УДК-159.9.075

Коцюк Юрій Анатолійович, аспірант кафедри вікової психології, викладач кафедри документознавства та інформаційної діяльності Національного університету "Острозька академія"

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПСИХОЛОГІЧНИЙ КОМФОРТ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація

У даній статті перевіряється наявність функціонального зв'язку між рівнем психологічного комфорту користувачів комп'ютерних інформаційних систем та їх знаннями/вміннями використовувати криптографічні засоби захисту інформації.

Ключові слова: комп'ютерні інформаційні системи, криптографічні засоби захисту інформації.

Останні роки у світі, як ніколи, активно відбувається формування інформаційного суспільства. Інформаційні системи та технології насичують усі сфери сучасного життя, вдосконалюються, розвиваються, стають незамінною складовою існування індивіда. І, напевне, найважливішим елементом такого поступу є глобальна мережа – Інтернет. Існує велика кількість визначень поняття Інтернет: від найпростішого, як то „мережа мереж” [1, с. 503] до більш складних, які розглядають Інтернет як сукупність розрізнених комп’ютерних вузлів з різноманітними функціями та сервісами [2, с. 68]. Проте сьогодні Інтернет набуває ще й іншого значення – значення життєвого простору. Інтернет дозволяє отримувати та розміщувати інформацію, вільно публікувати свої думки, здійснювати групове чи індивідуальне спілкування, обговорення тощо; через Інтернет можна отримати роботу та платню за неї, здійснити покупку чи перерахувати на певний рахунок гроші, розмістити рекламу та багато-багато іншого. В багатьох випадках використання Інтернет дозволяє замінити традиційні засоби листування на електронні, які, без сумніву, набагато зручніші та швидші. Сукупність усіх сервісів, що надає мережа Інтернет, дозволяє використовувати їх в якості потужної бази для забезпечення освітніх процесів. Причому інформаційні системи на базі Інтернет можуть слугувати як основою дистанційних форм навчання, так і ефективним опорним інструментом для підтримки денних та заочних форм навчання.

Щодня Інтернет здобуває собі нових користувачів як за рахунок величезної кількості сервісів, так і за рахунок зменшення їх вартості. Сьогодні будь-яка пересічна родина, що має телефонний зв’язок та комп’ютер удома, має також і можливість підключитися до Інтернет. Проте разом з очевидними благами, які так звана „Велика Мережа” несе у суспільство, існує й ряд негативних моментів. Серед них такі: нагромадження величезних масивів інформації, серед якої знайти потрібну доволі проблематично; свідоме та несвідоме розміщення неправдивої чи то некоректної інформації; розвиток злочинності у галузі інформаційних технологій, що дістав назву кібер-злочинності; втручання в особисте життя; різноманітні махінації з інформацією тощо [3]. На фоні усього вище сказаного особливо **актуальним** стає проблема інформаційно-психологічної безпеки.

Питання інформаційної безпеки вивчається та все активніше розглядається багатьма вітчизняними та зарубіжними дослідниками – Б.Ю. Аниним, М.И. Анохіним, М.Н. Аршиновим, С.У. Баричевим, Н.П. Варнавским, В.О. Голубєвим, В.В. Гончаровим, М.А. Ивановим, В.Н. Петровим, А.А. Петровим, Л.Е. Садовским, Р.Е. Сєровим, В.М. Сидельниковим, В.В. Ященко. Разом з тим існує ряд праць, присвячених інформаційно-психологічній безпеці особистості, – А.А. Баранова, Г.В. Грачева, М.А. Котика, Г.В. Ложкіна, А.А. Реана, в яких основний наголос робиться на особливостях інформаційних впливів на свідомість людини. Проте все ще недостатньо висвітленим залишається зв'язок інформаційної безпеки та психічних станів, зокрема, комфортних станів особистості.

Традиційно безпекою вважають захищеність людини (суспільства) від фізичної загрози. Проте лінгвістичний аналіз показав, що в суспільній свідомості поняття безпеки пов'язується не стільки з відсутністю загрози, скільки зі станом, почуттями і переживаннями людини [4, с. 78]. Наприклад, у великому тлумачному словнику сучасної української мови безпека визначається як «Стан, коли кому-, чому-небудь ніщо не загрожує» [5, с. 70]. Тобто безпека – це швидше не відсутність небезпеки, а встановлення захисту від неї.

