Конопліцька О.І.
к. філол. н., доцент кафедри документознавства,
інформаційної діяльності та українознавства
ТНЕУ

ІНФОРМАЦІЙНА БЕЗПЕКА У СИСТЕМІ ЕЛЕКТРОННОГО УРЯДУВАННЯ

У сучасному світі інформація є найціннішим глобальним ресурсом, вартість та значимість якого важко оцінити. З огляду на це, забезпечення інформаційної безпеки є актуальною і важливою функцією державного управління. Економічний потенціал держави переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас збільшується уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, кіберзлочинності, неналежної реклами та шахрайства у віртуальному просторі. В цих умовах держава повинна створювати адекватні наявним загрозам правові, організаційні, технічні та інші засоби та методи захисту інформаційного простору та безпосередньо важливої інформації, які є відображенням державної політики інформаційної безпеки [2]

Інформаційні відносини органів державного управління із суспільством мають відбуватись на основі забезпечення інформаційної безпеки – стану захищеності життєво важливих інтересів особистості, суспільства і держави, зведення до мінімуму неповноти, невчасності і недостовірності інформації, негативного інформаційного впливу, негативних наслідків функціонування інформаційних технологій. Небезпечним слід вважати такий інформаційний вплив, який має дестабілізуючі наслідки, утискає інтереси особистості, суспільства, держави. Фактично, інформаційну безпеку можна визначити як можливість нейтралізувати шкідливі впливи різних видів соціальної інформації [1].

Сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сферіскладають основні загрози інформаційній безпеці. Їх поділяють на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого та неправомірного впливу сторонніх осіб на інформацію, інформаційні ресурси та інформаційні системи (їх виробництво, використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову) [2].

Загрозами інформаційній безпеці у інформаційній сфері також є викрадення інформації, відомостей, які становлять таємницю, що охороняється законом; знищення інформації, програмних засобів, які забезпечують опрацювання даних або функціонування технічних засобів і систем; неправомірне «перехоплення» інформації; модифікація інформації, програмних засобів; неправомірне використання інформації, програмних засобів порушення функціонування або

виведення з ладу комп'ютерів і мереж; приховування (неповідомлення) інформації, яка торкається інтересів людини, громадянина, суспільства; збирання, накопичення і використання даних про особу та інші дії, які порушують основні права людини і громадянина [1].

Доктрина інформаційної безпеки України дає основу діяльності органів державної влади, а також інститутів громадянського суспільства у забезпеченні інформаційної безпеки України, з формування та реалізації державної інформаційної політики та визначає ***принципи інформаційної безпеки,*** а саме:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції.

Доктрина передбачає три основні напрями забезпечення державою національного інформаційного суверенітету*:*

1) Законодавче визначення стратегічних шляхів розвитку та захисту національних ринків інформаційних та телекомунікаційних послуг на основі єдиної державної політики.

2) Формування норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в національному інформаційному просторі.

3) Визначення та захист національних інтересів у світовому інформаційному просторі та міжнародних інформаційних відносинах.

Доктрина визначає реальні та потенційні загрози інформаційній безпеці України у зовнішньополітичній, воєнній, внутрішньополітичній, економічній, екологічній, науково-технічній, соціальній та гуманітарній сферах, у сфері державної безпеки.

Відповідно до сформульованих у Доктрині загроз визначено напрями державної політики у сфері інформаційної безпеки України [2].

Явища та процеси природного й штучного походження, що породжують інформаційні загрози, називають дестабілізуючими факторами.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так й організації та їх об'єднання. Особливу групу джерел складають інформаційні системи та засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їх проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин. Джерелом дестабілізуючих факторів може бути також природне середовище

Систему органів державного управління національною безпекою в інформаційній сфері, визначено в Законі України «Про основи національної безпеки України». Відповідно до ст. 4 Закону до складу такої системи входять такі *суб'єкти забезпечення національної безпеки в інформаційній сфері:* Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Національна експертна комісія України з питань

захисту суспільної моралі та ін.); суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні сили України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Служба зовнішньої розвідки України, МВС України, а також інші правоохоронні органи та військові формування, утворені відповідно до законів України.

Отже, розвиток інформаційних технологій має як позитивний, так і негативний бік. З одного боку, удосконалення засобів обробки і передачі інформації створює умови для розвитку демократичного суспільства, участі громадян у прийнятті найважливіших рішень, подолання відчуженості тощо. Але інформаційні технології можуть бути використані для створення системи всеохоплюючого, тотального контролю над суспільством взагалі та кожним його членом зокрема – як зазначається у праці відомого футуролога Й.Масуди «Комп'ютопія»: «….існує серйозна небезпека того, що ми рухаємося у напрямі контрольованого суспільства» [4].

ЛІТЕРАТУРА:

1. Дубов Д. В. Основи електронного урядування. Навчальний посібник / Д. В. Дубов, С. В. Дубова. — К.: Центр навчальної літератури, 2012. —176 с.
2. Електронне урядування. Опорний конспект лекцій / За ред. А.І. Семенченка. – Київ, 2012.
3. Клімушин П. С. Електронне урядування в інформаційному суспільстві : монографія] / П. С. Клімушин, А. О. Серенок. – Х., 2010. – 312 с.
4. Масуда Й. Комп'ютопія // Філософська і соціологічна думка. – 1993. – №6. – С.36-50.

Шкіцька І. Ю.
д.філол. н., доцент, професор кафедри
документознавства, інформаційної
діяльності та українознавства ТНЕУ

КОНФЛІКТОГЕННІСТЬ ЗВЕРТАНЬ У СИТУАЦІЯХ ДІЛОВОЇ ТА НЕФОРМАЛЬНОЇ КОМУНІКАЦІЇ

Виникнення конфліктних ситуацій під час формального та неформального спілкування частотні ще на початку спілкування, що зумовлено неправильним вибором форми звертання до співрозмовника.

Імена людей значущі та мають сакральний смисл, тому дуже часто негативну реакцію адресата викликає неправильне називання його імені чи по батькові адресантом. Зазвичай адресат, якого неправильно назвали, намагається виправити помилку. У деяких випадках – за короткотривалої неповторюваної інтеракції, незначущості імені для ідентифікації особи / документів і под., а також за наявності свідків розмови, нижчий за статусом адресат може не виправляти вищого за статусом співрозмовника.

Варіанти власних імен, будучи носіями соціальних і стилістичних конотацій, дають змогу в службових і особистих відносинах переключати спілкування з однієї тональності на іншу, виконуючи в такий спосіб