https://www.iso.org/standard/44375.html

Заєць Віталій Ігорович, студент групи 1БС-16б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Кобилянська Ірина Миколаївна, кандидат педагогічних наук, доцент, доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: akobilanskiy@gmail.com

Zayets Vitaliy Igorevich, student of the group 1SS-16b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnitsa.

Kobylyanska Irina M., Cand. Sc. (Ped.), Assistant Professor, Assistant Professor of Department of Health and Safety Studies, Vinnitsa National Technical University, Vinnytsia, e-mail: akobilanskiy@gmail.com.

УДК 004.77

Ю.О. Мисько
В.А. Колган

ПОПЕРЕДЖЕННЯ НЕБЕЗПЕК ІНФОРМАЦІЙНОГО ПРОСТОРУ

Вінницький національний технічний університет

Особистість може бути сформована тільки при наявності фізіологічних задатків та під впливом інформації, що поширюється в соціумі. В умовах суцільної інформатизації суспільства інформаційний вплив на особистість набуває глобальних масштабів.

До розвитку сучасних кібернетичних систем розуміння інформаційного простору зводилося до атмосфери, стратосфери, космосу, водних акваторій океанів і морів. Нині воно включає ще й кібернетичні та віртуальні системи. Розглядаючи вплив інформаційного простору на особистість, слід враховувати, що він поширюється на суспільство та державу і через них опосередковано на кожного індивідуума. Цей вплив може мати конструктивний (безпечний) і деструктивний (небезпечний) характер.

Ключові слова: небезпека, особистість, інформація, інформаційний простір, інформаційна безпека особи, інформаційні впливи, загрози, джерела загроз інформаційного простору.

AWARENESS OF INFORMATIVE SPACE INFRINGEMENT

A person can be formed only in the presence of physiological instincts and under the influence of information disseminated in the society. In the conditions of continuous informatization of society, the information influence on the person acquires a global scale.

Up to the development of modern cybernetic systems, the understanding of the information space was reduced to the atmosphere, stratosphere, space, water areas of the oceans and seas. Now it also includes cybernetic and virtual systems. Considering the influence of the information space on the person, it should take into account that it extends to society and the state and through them indirectly to each individual. This influence can be constructive (safe) and destructive (dangerous) character.

Keywords: danger, personality, information, information space,information security of a person, information influences, threats, sources of information space threats.

Ризиком відзначена як життєдіяльність людини в сучасному суспільстві, так і функціонування його систем: громадської, технічної, природної тощо. Розвиток світовою економіки обумовив створення спеціальних систем безпеки – протипожежної, санітарної, екологічної, технічної тощо. Отже, для зменшення негативних вливів сучасних ризиків потрібно формування у населення ризик-орієнтованого мислення на протязі життя як у навчальних закладах, так і самостійно [7-10].

Сучасні реалії, зумовлені значним ростом інформації, відкривають ще одну складну та ризикову сферу життєдіяльності людини – інформаційну. Життєдіяльність людини реалізується одночасно зі світом природи та у специфічному для людського суспільства інформаційному середовищі, що має свої закономірності розвитку і функціонування. Інформаційна сфера стає такою ж

важливою складовою суспільного життя, як економічна, виробнича, побутова, політична, військова та ін. Нові інформаційні технології, засоби масової комунікації багатократно підсилили можливості впливу на свідомість і підсвідомість як окремої людини, так і на великі групи людей та населення країни загалом.

Одне із головних завдань сучасної держави - гарантування інформаційної безпеки особи, яка характеризується захищеністю її психіки та свідомості від небезпечних інформаційних впливів; маніпулювання, дезінформації, образ, спонукування до самогубства тощо. Таким чином, питання кібербезпеки – це питання виживання країни і можливості її розвитку.

В Законі України «Про основні засади забезпечення кібербезпеки України» зазначено, що «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [5].

Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі [12].

Інформаційно-психологічна безпека особи (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 призводить до неадекватного сприйняття нею дійсності.

Інформаційно-психологічна безпека особи (в широкому розумінні) - це:

- належний рівень теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів та гармонійний розвиток незалежно від наявності інформаційних загроз;
- здатність держави створити умови для гармонійного розвитку й задоволення потреб особистості в інформації незалежно від наявності інформаційних загроз;
- гарантування, розвиток і використання інформаційного середовища в інтересах особистості;
- захищеність від різного роду інформаційних небезпек.

Результати дослідження

На сьогодні не існує достатніх гарантій захисту особистості від загроз, пов'язаних з порушенням інформаційної та інформаційно-психологічної безпеки особистості - неусвідомлюваним інформаційно-психологічним впливом [11].