Психологічна безпека згідно [4, с. 79] – це такий стан суспільної свідомості, у якому суспільство в цілому, і кожна людина зокрема, сприймають існуючу якість життя як адекватну і надійну, оскільки вона створює реальні можливості для задоволення особистих і соціальних потреб громадян нині і дає їм підстави для впевненості в майбутньому.

Отже, безпека людини полягає у стабільності її стану, а психологічна безпека – у відображенні цього стану у свідомості. Тому інформаційно-психологічну безпеку можна розглядати з позиції впливу інформаційної системи на суспільну й індивідуальну свідомість, що відображає відносини суспільства і громадян нині і в майбутньому. Під впливом інформаційної системи мається на увазі найширше коло процесів: формування або руйнування тих чи інших моральних, ідеологічних і політичних цінностей, включаючи інформаційну політику держави, систему освіти, діяльність ЗМІ, події культурного життя, масові явища тощо.

Підсумовуючи усе вище сказане, можна дати таке визначення інформаційно-психологічної безпеки (ІПБ): ІПБ – це відсутність небезпеки інформаційних впливів. Саме активний соціальний суб'єкт і його психіка зазнають безпосереднього впливу інформаційних факторів, які, змінюючи психологічний стан індивіда, тим самим впливають на його життєдіяльність та працездатність. Отже зменшення небезпечних інформаційних впливів тим самим підвищить інформаційно-психологічну безпеку як особистості, так і суспільства в цілому. Значну частку таких деструктивних інформаційних факторів складають порушення у сфері електронного документообігу. До них можна віднести несанкціонований доступ до конфіденційної інформації, відмова від авторства, підробка, підміна електронних документів тощо. Сьогодні існують ефективні методи боротьби з такими порушеннями, і в більшості випадків вони передбачають використання електронного цифрового підпису [6, с. 12]. Тому вивчення пересічними користувачами Інтернет можливостей криптографічного захисту інформації дозволить значно підвищити інформаційно-психологічну безпеку.

Досягнення стану інформаційно-психологічної безпеки є невід'ємною складовою інформаційного, а, значить, і психологічного комфорту користувачів Інтернет [7], тому **мета**

даної статті – з'ясувати, чи існує зв'язок між знаннями користувачів у галузі криптографії, вмінням на практиці їх використовувати та станом психологічного комфорту при роботі з інформаційними системами. Основна увага у статті звертається власне на менеджерів як на активних користувачів мережі Інтернет та її служб, які користуються послугами інформаційних систем як для особистих потреб, так і безпосередньо у роботі.

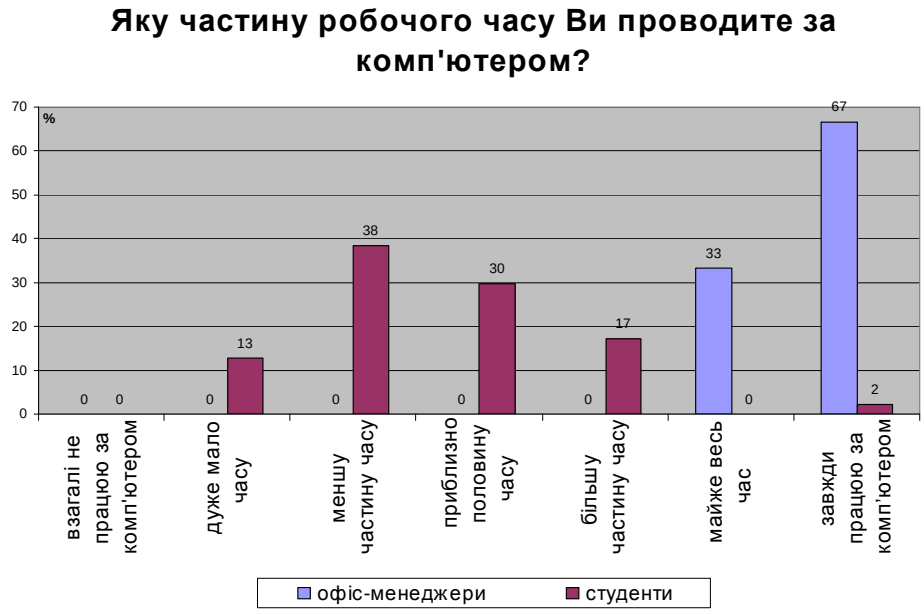

Рис. 1. Частка робочого часу опитаних офіс-менеджерів та студентів, проведена за комп’ютером

