4. Марковець О. В., Паздерська Р. Консолідація інформації про діяльність учасників групи в соціальній мережі Facebook. *Вісник Книжкової палати*. 2019. № 6(275). С. 22–27.

5. Мерещяков Д. С. Психологічні особливості суб'єктної активності в соціальних мережах. *Науковий вісник Херсонського державного університету*. Серія «Психологічні науки». 29/10/2018. № 4. С. 117–122.

Мазуркевич Таїсія Леонідівна
(наук. керівник – д-р іст. наук, доцент Ковальська Л. А.)
Донецький національний університет імені Василя Стуса, м. Вінниця

ВИКЛИКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ БЕЗПЕКИ В СУСПІЛЬСТВІ

Інформаційно-комунікаційне середовище соціуму та безпека інформації, як неодмінна складова організації сучасного інформаційного світу, охоплює комплекс заходів, які покликані забезпечити захищеність даних від несанкціонованого доступу, їх нецільового використання, оприлюднення, внесення змін чи знищення.

Головною метою інформаційно-комунікаційної безпеки в суспільстві є насамперед виключення будь-якої можливості зловживань при визначенні прав і свобод людини в інформаційній сфері. Першочерговим завданням у цьому напрямі є укріплення змісту правової основи інформаційної безпеки у суспільній свідомості, зокрема під час обґрунтування питань доступу до накопиченого в суспільстві інформаційного ресурсу і пов'язаних з цим норм інформаційного законодавства [1].

Концепцію інформаційної безпеки можна подати у вигляді систематизованої сукупності відомостей про інформаційну безпеку держави та шляхи її забезпечення. Таке формулювання узагальнене і демонструє основні напрями гарантування безпеки користувачів інформаційно-комунікаційного середовища.

На сьогодні інформаційна безпека посідає одне з ключових місць у системі забезпечення стратегічно важливих інтересів усіх без винятку країн світу. Оскільки через інформаційне середовище найчастіше здійснюються загрози національній безпеці в різних сферах діяльності особистості, суспільства й держави, тому питання захисту інформації актуальне і відкрите для спеціалістів, державних управлінців, підприємців, звичайних користувачів.

Окремо виділяється інформаційна безпека організації. Це цілеспрямована діяльність її керівництва та адміністрації з використанням дозволених сил і засобів задля досягнення стану захищеності інформаційного середовища організації, що забезпечить її нормальне функціонування і гарантуватиме динамічний розвиток і привабливість у партнерів. Сьогодні інформаційна безпека та конфіденційність інформації вимагає забезпечення обмеженого доступу до даних на основі розподілу прав доступу, захисту від несанкціонованого ознайомлення [2].

Існує велика загроза інформації / даних і в соціальному комунікаційному мережевому середовищі. Специфічність соціальної комунікації як соціального явища сьогодення полягає в тому, що вона є чинником, який забезпечує взаємозв'язок людей в їхній діяльності, побуті, дозвіллі, перенесення всієї персональної інформації у віртуальне середовище. З одного боку, – це зручність, швидкість надання інформації, комфорт використання її. Але з іншого боку, усвідомлюємо вразливість персональної інформації, неправомірні дії з персональною інформацією та злочини в інформаційному просторі.

Дослідники та спеціалісти з захисту виділяють такі види загроз інформаційній безпеці:

– отримання доступу до секретних або конфіденційних даних;

– порушення або повне припинення роботи комп'ютерної інформаційної системи;

– знищення або спотворення даних [3].

Вивчення цього феномена підтверджує, що останнім часом до проблем інформаційної безпеки включено питання інформаційного впливу на особистість і суспільство. Зокрема, автори колективної монографії, вивчаючи безпекове середовище, виділяють головні загрози національній безпеці України [4]. Це добре можна простежити сьогодні в умовах тривалої гібридної війни України, побачити вразливість інформації та виявити можливості маніпулювання через інформацію колективною свідомістю. Отож, безпека інформації та її захист, створення умов відкритого інформаційно-комунікаційного середовища є пріоритетним завданням керівництва та спеціалістів інформаційних технологій країн світу.

Інформаційна безпека передбачає можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й поширення інформації. Поняття інформаційної безпеки держави варто також розглядати у контексті створення безпечних умов існування інформаційних технологій, які охоплюють питання захисту інформації як інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів.

