
монографія. Київ: Пед. думка, 2015. 338 с.

2. Єршова Н. А. Формування компетентності вчителя початкових класів у галузі інформаційно-комунікаційних технологій у педагогічному коледжі : дис. канд. пед. наук : 13.00.02 / Державний педагогічний університет, 2009. 232 с.

3. Лапчик М. П. ІКТ-компетентність педагогічних кадрів: монографія. ОмДПУ, 2007. 144 с.

4. Овчарук О. В. Компетентність як ключ до оновлення змісту освіти. Освіта.ua. : вебсайт. 2007. URL: <http://ru.osvita.ua/school/method/381/> (дата звернення: 25.11.2021).

5. Панкова Т. В. Формування інформаційно-комунікаційної компетентності у студентів педагогічного внзу: автореф. канд. пед. наук: 13.00.01 / 2009. 27 с.

6. Федорук Г. М. Формування інформаційно-комунікаційної компетентності майбутніх учителів технологій у процесі професійної підготовки : дис. канд. пед. наук : 13.00.04. Вінниця, 2015. 259 с.

Клочко А.О. д.п.н, доцент
Прокопенко А.А.
НУОУ

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ВИКЛИКІВ СУЧАСНОСТІ

Інтенсивна інформатизація усіх сфер життєдіяльності суспільства є сьогодні одним із визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства.

В умовах швидкого розвитку інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки. При цьому одним із стратегічних пріоритетів забезпечення інформаційної безпеки державою визначено створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них [2].

Інформаційна сфера існує як самостійно, так і у

взаємозв'язку з іншими сферами життєдіяльності суспільства шляхом їх інформаційного обслуговування та забезпечення взаємодії за допомогою інформації. Інформація завжди втілює певне змістовне навантаження, а отже, інформаційна сфера має своїм змістом знання (інформацію) про інші сфери життєдіяльності суспільства.

Таким чином, інформаційна сфера та її окремі елементи дають змогу чинити опосередкований вплив на різні сфери життєдіяльності людського суспільства. Тому забезпечення інформаційної безпеки є запорукою забезпечення інших складових державної безпеки та національної безпеки в цілому.

Загрози інформаційного характеру можуть спрямовуватися до будь-яких складових державної безпеки, проте їхній негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план впливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, та вироблення механізмів протидії їм у всіх напрямках [3]. Тож, система загроз інформаційній безпеці має комплексний характер і в загальному вигляді містить такі їх типи: загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери та соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери.

До найбільш важливих властивостей загроз інформаційній безпеці держави слід віднести: вибірковість (характеризує націленість загрози на заподіяння шкоди тим чи іншим конкретним властивостям об'єкта безпеки); передбачуваність (наявність ознак виникнення загрози, що дозволяють заздалегідь прогнозувати можливість виникнення загрози та визначати конкретні об'єкти, на які вона буде спрямована); шкідливість (можливість завдати об'єкту безпеки шкоди різної тяжкості).

Окрім того, одним із джерел загроз інтересам суспільства в інформаційній сфері є також безперервне ускладнення

інформаційних систем. Тому особливою групою актуальних для України загроз інформаційній безпеці є загрози, зумовлені віртуалізацією – соціальним відчуженням людини, зануренням її в особистісний віртуальний світ. Змінені стани свідомості – транс, одержимість, депривація сну тощо є ознаками віртуальної інтенції в людині і при цьому атрибутивно виступають знаковосимвольною структурою віртуальності. За прискорених темпів інформаційного прогресу, особливо з розвитком «Інтернету речей», людина взагалі ризикує перетворитися на придаток до інформаційних технологій та інформаційних ресурсів [1].

Тому необхідно забезпечити не лише безпеку інформації від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку маршрутизації, але й інформаційну безпеку суспільства. Власне ж суспільство є носієм такої глобальної загрози інформаційній безпеці людини, як інформаційна дискримінація, котра проявляється в розподілі людей на тих, що мають доступ до інформації, і тих, котрі його позбавлені.

Принципове значення для сучасного суспільства при цьому має факт існування інформаційної картини світу. Відповідно, одним із найпоширеніших видів інформаційних загроз стає розповсюдження так званих патогенних текстів, які суперечать чинній ідеологічній системі, спрямовані, зокрема, на підірив національних та державних інтересів, загрожують суспільній моралі, чинять шкідливий психологічний вплив, призводять до нехтування основними правами і свободами, втручаються в особисте життя тощо.

Отже, задля ефективної реалізації державної політики забезпечення інформаційної безпеки потрібні вдосконалення організаційно-функціонального забезпечення інформаційної безпеки.

ЛІТЕРАТУРА:

1. Живко З.Б., Живко М.О. Інформаційні загрози: суть і проблеми. Безпека та захист інформації в інформаційних системах. 2019. 2. С.116-118.

2. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php