Отож в ході теоретичного дослідження було зроблено припущення, що рівень психологічного комфорту особистості менеджера, який займається інформаційною діяльністю з широким залученням комп'ютерних засобів комунікації, знаходиться у функціональній залежності від наявних знань механізмів криптографічного захисту інформації та вмінням використовувати їх на практиці.

Для перевірки припущення було проведено опитування серед студентів спеціальності «Документознавство та інформаційна діяльність», що навчаються на факультеті політико-інформаційного менеджменту Національного університету «Острозька академія». Основна маса студентів цієї спеціальності по закінченні навчання працює на посаді офіс-менеджера, тому обрання в якості вибірки студентів саме цієї спеціальності було цілком обґрунтованим, і вибірку можна вважати репрезентативною. Анкетування також проводилося і серед випускників інших факультетів університету, що нині працюють на посаді офіс-менеджера у м. Київ.

У результаті анкетування виявилося, що всі опитані значну частину часу проводять за комп'ютером (рис.1), причому 67% теперішніх офіс-менеджерів постійно працюють за комп'ютером. Студенти ж проводять за комп'ютером менше часу, і це легко пояснити: в той час як комп'ютерна техніка та програмне забезпечення – це основний робочий інструмент офіс-менеджерів, то для студентів під час навчання характерним є використання традиційних паперових носіїв; велику роль у навчанні відіграє також і безпосереднє спілкування з викладачами та колегами.

