УДК 621.391.1

Дідур І. В., *студент 4 курсу спеціальності «Комп'ютерна інженерія»*
Березюк О.В., *д.т.н., професор кафедри безпеки життєдіяльності та педагогіки безпеки*

ВПЛИВ ІНФОБЕЗПЕКИ НА ЖИТТЄДІЯЛЬНІСТЬ ЛЮДИНИ

Вінницький національний технічний університет, Україна

Основним завданням сучасної держави є гарантування інформаційної безпеки особистості, яка характеризується захищеністю психіки і свідомості від небезпечних інформаційних впливів: маніпулювання, дезінформування [1]. Зараз наше суспільство зазнає впливу від ЗМІ (зокрема їх інформаційно-пропагандистської спрямованості), комп'ютерних мереж, програмних засобів розповсюдження, реклами тощо [2, 3]. Нажаль, жодна з наведених сфер впливу на людину не можлива без шкоди її психологічному здоров'ю. Інформаційно-психологічна безпека особистості (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що приводить до неадекватного сприйняття нею дійсності [4]. Питання інформаційної безпеки придбало особливої значущості в новітніх умовах широкого використання інформаційних автоматизованих систем, заснованих на застосуванні комп'ютерних та телекомунікаційних засобів. Під час забезпечення інформаційної безпеки стали абсолютно імовірними загрози, що породжені навмисними (зловмисними) діями громадян. Перші звістки про несанкціонований доступ до інформації пов'язані були, як правило, з хакерами. В останнє десятиріччя порушення захисту інформації зростає разом із застосуванням програмних засобів, а також за допомогою мережі Інтернет. Дуже розповсюдженою загрозою інформаційної безпеки також є зараження комп'ютерних систем за допомогою комп'ютерних вірусів.

Інформаційна безпека становить собою стан рівня захищеності інформаційного середовища, а захист інформації – це діяльність направлена на запобігання витоку інформації, яка захищається, ненавмисних і несанкціонованих впливів на інформацію, яка захищається, тобто процес, що направлений на досягнення цього стану. Головною метою реалізації інформаційної безпеки будь-якого об'єкта є реалізація системи забезпечення інформаційної безпеки цього об'єкта.

Усвідомлюючи інформаційну безпеку як "стан рівня захищеності інформаційного середовища суспільства, що забезпечує її формування, розвиток і використання в інтересах організацій та громадян", правомірно встановити загрози безпеки інформації, їхні джерела, способи їхньої реалізації та мети, інші обставини та дії, що порушують безпеку. Природно, що при цьому потрібно розглядати також заходи захисту інформації від злочинних дій, що спричиняють нанесення збитку.

Під загрозами інформаційній безпеці розуміють можливі події або дії, які можуть вести до порушень інформаційної безпеки. Різновиди загроз інформаційній безпеці досить різноманітні та мають безліч класифікацій. За різновидом об'єкта впливу загрози поділяються на загрози: власне інформації, діяльності стосовно забезпечення інформаційної безпеки об'єкта та персоналу об'єкта. Після більш детального розгляду загроз інформації, їх можна класифікувати на загрози: носіям конфіденційної інформації, місцям їх розташування (розміщення), системам інформаційного обміну (каналам передачі), а також інформації, що зберігається в електронному (документованому) вигляді на різних носіях інформації.

Засоби масової інформації (ЗМІ) є найбільш ефективними для здійснення інформаційно-психологічного впливу на великі маси людей, що дозволяє розглядати їх як

складову частину стратегічних сил інформаційної війни. Найнебезпечнішою рисою засобів масової інформації, як вважають багато фахівців, є здатність подавати інформацію таким чином, щоб за видимою об'єктивністю у великої маси людей формувалася віртуальна картина реальності. Однак, як тільки людина починає сумніватися у віртуальній картині світу, ефективність інформаційно-психологічного впливу різко падає. Ці сумніви можуть бути підтримані технологіями контрпропаганди, також реалізованими за допомогою засобів масової інформації.

