулированы в Доктрине информационной безопасности Украины. Однако, практические рекомендации для реализации сформулированных в Доктрине требований, их уточнение, координация дополнительно не задекларированы. Это приводит к отсутствию действенных методик противодействия угрозам в СИС. В статье проведен анализ угроз информационной безопасности государства и определены жизненно важные интересы личности, общества, государства в СИС. Установлены последствия реализации угроз в СИС в разрезе сфер общественной деятельности, что позволило сформулировать концептуальный базис противодействия. Предложено осуществлять взаимодействие государства с общественными организациями в области информационной безопасности для координации противодействия угрозам и дальнейшего построения эффективной системы обеспечения информационной безопасности государства в СИС.*

Ключевые слова: социальные интернет–сервисы; угрозы; доктрина; информационная безопасность государства; сферы общественной деятельности

Molodetska–Hrynchuk Kateryna
Candidate of Engineering Sciences, Associate Professor, Associate Professor of IT and Simulation Department, orcid.org/0000–0001–9864–2463
Zhytomyr National Agro–Ecological University, Zhytomyr

ANALYSIS OF INFLUENCE THREATS OF AN INFORMATION SECURITY OF THE STATE IN A SOCIAL INTERNET–SERVICE TO THE SPHERES OF PUBLIC ACTIVITIES

Abstract. *Social networking services (SNS) have become an effective tool of actor's interaction. The main communication advantages of SNS are content sharing and interaction coordination between actors, as they are used in the processes of self-organization of civil society. If the content is incomplete, inaccurate or distorted then SNS became a source of threats to information security. Strategic actions for ensuring national security at the information sphere set out on Information Security Doctrine of Ukraine. However, practical guidelines for the implementation of requirements contained in the Doctrine, their refinement, additional coordination is not declared. This causes to a lack of effective methods of countering threats in SNS. In the article are analyzed the state of information security threats and defined vital interests of the individual, society and state in the SNS. It is established consequences of threats in the SNS in terms of spheres of social activity that allowed to formulate the conceptual basis of counter. Differentiated responsibilities of government agencies to develop counter threats to information security. Proposed implementation of interaction among government agencies with civil society organizations in the area of information security to coordinate counter threats and further an effective system to ensure information security in SNS.*

Keywords: social networking services; threats; doctrine; information security; spheres of social activity

References

1. Hryshchuk, R. & Danyk, Y. (2016). Fundamentals of cyber security. Zhytomyr, Ukraine: ZhNAEU.

2. Onyshchenko, O., Horovyi, V., & Popyk, V. (2015). Technology development and protection of the national information space. Kyiv, Ukraine: NAN Ukrainy, Nats. b–ka Ukrainy im. V. I. Vernadskoho.

3. Leonov, A. (n.d.) Aktualnye problemy informatsionnoi bezopasnosti v kontekste globalizatsii [Topical problems of information security in the context of globalization]. Retrieved from http://www.itsec.ru/doc/leonov.doc.

4. Popova, T. (2017). What does the "Information Security Doctrine of Ukraine" means? [Web log post]. Retrieved April 8, 2017, from http://www.radiosvoboda.org/a/28337376.html.

5. Hurkovskyi, V. (2014). Organizational and legal bases providing information and psychological security operation in the context of the study of traditional and converged media. Efektyvnist derzhavnoho upravlinnia, 40, 116–125.

6. Konakh, V. (2013). National information space of Ukraine: problems of formation and state regulation analytical report. Kyiv, Ukraine: Nats. in–t strateh. doslidzh.

7. Ukraine, An official of President of Ukraine. (2017, February 25). Information Security Doctrine of Ukraine. Retrieved April 8, 2017, from http://www.president.gov.ua/documents/472017–21374.

8. Konakh, V. (n.d.). Internet media in Ukraine: the problem of determining the legal status and resolution [Web log post]. Retrieved from http://www.niss.gov.ua/articles/1085/#_ftn2.

9. Molodetska, K. (2016). Social Internet services as an information security. Information Technology and Security, 4(1(6)), 13–20 [in Ukrainian].

10. Fedushko, S., & Melnyk, D., (2016). Development of algorithm of adequacy data determination for virtual communities member' information image. Management of development of difficult systems, 27, 132–138 [in Ukrainian].

11. Yehorchenkov, V., Lysytsin, O., & Kataev, D. (2013). Optimize information management in food systems project management. Management of development of difficult systems, (13), 28–31 [in Ukrainian].

12. Huminskyi, R. (2016). Methods and detection of information threats virtual communities in online social networking environment [Metody i zasoby vyiavlennia informatsiinykh zahroz virtualnykh spilnot v internet seredovyshchi sotsialnykh merezh]. Extended abstract of candidate's thesis. Kyiv: NAU [in Ukrainian].

13. Molodetska, K. (2016). Generalized classification of information security threats to the state social networking services [Uzahalnena klasyfikatsiia zahroz informatsiinii bezpetsi derzhavy v sotsialnykh internet–servisakh]. Zashchyta ynformatsyy, (23), 75–87 [in Ukrainian].

14. Zakon Ukrainy «Pro osnovy natsionalnoi bezpeky Ukrainy» [The Law of Ukraine "On National Security of Ukraine"]. (7 August 15). Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine. Kyiv: Parlam. vyd–vo [in Ukrainian].

15. Lipkan, V., Maksymenko, Y., & Zhelikhovskyi, V. (2006). Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii. Kyiv: KNT.

16. Proekt Kontseptsii informatsiinoi bezpeky Ukrainy [Draft Concept of information security Ukraine]. Ofitsiinyi sait Ministerstva informatsiinoi polityky Ukrainy – Official site of the Ministry of Information Policy of Ukraine. Retrieved from http://mip.gov.ua/documents/30.html.

17. Bohush, V., & Yudin, O. (2005). Informatsiina bezpeka derzhavy. Kyiv: MK–Pres.

18. Ofitsiinyi sait Ministerstva informatsiinoi polityky Ukrainy – The official website of the Ministry of Information Policy of Ukraine. Retrieved from http://mip.gov.ua.

Посилання на публікацію

APA *Molodetska-Hrynchuk, Kateryna, (2017). Analysis of influence threats of an information security of the state in a social internet–service to the spheres of public activities. Management of Development of Complex Systems, 30, 121–127.*

ГОСТ *Молодецька-Гринчук, К. В. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності / К. В. Молодецька-Гринчук // Управління розвитком складних систем. – 2017. – № 30. – С. 121–127.*