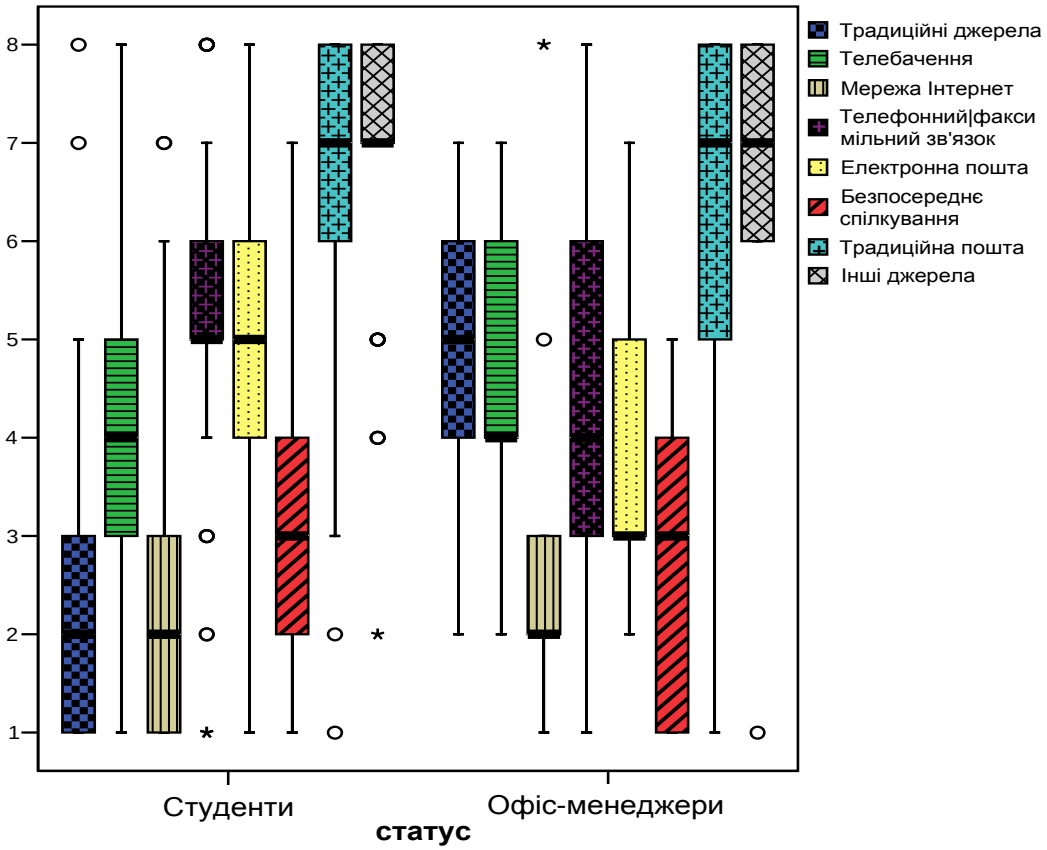

Рис. 2. Ранг частот використання джерел інформації серед опитаних студентів та офіс-менеджерів

В цілому, розглянувши результати опитування (рис. 2), можна зробити висновок, що як для студентів, так і для офіс-менеджерів, першочергове місце в якості джерела отримання інформації займає мережа Інтернет, причому для студентів таке ж значення мають і традиційні паперові носії інформації, такі, як підручники, збірники, довідники тощо, в той час як для менеджерів вони "втратили" свої позиції. Натомість, слід відзначити зростання ролі електронної пошти для офіс-менеджерів у порівнянні зі студентами і разом з тим набагато вищу вагу електронної пошти як для студентів, так і для офіс-менеджерів у порівнянні зі звичайною поштою.

Основні блоки анкетування були орієнтовані на дослідження можливості існування функціонального зв'язку між категорією "психологічного комфорту" та знаннями/вміннями використовувати криптографічні засоби захисту інформації, які надалі розглядатимуться як одна змінна з умовним позначенням "крипт". Для формування значення цієї змінної у метричній шкалі були просумовані бали відповідей для кожного респондента на такі запитання:

1. Чи знають респонденти про небезпеку перехоплення електронних повідомлень.
2. Чи знають респонденти, що таке електронний цифровий підпис.
3. Чи вміють респонденти визначати справжність web-сайту.
4. Чи змогли б респонденти при потребі надіслати підписаний електронний лист.
5. Чи змогли б респонденти при потребі надіслати зашифрований електронний лист.
6. Чи отримували респонденти підписаний електронний лист.
7. Чи отримували респонденти зашифрований електронний лист.

За ствердну відповідь респонденту нараховувався у змінну один бал, за негативну відповідь – 0 балів.

Статистична гіпотеза про зв'язок двох метричних змінних перевіряється у відношенні коефіцієнта кореляції r-Пірсона, який обраховується за формулою:

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - M_x)(y_i - M_y)}{(N-1)\sigma_x\sigma_y},$$ де

$x_1, x_2, ..., x_i, ..., x_N$ та $y_1, y_2, ..., y_i, ..., y_N$ – значення порівнюваних змінних; i – поточний номер опитаного; N – загальна кількість опитаних; M_x та M_y – відповідні середні арифметичні значень змінних; σ_x та σ_y – стандартні відхилення (середньоквадратичні відхилення) для змінних x та y, відповідно; r_{xy} – коефіцієнт кореляції r–Пірсона між змінними x та y [8, с. 70].

Нульовою статистичною гіпотезою в нашому випадку буде рівність r–Пірсона нулю в генеральній сукупності ($H_0 : \bar{r}_{xy} = 0$). Визначення p–рівня значимості здійснюється з допомогою критерія t–Стьюдента:

$$t_e = \frac{r_{xy}\sqrt{N-2}}{\sqrt{1-r_{xy}^2}},\ df = N-2$$ [8, с. 148].

