обробки інформації.

На сьогоднішній день системи документообігу в більшості випадків є локальними комплексами, які забезпечують діяльність окремих державних і комерційних структур, але вони не здатні взаємодіяти один з одним для забезпечення необхідної якості надаваних сервісів. [2]

Питаннями впровадження уніфікованого електронного документообігу та організації захисту інформації в інформаційних системах в державі сьогодні займаються Міністерство юстиції, Держспецзв'язку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ), а для банківської системи - Національний банк. Але в зв'язку з відсутністю єдиного координуючого органу, а також чітко визначених повноважень і відповідальності на даному етапі не вирішено багато проблемних безпекових питань:

- відсутність необхідного рівня стандартизації в сфері ІКТ відповідно до міжнародних та європейських стандартів;
- несумісність впроваджених автоматизованих інформаційних систем державних органів через відсутність уніфікованих вимог до створення таких систем і регламентів обміну інформацією;
- багаторазове дублювання збору та обробки даних різними державними службами, недостатня повнота і достовірність інформації, що зберігається;
- відсутність єдиних правил, регламентів обміну інформацією та форматів даних в інформаційних системах органів влади з використанням електронного підпису (ЕП), визначеної законом, а також альтернативних засобів підтвердження автентичності;
- недостатня кількість сервісів надання широкого спектра послуг в електронному вигляді органами влади і місцевого самоврядування громадянам і бізнесу в режимі «єдиного вікна».

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. http://zakon.rada.gov.ua/laws/show/67-2018-р.

2. Зубарева Е.А., Белов С.В. Система электронного правительства Украины и способ повышения безопасности ее функционирования. Кибернетика и системный анализ. 2015. 51, № 3. С. 178-187. DOl 10/1007/S10559-015-9739-4.

Ганна Пашкова,
старший викладач кафедри
психології та педагогіки
Дніпропетровського державного
університету внутрішніх справ,
кандидат наук з державного управління

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ДІДЖИТАЛІЗАЦІЇ: УПРАВЛІНСЬКИЙ ПІДХІД

Сьогодні в Україні через недосконаліть систем інформатизації, інформаційного простору та системи його захисту посилюються загрози національній безпеці, а також поширюється зовнішній інформаційний вплив, що призводить до значних політичних, воєнних, економічних і суспільних збитків.

У нашій державі за роки незалежності вийшла значна кількість наукових праць щодо проблем національної безпеки, зокрема захисту інформаційного простору. Питання інформаційної безпеки найчастіше пов’язувалося з технічним і криптографічним захистом інформації [1]. Проте в умовах гібридних війн (як економічних, так і політичних) пріоритетом є захист громадян і суспільства від негативних інформаційних впливів, поширення неправдивої інформації тощо [2]. Особливо це завдання актуалізується в період реформи діджиталізації, що передбачає посилення рівня відкритості систем.

Забезпечення інформаційної безпеки ґрунтується на аналізі структури та змісту системи управління, а також дослідженні інформаційних процесів і використання відповідних технологій їх захисту. При цьому визначальними факторами при розробці засобів інформаційного захисту сьогодні є саме індивідуальні особливості людини, соціальних груп і соціуму загалом. Для того, щоб змоделювати поведінку людини, громади та суспільства в разі інформаційної атаки, необхідно знати саме індивідуальні особливості та переваги [2]. В умовах активного проникнення Інтернету в усі сфери життя, забезпечення відкритості си-

стем це стає все легше. Це стосується інформації відкритих джерел, соцмереж тощо.

Дійсно, із розвитком ІКТ та широкого доступу до Інтернету обсяги даних про громадян безперервно збільшуються. Людина залишається найуразливішим місцем будь-якої інформаційно-телекомунікаційної системи. Проблема захисту інформації у такому середовищі знаходиться у компромісі між правом на анонімність (приватність) громадянини та контролем за поширенням інформації [3].

