ПІДХІД ДО КЛАСИФІКАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Молодецька К. В.
Житомирський національний агроекологічний університет

Анотація. На сучасному етапі розвитку високотехнологічного суспільства соціальні інтернет-сервіси (СІС) є ефективним засобом комунікації і суб'єктом інформаційного простору держави. Окрім позитивних комунікаційних характеристик СІС є джерелом загроз, які націлені на акторів віртуальних спільнот. Встановлено, що існуючі класифікації загроз інформаційній безпеці держави характеризують їх у аспекті функціонування інформаційно-комунікаційних систем чи складової інформаційного простору держави. З метою розробки ефективних методів протидії загрозам інформаційній безпеці держави в СІС розроблено їх узагальнену класифікацію. Перевагою запропонованого підходу є врахування особливостей функціонування СІС і взаємодії акторів у віртуальних спільнотах, актуальність сучасним викликам інформаційній безпеці держави, можливість додавання класифікаційних ознак та груп для подальшого розширення чи досягнення заданого рівня глибини класифікації.

Ключові слова: соціальні інтернет-сервіси, актори, загрози, класифікація, інформаційна безпека держави.

APPROACH TO THE CLASSIFICATION OF THREATS TO INFORMATION SECURITY OF THE STATE IN SOCIAL NETWORKING SERVICES

Molodetska K.
Zhytomyr National Agro-Ecological University

Abstract. At the present stage of development of high-tech society social networking services (SNS) is an effective means of communication and the subject of the information space of the state. In addition to positive communication specifications SNS is a source of threats aimed at actors virtual communities. It was established that the existing classification of state information security threats characterize them in terms of the functioning of information and communication systems or part of the information space of the state. In order to develop effective methods to counter threats to information security of the state in SNS developed their generic classification. The advantage of the proposed approach is to take account of the functioning of SNS actors and interaction in virtual communities, relevance to contemporary challenges of information security of the state, the ability to add classifications and groups to further expand or achieve a given level of depth of classification.

Keywords: social Internet services, actors, threat classification, information security state.

Вступ. Соціальні інтернет-сервіси (СІС) використовуються учасниками віртуальних спільнот – акторами, не тільки для спілкування, поширення і обміну контентом різного типу, але й поступово перетворюються в ефективний інструмент суспільних перетворень, створення об'єднань громадян тощо [1]. Позитивні комунікаційні властивості СІС можуть бути використані зловмисниками для реалізації власних інтересів шляхом поширення у віртуальних спільнотах недостовірного, неповного чи упередженого контенту. Наслідком таких дій може бути виникнення передумов маніпулюванню індивідуальною або масовою свідомістю громадян з метою поширення у суспільстві соціальної напруженості, міжнаціональної ворожнечі, протестних настроїв тощо. Недостатній рівень теоретичного розроблення класифікації видів загроз у СІС ускладнює процедури реалізації дієвої протидії загрозам, тому є актуальним теоретико-прикладним завданням для вирішення проблеми забезпечення інформаційної безпеки (ІБ) людини, суспільства, держави.

Постановка задачі. Проведення наукових досліджень у обраному напрямку ускладнюється відсутністю прийнятого нормативно-правового забезпечення для розробки дієвих механізмів впливу на інформаційний простір СІС на державному рівні. Тому класифікація загроз ІБ держави в СІС є особливо актуальною і потребує подальшого

дослідження. Для цього необхідно розв’язати такі частинні задачі: аналіз існуючих наукових підходів до класифікації загроз ІБ держави; визначення загроз ІБ держави в СІС; розробка нового підходу до узагальненої класифікації загроз ІБ держави в СІС і їх формалізація.

Мета досліджень полягає в аналізі загроз ІБ держави в СІС і розробці узагальненої класифікації для реалізації ефективного їх виявлення та протидії.

Основна частина. Стратегія кібербезпеки України визначає кібернетичну загрозу як наявні та потенційно можливі явища і чинники, що загрожують кібернетичній безпеці. Серед вітчизняних вчених проблема класифікації загроз ІБ держави представлена в працях О. Г. Корченка, В. А. Ліпкана, Р. В. Грищука та інших [2-4]. Розглянуті класифікації загроз ІБ держави сформульовані у розрізі кібербезпеки, безпеки інформаційно-комунікаційних систем, національної безпеки, однак не враховують особливості функціонування СІС і взаємодії акторів у віртуальних спільнотах, нових викликів ІБ громадянина, суспільства, держави у СІС, пов'язаних з гібридною війною і агресією Російської Федерації.

Узагальнюючи відомі підходи [2-4] до класифікації загроз ІБ держави, особливості функціонування і взаємодії акторів віртуальних спільнот у СІС як об’єкта державного інформаційного простору, запропоновано авторський підхід до класифікації загроз ІБ держави в СІС, що не суперечить матеріалам інших досліджень. Встановлено такі основні ознаки класифікації загроз ІБ в СІС:

1. По відношенню до акторів СІС виділяють: внутрішні і зовнішні загрози.

2. За видами суб’єктів загроз: іноземні держави; групи осіб; окремі особи.

3. За характером загрози по відношенню до СІС: комунікаційні і технологічні.

4. Залежно від мети загрози: вплив на психічний і емоційний стан акторів СІС; вплив на свободу вибору акторів у прийнятті будь-яких рішень від зовнішніх факторів; заклики до сепаратизму, повалення конституційного ладу, порушення територіальної цілісності; дискредитація органів державної влади, наслідком якої є ускладнення процесів прийняття політичних рішень, створення негативного іміджу держави, шкода національним інтересам; підтримка, супроводження чи активізація злочинної або терористичної діяльності.

5. За способом дії загрози у СІС: інформаційні впливи через СІС; несанкціонований доступ і кібератаки на аккаунти в СІС керівників держави, лідерів громадської думки тощо; розголошення інформації з обмеженим доступом у СІС; розповсюдження шкідливого програмного забезпечення; розвідувальна діяльність у СІС.

6. За частотою повторюваності: одноразові; повторювані; продовжувані.

7. За прихованістю прояву: латентні і явні.

8. За можливістю реалізації: потенційні; реальні; реалізовані; псевдореальні.

9. За рівнем впливу на акторів і віртуальних спільноти СІС: допустимі і недопустимі.

Висновки. Запропонована класифікація загроз ІБ держави у СІС дозволяє формалізувати процеси їх виявлення у СІС, підвищити швидкодію і ефективність систем забезпечення ІБ держави.

Список використаних джерел

1. Онищенко О. С., Горовий В. М., Попик В. І. Соціальні мережі як інструмент взаємовпливу влади та 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., 2014. – 260 с.

2. Корченко О. Г., Казмірчук С. В., Паціра Є. В., Гнатюк С. О., Кінзерявий В. М. 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. – №4, т. 1. – С. 184–193.

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

4. 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. – 411 с.