Отже виділимо метричні змінні, для яких ми шукатимемо коефіцієнт кореляції r–Пірсона:

- рівень комфорту – визнався шляхом власних оцінок респондентів з використанням десятибальної метричної шкали від 1 до 10, де одиниця відповідала найнижчому рівню комфорту, 10 – найвищому;
- комфорт графічний – визначався шляхом власних оцінок респондентів з використанням графічної семибальної шкали (рис. 3), яка була переведена у метричну від 1 до 7, де одиниця відповідала найнижчому рівню комфорту, 7 – найвищому;

- довіра – визначалася шляхом оцінки відповідей респондентів на запитання "Наскільки захищено Ви почуваєтеся, використовуючи електронні засоби зв'язку?", причому найнижчий рівень довіри оцінювався в 1 бал, найвищий – у 6 балів, тому була використана шестибальна метрична шкала;

Рис. 3 Шкала-рисунок для визначення рівня психологічного комфорту при роботі з електронними засобами зв’язку

- стать – для позначення жіночої статі використовувалася "1", для позначення чоловічої

– "0";

- навчання – використовувалася восьмибальна шкала від 1 до 8, де 1 – відповідала тим, хто ще не навчався, 2 – студентам першого року навчання, 3 – студентам другого року навчання, 4 – студентам третього року навчання, 5 – студентам четвертого року навчання, 6 – студентам п'ятого року навчання, 7 – студентам шостого року навчання, 8 – офіс-менеджерам;
- крипт – метрична кумулятивна змінна на шкалі від 0 до 7, яка визначалася шляхом сумування відповідей респондентів на сім запитань анкети, зазначених вище, і яка представляє собою загальні знання опитуваних про криптографічні засоби захисту інформації та вміння використовувати їх на практиці.

У результаті підрахунків була побудована кореляційна матриця (табл. 1).

Розмір нашої вибірки менший 100 ($N = 55$), тому вірогідність помилки першого роду встановимо $\alpha = 0{,}05$. Якщо $p < \alpha$, тоді можна говорити про відхилення H_0 і існування статистично достовірного зв'язку між порівнюваними змінними.

Таблиця 1

Кореляційна матриця

		рівень комфорту	довіра	графічний комфорт	стать	рік навчання	крипт
рівень комфорту	Кореляція Пірсона	1	,105	,618(**)	-,485(**)	,438(**)	,460(**)
	Знч.(2-сторон)	.	,444	,000	,000	,001	,000
	N	55	55	55	55	55	55
довіра	Кореляція Пірсона	,105	1	,128	-,115	,161	-,041
	Знч.(2-сторон)	,444	.	,351	,405	,239	,766
	N	55	55	55	55	55	55
графічний комфорт	Кореляція Пірсона	,618(**)	,128	1	-,117	,336(*)	,530(**)
	Знч.(2-сторон)	,000	,351	.	,395	,012	,000
	N	55	55	55	55	55	55
стать	Кореляція Пірсона	-,485(**)	-,115	-,117	1	-,383(**)	-,351(**)
	Знч.(2-сторон)	,000	,405	,395	.	,004	,009
	N	55	55	55	55	55	55
рік навчання	Кореляція Пірсона	,438(**)	,161	,336(*)	-,383(**)	1	,478(**)
	Знч.(2-сторон)	,001	,239	,012	,004	.	,000
	N	55	55	55	55	55	55
крипт	Кореляція Пірсона	,460(**)	-,041	,530(**)	-,351(**)	,478(**)	1
	Знч.(2-сторон)	,000	,766	,000	,009	,000	.
	N	55	55	55	55	55	55

* Кореляція, значима на рівні 0.05 (2-сторон.).
** Кореляція, значима на рівні 0.01 (2-сторон.).

Перш за все слід відзначити, що між змінними "рівень комфорту" та "графічний комфорт" існує статистично достовірний зв'язок із прийнятим рівнем значимості та $\alpha = 0{,}05$ і становить $r_{xy} = 0{,}618$. Доволі високий показник свідчить про те, що дві шкали (метрична та графічна), обрані нами для оцінки рівня психологічного комфорту, доволі сильно пов'язані між собою.

Для змінних "рівень комфорту" та "довіра" підтверджується нульова гіпотеза H_0, так як коефіцієнт кореляції Пірсона доволі низький ($r_{xy} = 0{,}105$), крім того емпіричний p −рівень значимості значно більший теоретичного ($p_e > p_{0,1}$ так як $0{,}444 > 0{,}1$), тобто кореляція статистично

не значима. Та ж ситуація спостерігається і для пари змінних "графічний комфорт" та "довіра": , $p_e = 0{,}351$. Знову ж таки приймаємо гіпотезу H_0 і робимо висновок про відсутність зв'язку між такими категоріями як "психологічний комфорт" та "довіра до засобів електронного зв'язку".