Отже, сучасний свідомий громадянин повинен бути медіаграмотним, володіти культурою роботи в інформаційному діджиталізованому просторі, тоді держава зможе ефективніше протистояти внутрішнім і зовнішнім загрозам і належно захищати його [4]. Задля цього потрібно розвинути на відповідному рівні інформаційну культуру, що має стати важливим завданням інформаційної політики управлінських органів всіх рівнів, а також і самого громадянина.

Нині відзначається тенденція до збільшення в зарубіжних і вітчизняних засобах масової інформації обсягу матеріалів, що містять негативну, хибну (підривну) оцінку державної політики, керівництва держави, проти якої здійснюється агресія (наприклад, України в умовах російської агресії). Наростає інформаційний вплив, передусім для розмивання традиційних і національних цінностей. Різні терористичні і екстремістські організації широко використовують механізми інформаційного впливу на індивідуальну, групову і суспільну свідомість для нагнітання соціальної напруженості, розпалювання ворожнечі, пропаганди власної ідеології, підміни понять. Зростають масштаби комп'ютерної злочинності, перш за все, в кредитно-фінансовій сфері, збільшується число злочинів, пов'язаних із порушенням конституційних прав і свобод людини і громадянина, зокрема в частині, що стосується недоторканності приватного життя, особистої таємниці, при обробці персональних даних із використанням інформаційних технологій [5].

До того ж методи, способи і засоби вчинення таких злочинів стають все витонченішими. Їх стає все складніше розпізнавати.

Отже, найпотужнішим впливом на забезпечення національної безпеки України в еру діджиталізації є інформаційний, що здійснюється через глобальні та локальні інформаційні мережі. Тому інформаційна безпека виступає системоутворюючим чинником, поєднуючи в єдиному інформаційному просторі всі інші сфери безпеки держави, через що має посісти чільне місце у загальній структурі безпеки. У свою чергу, система її забезпечення – одне з ключових завдань державної безпеки, адже значна частина зовнішніх інформаційних загроз фактично є різновидом воєнних загроз. Сучасні інформаційні загрози є системними і високоорганізованими, вони можуть наносити суттєві збитки національним інтересам у сфері воєнної безпеки, тому протидіяти їм також можливо лише системно [5].

Тому в умовах діджиталізації інформаційну безпеку слід розглядати виключно з позицій системного підходу. Такі системи мають ієрархічну побудову з наявною підсистемою активних дій в інформаційному просторі. Водночас можемо констатувати, що в України досі актуальною є проблема побудови цілісної системно структурованої та реально функціонуючої системи захисту інформаційної безпеки з усіма необхідними підсистемами, які б виконували всі функції забезпечення інформаційної безпеки і ведення інформаційної боротьби в умовах інформаційної атаки.

Також потребує опрацювання науково-методологічний апарат щодо побудови та функціонування системи захисту інформаційної безпеки, як і законодавчі основи створення і функціонування єдиної загальнодержавної системи захисту інформаційної безпеки.

1. Libicki M. Conquest in cyberspace. National security and information warfare, Cambridge, 2019. – 207 p.
2. Галєєв В. А. Захист інформаційного простору в контексті без пекової політики України / В. А. Галєєв, О. А. Омельченко // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 15 травня 2020 р.). [Електронне видання]. – Київ : НА СБУ, 2020. –С. 80 – 82.
3. Давидюк А. В. Середовище та ризики формування інформаційної безпеки держави / А. В. Давидюк // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 15 травня 2020 р.). [Електронне видання]. – Київ : НА СБУ, 2020. – С. 93.
4. Іжутова І. В. Інформаційна безпека в умовах сучасного інформаційного середовища / І. В. Іжутова // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 15 травня 2020 р.). [Електронне видання]. – Київ : НА СБУ, 2020. – С. 108.
5. Богданович В. Ю. Інформаційна безпека як основа воєнної безпеки держави та суспільства / Богданович В. Ю., Ворович Б. О., Марко Є. І. // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. 2018. – №3 (64). – Режим доступу : http://znp-cvsd.nuou.org.ua/article/view/168924.