У сучасних умовах розвитку суспільства спостерігаються суперечливі цілі та інтереси користувачів соціальних комунікацій, які нерідко призводять до конфліктів, появи різних інформаційних стратегій і тактик їхнього вирішення, до маніпулювання. Подальший розвиток конфліктів в інформаційному середовищі може проявлятися як деструктивно, так і конструктивно. Отож, безпека інформації користувачів соціальних мереж і сучасних засобів комунікації вимагає не обмеження доступу чи закриття інформації, а постійного аналізу інформаційних потоків, моніторингу використання даних, отримання та накопичення відомостей. Звідси, інформаційна безпека – це не разова захисна технологія, а постійний, тривалий і відповідальний механізм контролю інформації та інформаційних процесів у віртуальному середовищі, аналіз запитів користувачів тощо.

Необхідний рівень інформаційної безпеки гарантується наявністю політичних, економічних, організаційних заходів, спрямованих на запобігання, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян. Характерною ознакою так званої «інформаційної революції» у сфері інформаційно-комунікаційної діяльності стало народження електронної комерції, яка розвивається відповідно до законів ринку та вільної конкуренції [5]. Зі свого боку має позитивні наслідки розвитку економічних можливостей, але заразом розширює можливості кіберзлочинності і вимагає захисту інформації та користувачів. Загалом, інформаційна безпека держави є станом захищеності інформаційного середовища, що забезпечує умови функціонування незалежно від ймовірних і реальних внутрішніх та зовнішніх загроз.

Отже, інформаційна культура, яка формується в системі сучасної комунікації, створює віртуальну реальність глобального масштабу, що сприяє зростанню нових можливостей, відкритості і доступності інформації. А така відкритість генерує нові інформаційні загрози, що вимагають дослідження, впорядкування і систематизації для подальшої їхньої регламентації і подолання. Виклики інформаційно-комунікаційної безпеки у світі потребують всебічного постійного контролю стану захисту інформаційної сфери, аналізу інформаційного середовища, класифікації загроз і наступного раціонального перерозподілу сил і засобів для нейтралізації виявлених небезпек.

Список використаних джерел

1. Зернецька О. Інформаційна безпека в інформаційному суспільстві: глобалізаційні загрози та ризики. *Інформаційне суспільство: Антологія*. Київ: ІМВ, 2018. С. 315–323.
2. Дідик В. Ю. Проблеми впровадження культури безпеки в Україні: аналітична доповідь. Київ: НІСД, 2018. 256 с.
3. Галамба М. Інформаційна безпека України: поняття, сутність та загрози. *Інформаційні технології в освіті*. 2018. С. 38–43. 2019. № 2. С. 11–18.
4. Парахонський Б. О. Міжнародне безпекове середовище: виклики і загрози національній безпеці України. Київ: НІСД, 2019. 56 с.
5. Кудлай В. О. Інформаційно-комунікаційної безпеки в суспільстві. *Вісник Маріупольського державного університету*. Серія: Філософія, культурологія, соціологія. 2018. Вип. 10. С. 97–104.

Зарудняк Вікторія Ігорівна
(наук. керівник – канд. пед. наук Яворська Т. М.)
Донецький національний університет імені Василя Стуса, м. Вінниця

ВАЖЛИВІСТЬ ФОРМУВАННЯ ЦИФРОВОЇ КУЛЬТУРИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційне суспільство – це суспільство інтерактивних обмінів, мобільних та віртуальних взаємодій, трансформацій. Його потрібно розглядати як крок до формування нового типу взаємин влади і суспільства, побудованого на моральних принципах управління, з погляду понятійно-ціннісної платформи і методології спілкування з громадянами, без кордонів і зайвих бюрократичних надбудов, зі стратегією збереження укладу корінних народів, їхньої ідентичності [1].

Розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67 схвалено Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 рр. та затверджено план заходів щодо її реалізації.

Серед основних цілей цифрового розвитку держави Концепцією визначено, зокрема, розвиток та поглиблення цифрової компетенції громадян для забезпечення їхньої готовності до використання цифрових можливостей, а також подолання супутніх ризиків. Концепція передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрової компетенції, а також визначає критичні сфери та проєкти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій.

Відповідно до п. 3 Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, існує чіткий перелік сфер реалізації діяльності Міністерства. Зокрема, визначено напрями державної політики, пов’язані з процесами цифровізації. Питання розвитку цифрових навичок та цифрових прав громадян об’єднано в одну сферу, що вказує на комплексний підхід держави. Державою створюються умови для забезпечення громадянам можливості розвитку своїх цифрових навичок [3].

В умовах сьогодення спостерігається швидкий темп розвитку інформаційних технологій, невпинно зростає кількість користувачів мережі Інтернет, постійно