Секція: Державне управління, самоврядування та державна служба

Геворкян Артем Юрійович
кандидат економічних наук, доцент
Національний технічний університет
«Харківський політехнічний інститут»
м. Харків, Україна

ІДЕНТИФІКАЦІЯ ТА ШЛЯХИ ПОДОЛАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВУ ЯК ФАКТОР ЗМІЦНЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У новітніх глобалізаційних умовах існування стан захищеності окремого індивіду від внутрішніх і зовнішніх інформаційних загроз є важливою складовою національної безпеки. Динаміка і характер розвитку інформаційного суспільства створюють нові та підсилюють існуючи виклики і небезпеки, які спрямовані на особистість як найуразливіший суб'єкт інформаційно-комунікаційних відносин [1].

Інтенсивність використання гіперглобальних комунікаційних мереж, транскордонність інформаційного суспільства викликає численні деструктивні явища, інформаційні ризики й загрози, які зумовлюють наявність прямої залежності між ними та постійно виникаючими проблемами національної безпеки [2]. Все це актуалізує сучасні тенденції реалізації «трикутника» інтересів основних суб'єктів інформаційно-комунікаційних відносин в галузі забезпечення інформаційної безпеки, зокрема: особистості, суспільства і держави.

Відзначимо, що постійний розвиток та вдосконалення системи інформаційно-комунікаційних технологій є наслідком її ускладнення та найчастіше відображають неготовність суб'єктів протидіяти сучасним

кібератакам (перш за все, це стосується численних користувачів Інтернету). Треба зазначити, що результатом цих адресних кібератак є ситуація, коли суб'єкт, який здійснює кібератаку (хакер), отримує повний контроль над мобільним чи стаціонарним інформаційно-комунікаційним пристроєм а, отже, й доступ до всієї інформації про власника, включаючи конфіденційну інформацію, що є прямою загрозою національній безпеці країни. Такі цілеспрямовані атаки часто націлені саме на користувачів, що мають певний політико-фінансовий або інший статус та володіють важливою інформацією державного значення [3].

Для розробки механізмів протидії зазначеним негативним тенденціям постає нагальна необхідність згрупувати основні види та форми загроз й запропонувати шляхи їх подолання, які спрямовані на формування та зміцнення національної безпеки в сфері інформаційно-комунікаційних технологій (табл. 1).

Таблиця 1

Виявлення та шляхи подолання загроз інформаційному суспільству як фактор зміцнення національної безпеки

№ з/п	Види загроз	Форми загроз	Комплексні шляхи подолання загроз як фактор зміцнення національної безпеки
1.	Залежно від мети, переслідуваної суб'єктом, який здійснює загрозу	– вплив на свідомість та психологічний стан члена інформаційного суспільства; – надання деструктивного впливу, що може завдати шкоди здоров'ю особистості; – оволодіння особистою (конфіденційною) інформацією з метою використання її в протиправних цілях; – поширення ідеології тероризму, радикальних ідей в інформаційно-комунікаційних мережах; – фінансове шахрайство; – розвиток антигромадських стереотипів поведінки	– виявлення суб'єкту який здійснює загрозу та здійснення відповідних заходів щодо припинення його протиправних дій; – роз'яснення інформаційному суспільству основних способів уникнення загроз та засад демократії і свободи, які є головним політичним курсом країни; – впровадження механізмів економічної та фінансової безпеки
2.	В залежності	– злочинці та злочинні угруповання,	– постійний моніторинг

	від джерела загрози	діяльність яких спрямована на крадіжку інформації, персональних даних, розкрадання чужого майна шляхом шахрайства у інформаційній сфері; – злочинці та злочинні угруповання, що поширюють в глобальному інформаційному просторі різні форми сексуального насильства та здійснюють торгівлю забороненими наркотичними засобами і психотропними речовинами	інформаційно-комунікаційних джерел з метою виявлення та запобігання порушення адміністративного та кримінального законодавства країни у сфері розповсюдження забороненої інформації; – створення нових та удосконалення існуючих засобів захисту носіїв інформації з метою їх розповсюдження серед суб'єктів інформаційно-комунікаційних відносин
3.	Загрози в мережі Інтернет	– небезпечні інтернет-сайти (ряд пошукових сервісів передбачають різні способи інформування користувачів про рівень благонадійності того чи іншого сайту); – фішингові сайти; – шкідливе програмне забезпечення; – спам-розсилки; – шахрайські сайти, рекламовані з метою отримання прибутку (фінансові піраміди, так звані лже-вірусники, фальшиві інтернет-магазини та ін.); – інтернет-майданчики, спрямовані на вплив на індивідуальну свідомість молоді	– удосконалення нормативно-правового поля країни щодо контролю за мережею Інтернет та розповсюдженням в неї забороненої інформації та сайтів; – підвищення інформаційної грамотності суспільства та суб'єктів господарювання в сфері захисту особистої і корпоративної інформації від злочинців; – повне блокування підозрілих сайтів, які можуть загрожувати національній безпеці країни; – виявлення та притягнення до відповідальності осіб, які займаються розповсюдженням забороненої інформації і шахрайством на теренах Інтернету
4.	Загрози національній безпеці у інформаційній сфері новітнього типу	– загрози від файлів cookies, які можуть чинити прямий або непрямий вплив на політичні погляди в інформаційному суспільстві, а також інші загрози національній безпеці; – загрози, спрямовані на трафік віртуальної валюти Bitcoin; – загрози конфіденційності персональних даних внаслідок новітньої технології онлайн-реклами Real-TimeBidding (RTB)	– розробка нових технологій щодо блокування завантажень файлів cookies на інформаційно-комунікаційні пристрої; – можлива заборона віртуальної валюти Bitcoin на усій території країни у зв'язку з неможливістю її контролювати з боку уповноважених державних органів; – своєчасне реагування на виникаючі нові загрози та небезпеки у мінливому інформаційно-комунікаційному просторі

Джерело: розроблено автором на основі [3-6]

Таким чином, можна зробити висновок, що глобальний характер інформаційного розвитку, формування транснаціональної інформаційної інфраструктури та інформаційного суспільства породжує чимало нових і непростих проблем, пов'язаних із забезпеченням національної безпеки в сфері застосування та неналежного користування інформаційно-комунікаційними технологіями. Вирішення багатьох з цих проблем можливе лише на засадах вдосконалення відповідного національного законодавства, а також багатостороннього міжнародного співробітництва, послідовного висунення пропозицій, здатних поставити під національний та міжнародний контроль джерела загроз інформаційній безпеці.

Література

1. Антоюк В.П. Залученість населення України в процеси цифровізації. Побудова інформаційного суспільства: ресурси і технології : мат-ли XVIII Міжн. наук. практ. конф. (Київ, 19-20 вересня 2019 р.). Київ : УкрІНТЕІ С.13-17.
2. Хаба Р.С. Деструктивні інформаційні впливи в сучасних умовах. Інформаційна безпека людини, суспільства, держави. 2017. № 1(21). С. 216-224.
3. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
4. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, Том 1. 2017. С. 34-39.
5. Ткачук Т. Ю. Інформаційна безпека: сучасні підходи до визначення категорії. Актуальні питання публічного та приватного права. 2017. № 2 (16). С. 45–54.

6. Золотар О.О. Досвід правового забезпечення інформаційної безпеки в країнах східного партнерства ЄС (Молдова, Грузія). LEX PORTUS. 2017. № 3 (5) С. 70-80.