Джерелами загроз інформаційного простору є суперечності певних інтересів, системи цінностей, цілей між особистістю та суспільством, державою або наявністю в однієї зі сторін стосовно іншої домагань, претензій або інших спонукань до конфлікту. Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливостей маніпулювання свідомістю людини через створення навколо неї індивідуального віртуального інформаційного простору, а також можливість використання технологій впливу на її психічну діяльність [11].

Для усвідомлення сутності та змісту завдань інформаційно-психологічного захисту особи та суспільства від деструктивного впливу в умовах сучасного інформаційно-психологічного протиборства необхідно зрозуміти загрози впливу на поведінку особистості.

До основних інформаційних загроз відносяться:

- надання цілеспрямованого інформаційного впливу на населення через засоби масової інформації, Інтернет, яке може привести до негативних соціально-політичних наслідків;
- неповна реалізація прав громадян у сфері отримання та обміну достовірної інформації;
- провокування соціальної, міжнаціональної, релігійної напруженостей через діяльність окремих ЗМІ;
- маніпулювання масовою свідомістю з використанням інформаційно-психологічного впливу;
- втрата відомостей з інформаційних ресурсів у найважливіших сферах політичної, економічної, науково-технічної та військової інформації;
- поширення зловживань у кредитно-фінансовій сфері, пов'язаних з проникненням кримінальних елементів в комп'ютерні системи та мережі;
- спотворення в інформаційних джерелах історичного досвіду, економічного укладу та

національних традицій народу;

- безвідповідальне ставлення ряду засобів масової інформації до питань формування суспільної свідомості [1].

Знання методів інтерактивного обмеження при використанні інформаційних ресурсів є першим кроком до психологічного та правового захисту особи. Держава й суспільство мають організувати просвіту населення, особливо молоді, щодо проблем сприйняття медіа матеріалів [4]. Звичайно, починати цю роботу слід у школах, професійно-технічних та вищих навчальних закладах. Наприклад, педагог може завчасно пояснити правила безпечного використання інтернету та інших інформаційних ресурсів, допомогти вибрати нік, пароль та індивідуальні адреси електронної пошти ще до того, як молоді люди отримають доступ до мережі. Разом з вихованцями педагоги вивчають зміст інформації, обирають механізми попередження непристойних, шкідливих, небажаних дій, дотримуються етикету під час отримання та користування інформацією [2]. При розробці критеріїв безпечного користування інформацією можна застосовувати методику порівняння дій людини у реальному житті із вербальною поведінкою. Доцільно дати зрозуміти молоді залежність вільного доступу до інформації, з готовністю бути не менш відкритими для інших у цьому просторі.

Іншими словами, йдеться про необхідність створення таких умов, щоб кожний громадянин володів механізмом критичного осмислення і корегування інформації, уміннями інтерпретувати, аналізувати та оцінювати медіа тексти, розуміти їхню суть, адресну спрямованість, мету, викривати приховане значення та шкідливий вплив окремої медіа інформації, протиставити цьому впливу зразки високих національних культурних цінностей [3].

Для того, щоб щоденний контакт із зовнішнім світом приносив більше користі й менше демотивував, досить дотримуватися наступних простих рекомендацій.

Перший крок до того, щоб почати отримувати більше користі з часу, проведеного в мережі – більш усвідомлена фільтрація контенту, який споживається. Процес серфінгу, найчастіше має безконтрольний характер. З іншого боку, усвідомлений і активний контакт з мережею передбачає наявність конкретних цілей – пошук конкретної інформації, придбання потрібних контактів, просування свого продукту, демонстрація ідей, творчих досягнень тощо. Це робить індивіда більш сфокусованим і істотно спрощує завдання не змарнувати час на непотрібний контент.

Другий крок - не заходити в мережу «просто так» - лише «у справах». Щоб розуміти, чому говорити "ні" в процесі споживання інформації, необхідно чітко розуміти, чому говорити «так».

Перш за все потрібно визначити категорії цікавої інформації, щоб фільтрація контенту набула системного характеру.

Щойно систематизується цікава інформація в соціальній мережі, можна визначити, на які сайти, пабліки та акаунти варто звертати увагу, а які можна спокійно ігнорувати.

Третій крок - не споживати інформацію з Інтернету в перші дві години після пробудження і за дві години до сну. Також не варто читати коментарі в практично будь-якому російськомовному блозі в 99,9% випадків це «забруднює» інформаційний фон.

Для психічного здоров’я, як одного з прикладів, є найбільшою небезпека від інформаційного впливу, що криється у виникненні залежності – комп'ютерної та інтернет-залежності. Проблема аддикції (патологічної залежності) починається тоді, коли прагнення втечі від реальності, пов’язане зі зміною психічного стану, починає домінувати у свідомості, стаючи центральною ідеєю, що вдирається в життя, веде до відриву від реальності. Відбувається процес, під час якого людина не тільки не вирішує важливих для себе проблем (наприклад, побутових, соціальних), але й зупиняється у своєму особистісному розвитку [1].