Пара змінних "рівень комфорту" та "крипт" позитивно корелюють між собою із коефіцієнтом кореляції $r_{xy} = 0{,}460$ і прийнятим рівнем значимості ($p_e < p_{0,001}$). Схожа залежність спостерігається між змінними "графічний комфорт" та "крипт": $r_{xy} = 0{,}530$, а також $p_e < p_{0,001}$, тобто для обох випадків $H_0 : \bar{r}_{xy} = 0$ відхиляється для $\alpha = 0{,}05$ і робимо висновок, що між рівнем психологічного комфорту та знаннями/вміннями використовувати криптографічні засоби захисту інформації існує позитивний достовірний зв'язок ($r_{xy} = 0{,}460, N = 55, p < 0{,}001$ для випадку використання десятибальної шкали та $r_{xy} = 0{,}530, N = 55, p < 0{,}001$ для випадку графічної семибальної шкали).

Таким чином робимо загальний висновок про існування певного помірного позитивного статистично-достовірного зв'язку між вміннями використовувати криптографічні засоби захисту інформації та рівнем психологічного комфорту менеджерів, які займаються інформаційною діяльністю. Наявність такого зв'язку безперечно вимагає подальших ґрунтовних досліджень у цьому напрямку, так як забезпечення підвищення рівня психологічного комфорту особистості матиме не тільки персональний, а й груповий позитивний вплив.

Список використаних джерел

1. Макарова М.В., Карнаухова Г.В., Запара С.В. Інформатика та комп'ютерна техніка: Навчальний посібник / За заг. ред. к. е. н., доц.. М.В. Макарової. – Суми: ВТД "Університецька книга", 2003. – 642 с.
2. Литвин І.С. Нові інформаційні технології. – Тернопіль: Економічна думка, 1999. – 140 с.
3. Голубєв В. Теоретико-правові питання захисту інформації в автоматизованих системах // Центр дослідження комп'ютерної злочинності. – http://crime-research.iatp.org.ua/library/Golubev_new_ukr.doc
4. Ложкін Г. Інформаційно-психологічна безпека особистості // Персонал. – 2003. – № 3.– С. 78–81.–
5. http://personal.in.ua/pdf/2003-03.pdf
6. Великий тлумачний словник сучасної української мови (з дод. І допов.) / Уклад. І голов. ред. В.Т. Бусел. – К.; Ірпінь: ВТФ "Перун", 2005. – 1728 с.– http://www.slovnyk.net/?swrd=%C1%E5%E7%EF%E5%EA%E0
7. Ємець В., Мельник А, Попович Р. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. – 144 с.
8. Нориганова О.А. Методология оценки туристской услуги как рыночной категории // Культура народов Причерноморья. – 2002. – № 36. – С. 37–42. – http://www.nbuv.gov.ua/Articles/kultnar/knp200236/knp36_9.doc
9. Наследов А.Д. Математические методы психологического исследования. Анализ и

интерпретация данных. Учебное пособие. 2-е изд., испр. и доп. – СПб.: Речь, 2006. – 392 с.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И ПСИХОЛОГИЧЕСКИЙ КОМФОРТ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

Коцюк Ю.А.

Аннотация

В статье проверяется наличие функциональной связи между уровнем психологического комфорта пользователей компьютерных информационных систем и их знаниями/умениями использовать криптографические средства защиты информации.

Ключевые слова: компьютерные информационные системы, криптографические средства защиты информации.

CRYPTOGRAPHIC MEANS OF INFORMATION PROTECTION AND PSYCHOLOGICAL COMFORT OF THE USERS OF COMPUTER INFORMATIONAL SYSTEMS

Kotsuk Yu.

Resume

The article checks up the existence of functional relation between the level of psychological comfort of the users of computer informational systems and their awareness/skills to use cryptographic means of information protection.

Keywords: computer informational systems, cryptographic means of information protection.