Соціальні мережі є найпопулярнішою складовою сучасного Інтернету [5-8], яким у світі користуються нині понад 2 млрд. осіб. Понад 60% з них є активними користувачами інтерактивних сервісів Web 2.0. Зі 100 найбільш відвідуваних сайтів у світі 20 – це класичні соціальні мережі, ще 60 – тією чи іншою є соціалізованими. Сегменти соціальних мереж Facebook, Twitter, та інших на сьогодні є найменш застрахованими від негативних зовнішніх інформаційних впливів, і це особливо небезпечно в умовах інформаційно-психологічної війни, у які втягнута сьогодні наша держава [9-12]. Небезпека пов'язана з низкою факторів.

Серед цих факторів варто виділити такі:

− не адаптованість сучасної людини до зростаючих масивів навої інформації, різної за якістю, достовірністю і соціальною значущістю;

− непідготовленість переважної більшості учасників інформаційних обмінів у мережах у технологічному плані [13], відсутність навичок пошуку якісної інформації;

− надмірна ідеалізація спілкування в соціальних мережах (при низькій довірі до вітчизняних ЗМІ, політиків);

− відсутність знань про загрози, які несе із собою інформаційна війна, про збитки, яких вона може завдати державі і конкретній людині [14].

Через ці фактори учасники обмінів можуть легко потрапляти під дією спеціальних маніпулятивних технологій, бойових технологій інформаційної війни. Особливо багато в соціальних мережах організовано груп на населення України. Подібні мережеві спільноти є одним з основних засобів організації масових політичних акцій, вуличних заворушень. Ще один маніпулятивний прийом в соцмережах пов'язаний із вливанням частини інформації, яка змушує індивіда додумати певну подію, ситуацію потрібну для маніпулятора руслі.

У соціальних мережах, як у найбільш зручному каналі спілкування, особливу небезпеку становлять сугестивні впливи. Ще зовсім нещодавно сугестія (навіювання) розглядалася у двох вимірах. По-перше, як психічний вплив однієї людини на іншу, унаслідок якого у людини-об'єкта навіювання в супереч її волі та свідомості виникають певні уявлення, судження, вчинки. І по-друге, під цим поняттям розуміється психічний вплив на людину, яка перебуває в стані гіпнозу [15].

Але на сьогодні, з розвитком інформаційних технологій, наведене формування не можна вважати вичерпним. Третім компонентом цього визначення, очевидно, треба вважати вплив сучасних, насамперед електронних, інформаційних технологій на свідомість людини.

Отже, вплив несвідомої інформації на людину зараз є дуже актуальною проблемою суспільства. Щоб уникнути інформаційної війни, необхідно збільшити рівень інформаційної безпеки, підготовлювати людей з раннього віку. Зокрема, навчитися: адаптуватися до зростаючих обсягів інформації; шукати правдиву інформацію; надавати перевагу живому спілкуванню, а не через соціальні мережі; критично відноситися до інформації, що отримала від джерел, які викликають сумнів.

Перелік джерел посилання

1. Булейко А. А. Життєдіяльність та інформаційна безпека людини у сучасних умовах / А. А. Булейко, Н. Б. Мітіна, А. В. Кудрявцев // Третій том збірника тез доповідей IX Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених «Хімія та сучасні технології», 24-26 квітня 2019 р. – Дніпро, 2019. – Т. III. – С. 40-41.

2. Березюк О. В. Безпека життєдіяльності : навчальний посібник / О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2011. – 204 с.

3. Березюк О. В. Безпека життєдіяльності : практикум / О. В. Березюк, М. С. Лемешев, І. В. Заюков, С. В. Королевська. – Вінниця : ВНТУ, 2017. – 99 с.

4. Палагнюк Д. М. Принципи забезпечення інформаційної безпеки / Д. М. Палагнюк, Д. С. Тищук, О. В. Березюк // Якість і безпека. Сучасні реалії. Матеріали Науково-практичної конференції 14-15 березня 2018 року : збірник тез доповідей. – Вінниця : ВНТУ, 2018. – С. 19-22.