Головним механізмом захисту від негативних інформаційно-психологічних впливів на рівні особистості є необхідність формулювання мети пошуку, отримання, обробки, збереження та забування тої чи іншої інформації та відмову від зайвої чи непотрібної інформації.

Для запобігання загрозам інформаційній безпеці держави розробляють та впроваджують превентивні заходи, серед яких виділяють правові (криміналістичні) та організаційно-технічні. Прийнятними та зрозумілими для усіх громадян є організаційні, а також заходи технічного характеру (апаратні, програмні та комплексні), останні з яких цілком можуть реалізувати й самі користувачі Інтернету та інформаційних систем.

Висновки

Головною умовою успішного співіснування людина-комп'ютер та людина-інтернет має бути вирішення питання регулювання відносин і розуміння важливості саморегуляції поведінки в мережі

на основі морально-етичних норм. І тоді людство може позбутися або суттєво скоротити інформаційні загрози, які так поширені в нашому сучасному інтернет-мережному просторі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гнатюк С. Л. Проблеми становлення інформаційного суспільства в Україні / С. Л. Гнатюк // Стратегічні пріоритети. – 2007. – № 1(2). – С. 95-101.

2. Новицкий Г. В. Проблемы обеспечения национальной безопасности в условиях глобализации / Г. В. Новицкий // Геополитика – безопасность – терроризм: сб. ст.; под. ред. Е. А. Вертлиба, Л. М. Бонданца. – Бишкек: Изд-во Бийиктик, 2006. – С. 123-128.

3. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

4. Виноградов В. А., Скворцов Л. В. Информационные потребности и информационная культура // Теория и практика общественно-научной информации. - М., 1990. - Вып. 4. - С. 48-60.

5. Закон України «Про основні засади забезпечення кібербезпеки України». – Режим доступу: http://zakon3.rada.gov.ua/laws/show/ru/2163-19

6. Кара-Мурза С. Г. Манипуляция сознанием. - М.: Эксмо, 2006.-832 с.

7. Кобилянська І. М. Самостійна пізнавальна діяльність студентів у процесі вивчення безпеки життєдіяльності / І. М. Кобилянська, О. В. Кобилянський // Формування готовності вчителів фізико-математичних дисциплін до організації самостійної пізнавальної діяльності учнів : матеріали Всеукраїнської наук.-практ. конфер. / уклад. В. О. Савош. – Луцьк : ВІППО, 2015. – С. 97–101.

8. Кобилянський О. В. Застосування сучасних методів дослідження і аналізу ризиків та небезпек на робочих місцях / О. В. Кобилянський, І. В. Заюков // Молодь в технічних науках : дослідження, проблеми, перспективи : Матеріали Міжнар. Інтернет-конф. (23–26 квітня 2015 року). – Вінниця : ТОВ Нілан-ЛТД, 2015. – С. 169–171.

9. Дембіцька С. В. Формування ризик-орієнтованого мислення у майбутніх фахівців енергетичної галузі / С. В. Дембіцька, О. В. Кобилянський // Зб. наук. праць Кам'янець-Подільського нац. ун-ту ім. І. Огієнка. Серія педагогічна. – Вип. 23. – Кам'янець-Подільський : Кам'янець-Подільський нац. ун-т ім. І. Огієнка, 2017. – С. 85–87.

10.Кобилянський О. В. Формування ризик-орієнтованого мислення в процесі вивчення дисципліни «Безпека життєдіяльності» / О. В. Кобилянський, І. М. Кобилянська // Наукові записки ВДПУ ім. М. Коцюбинського. Серія: Педагогіка і психологія: Зб. наук. праць. – Вип. 39. – Вінниця: ТОВ Планер, 2013. – С. 41–46.

11.Навчальні матеріали онлайн [Електронний ресурс] – Режим доступу до ресурсу: http://pidruchniki.com.

12 ISO/IEC 27032:2012 - Information technology – Security techniques. – Режим доступу: https://www.iso.org/standard/44375.html

Юлія Олегівна Мисько — студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: yuliia.mysko@gmail.com;

Вікторія Альбертівна Колган — студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vikusha.kolgan@gmail.com.

Науковий керівник: ***Кобилянська Ірина Миколаївна***, кандидат педагогічних наук, доцент, доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: akobilanskiy@gmail.com

Mysko Yuliia O. — student, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, email: yuliia.mysko@gmail.com;

Kolgan Victoriia A. — student, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, email: vikusha.kolgan@gmail.com.

Supervisor: ***Kobylyanska Irina M.***, Cand. Sc. (Ped.), Assistant Professor, Assistant Professor of Department of Health and Safety Studies, Vinnitsa National Technical University, Vinnytsia, e-mail: akobilanskiy@gmail.com.