УДК 329.09.5 (477)

Чижевська М.Б., к.е.н., доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)
Романовська Н.І., к.е.н., доцент
Венгер В.В., д.е.н., с.н.с.
ДУ «Інститут економіки та прогнозування НАН України», (м. Київ, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

XXI століття характеризуються бурхливим розвитком інформаційних мереж, активний сплеск яких припадає на останні роки, які стали знаковими у зміні парадигми суспільних комунікацій, що спричинило активізацію їх цифровізації.

Цивілізація вступила в еру інформаційного суспільства, в якому інформація стає вирішальним чинником у багатьох сферах життєдіяльності. Сьогодні практично неможливо знайти площину соціальної активності, яка б не зазнала впливу інформаційних технологій: політика, право, економіка, медицина, освіта, культура, релігія, сфера послуг і розваги [1].

Не викликає заперечень той факт, що інформаційна сфера стала системоутворюючим фактором життя суспільства й активно впливає на стан політичної, економічної, оборонної та інших складових частин безпеки країни, нові загрози стають набагато масштабнішими, ніж раніше. І головною метою інформаційної безпеки як ніколи постає проблема забезпечення безперервності функціонування держави, захищення інформаційних даних та інфраструктури від випадкового або навмисного втручання, що може стати причиною втрати даних або їх несанкціонованої зміни.

Розглядаючи проблему інформаційної безпеки, важливо виділити загрози для інформаційної безпеки - явища, дії факторів, що мають негативний характер або процеси, що зумовлюють: часткове або повне втрачання можливості забезпечити власні інтереси в межах інформаційної сфери соціальними об’єктами, які підлягають інформаційній безпеці; порушення нормальної життєдіяльності, здійснення руйнації або стримування розвитку об’єктів технічного інформаційного спрямування у сфері безпеки [2].

До політичної відносяться система державного управління; системи підготовки прийняття політичних рішень; виборчі системи; телекомунікаційні системи спеціального призначення. Якщо розглядати економічну сферу, то тут зазначимо систему прийняття рішень; банківську інфраструктуру; управління економічним станом в умовах надзвичайних ситуацій; систему управління державними комунікаціями, які мають економічний характер; корпоративні війни і промисловий шпіонаж. До суспільної відносять загрози для системи формування громадської думки; системи ЗМК; структури політичних партій, громадських рухів, релігійних організацій; структури забезпечення основних прав і свобод людини. В науково-технічній: системи накопичення ноу-хау; об’єкти інтелектуальної власності; структури фундаментальних і прикладних досліджень; структури аналізу та прогнозування тенденцій в науково-технічній сфері; бази і банки даних конфіденційного характеру. Але головна увага на сьогодні зосереджена саме на воєнній: інформаційні ресурси збройних сил; системи управління військами; системи постійного контролю і спостереження; канали надходження інформації стратегічного, оперативного і розвідувального характеру.

Від 24 лютого 2022 року на території всієї України був запроваджений воєнний стан, пов'язаний з порушенням територіальної цілісності України, збройної агресії і відкритим нападом російської федерації.

Загрозами інформаційної безпеки, в тому числі телекомунікаційних систем на території України наразі є: протиправні збирання та використання інформації; порушення технології обробки інформації; впровадження в апаратні і програмні вироби компонентів, що

реалізують функції, не передбачені документацією на ці вироби; розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації; знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку; вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації; компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах; впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності; знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації; перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації; використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення й розвитку української інформаційної інфраструктури; несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації [3].

У сучасних умовах інформаційна війна розглядається військовими теоретиками як якісно новий вид бойових дій, активна протидія в інформаційному просторі, а інформація при цьому - як потенційна зброя та зручна ціль [4]. Якщо раніше за допомогою інформації людям лише повідомляли про події державного та світового масштабу, то нині інформація використовується як додаткова і досить дієва зброя з метою посилення дестабілізації політичної системи в державі, втраті довіри до влади, приниження демократичних цінностей.

Дбаючи про захист інформаційних інтересів, «враховуючи пряму військову агресію з боку російської федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії російської федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану», РНБО України вирішило: «установити, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об’єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні “Єдині новини #UAразом”». Президент України підписав Указ №152/2022, яким ввів в дію рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану».

Список використаних джерел

1. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки країни. *Юридичний науковий електронний журнал*. 2020. №2. С. 200-203. URL: http://lsej.org.ua/2_2020/54.pdf

2. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети. К.: НіСД, 2014. № 4. С. 5-12.

3. Турчак А.В. Перспективні напрямки застосування механізмів реалізації державної політики інформаційної безпеки в Україні. *Економіка та держава*. *Серія державне управління*. 2019. №4 (12). С. 114-117.

4. Горбулін В. П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ : Інтертехнологія, 2009. 164 с.