5. Березюк О. В. Застосування комп'ютерних технологій під час вивчення студентами дисциплін циклу безпеки життєдіяльності / О. В. Березюк // Педагогіка безпеки : міжнародний науковий журнал. – 2016. – № 1 (1). – С. 6-10.

6. Веліховська А. Б. Мережеві технології формування професійних якостей майбутніх фахівців готельно-ресторанної справи / А. Б. Веліховська, С. Б. Літвінчук, В. М. Курепін // Актуальні проблеми в системі освіти: заклад загальної середньої освіти – доуніверситетська підготовка – заклад вищої освіти : Матеріали VI Всеукраїнської науково-практичної конференції, м. Київ, 9 червня 2020 р. – Київ : НАУ, 2020. – С 47-54.

7. Березюк О. В. Міжпредметні зв'язки у процесі вивчення дисциплін циклу безпеки життєдіяльності майбутніми фахівцями радіотехнічного профілю / О. В. Березюк // Педагогіка безпеки. – 2017. – № 2. – С. 21-26.

8. Березюк О. В. Комп'ютерна програма для тестової перевірки рівня знань студентів / О. В. Березюк, М. С. Лемешев, І. В. Віштак // Тезиси науково-технічної конференції студентів, магістрів та аспірантів «Інформатика, управління та штучний інтелект», 26-27 листопада 2014 р. – Харків : НТУ «ХПІ», 2014. – С. 7.

9. Березюк О. В. Перспективи тестової комп'ютерної перевірки знань студентів із дисципліни "Безпека життєдіяльності" / О. В. Березюк, М. С. Лемешев, М. А. Томчук // Матеріали дев'ятої міжнародної науково-методичної конференції "Безпека життя і діяльності людини – освіта, наука, практика". – Львів : ЛНУ, 2010. – С. 217-218.

10. Bereziuk O. V. Means for measuring relative humidity of municipal solid wastes based on the microcontroller Arduino UNO R3 / O. V. Bereziuk, M. S. Lemeshev, V. V. Bohachuk, M. Duk // Proceedings of SPIE, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2018. – 2018. – Vol. 10808, No. 108083G. – http://dx.doi.org/10.1117/12.2501557

11. Березюк Л. Л. Тестова комп'ютерна перевірка знань студентів із дисципліни «Медична підготовка» / Л. Л. Березюк, О. В. Березюк // Науково-методичні орієнтири професійного розвитку особистості: тези доп. уч. IV Всеукр. наук.-метод. конф., 20.04.2016. – Вінниця, 2016. – С. 96-98.

12. Bereziuk O. Ultrasonic microcontroller device for distance measuring between dustcart and container of municipal solid wastes / O. Bereziuk, M. Lemeshev, V. Bogachuk, W. Wójcik, K. Nurseitova, A. Bugubayeva // Przeglad Elektrotechniczny. – Warszawa, Poland, 2019. – No. 4. – Pp. 146-150. – http://dx.doi.org/10.15199/48.2019.04.26

13. Курепін В. М. Виховання культури безпеки життєдіяльності майбутніх фахівців у закладах вищої освіти / В. М. Курепін, К. М. Горбунова // Педагогічні науки : збірник наукових праць. Глухів : ГНПУ ім. О. Довженка, 2018. – С. 127-135.

14. Курепін В. М. Підвищення рівня підготовки здобувачів вищої освіти освітнього ступеню «Магістр» з дисципліни «Цивільний захист» / В. М. Курепін // Актуальні питання техногенної та цивільної безпеки України : матеріали II Всеукраїнської наукової конференції, м. Миколаїв, 18-19 вересня 2020 р. – Миколаїв : Національний університет кораблебудування імені адмірала Макарова, 2020. – С. 172-175.

15. Курепін В. М. Психолого-педагогічні методи формування креативного мислення в майбутніх інженерів-педагогів / В. М. Курепін, В. С. Іваненко // Осінні наукові читання : матеріали XXIII міжнародної науково-практичної інтернет-конференції, секція № 10. Педагогічні науки, м. Тернопіль, 27 листопада 2019 р. – Тернопіль : ГО «Наука та освіта без кордонів», 2019. – С. 48-51.