Коцюк Ю. А.

ТРЕНІНГ З КРИПТОГРАФІЇ ЯК ЗАСІБ ПІДВИЩЕННЯ КОМФОРТУ КОРИСТУВАЧІВ ПРИ РОБОТІ З ІНФОРМАЦІЙНИМИ СИСТЕМАМИ

У статті подаються результати формувального експерименту, метою якого було підвищення комфорту користувачів при роботі з інформаційними системами шляхом проведення тренінгу з криптографії.

The article provides the results of generic experiment, conducted with the aim to raise the level of psychological comfort of informational system users by means of training of cryptography.

Статья предлагает результаты формирующего эксперимента, целью которого было повышение комфорта пользователей информационных систем путем проведения тренинга по криптографии.

Тенденції розвитку сучасного суспільства характеризуються активним використанням інформаційних систем. Інформація є важливим стратегічним ресурсом як на державному, регіональному рівнях, так і на рівні підприємств чи організацій. Процеси інформаційного обміну, які супроводжують будь-яку людську діяльність, все частіше набувають "електронної" форми, характеризуються прозорістю кордонів та високою швидкістю. Зростає актуальність вимог до точності, достовірності, автентичності інформаційного матеріалу, забезпечення конфіденційності передачі повідомлень. Вищеназвані вимоги безпосередньо стосуються питань інформаційної безпеки, які неодноразово висвітлювалися як у наукових працях, так і в періодичних виданнях вітчизняних та зарубіжних вчених (Б. Ю. Анін, М. І. Анохін, С. У. Баричев, В. О. Бондаренко, В. О. Голубєв, В. В. Гончаров, М. А. Іванов, В. Г. Крисько О. В. Литвиненко, В. Н. Петров, А. А. Петров, В. С. Пущін, А. Г. Серго, В. В. Ященко). Слід відзначити, що у більшості публікацій розглядаються загальні питання інформаційної безпеки держави, суспільства,

організації. Натомість практична реалізація інформаційної безпеки пересічних користувачів лишається поза увагою.

Основні види діяльності, які здійснює користувач при роботі з інформаційними системами базуються на використанні сервісів обміну повідомленнями, завантаженні та перегляді інформаційних сторінок, здійсненні пошуку інформації []. Тому доцільно розглянути саме методи захисту від загроз інформаційній безпеці, які характерні саме зазначеним видам діяльності. До таких загроз відносять:

- відмову (респондент, що надіслав повідомлення відмовляється від авторства, або ж респондент що отримав повідомлення, відмовляється від факту його отримання);
- фальсифікацію (видачу себе за іншого користувача; санкціонування недозволеного обміну інформацією; нав'язування раніше пересланого повідомлення; приписування авторства повідомлення, сформованого самим порушником, іншій особі і т.п.);
- несанкціонований доступ до конфіденційної інформації (перехоплення повідомлень з метою довідатися їх зміст) [].

Перераховані загрози стають причиною дискомфорту при роботі з інформаційними системами, і навпаки – усунення їх дозволяє підвищити рівень інформаційного комфорту особистості []. Криптографічні засоби захисту інформації якраз і є тим інструментом, який дозволяє захиститися звичайним користувачам від згаданих вище деструктивних впливів.

Метою даної статті є дослідження тренінгу з криптографії як засобу підвищення комфорту користувачів при роботі з інформаційними системами.

Основною складністю вивчення криптографії є потреба оволодіння складним математичним апаратом, який вимагає значних затрат часу для його правильного розуміння та усвідомлення; відповідного "математичного" складу розуму. Вищеозначені фактори є причиною того, що більшість користувачів просто відмовляються від криптографічних засобів захисту інформації в силу їх "незрозумілості". Тому основне завдання запропонованого тренінгу з

криптографії – навчити учасників використовувати засоби криптографії без глибокого розуміння функціонування криптосистем.

Тренінг передбачав кілька структурних частин:

1. Організаційна частина. В ній пояснювалися причини проведення тренінгу, його модулі та розклад.
2. Визначення рівня психологічного комфорту групи учасників. Здійснювалося з допомогою інформаційної модульної системи "MOODLE" Національного університету "Острозька академія", зокрема її модуля "Тест". Студентам пропонувалося дати відповідь на три запитання:

1. Спробуйте оцінити рівень Вашого психологічного комфорту при роботі з електронними засобами зв'язку використовуючи подану нижче шкалу де 1 бал відповідає найнижчому рівню комфорту, 10 балів - найвищому рівню комфорту.

Виберіть одну відповідь

- a. 1 бал
- b. 2 бали
- c. 3 бали
- d. 4 бали
- e. 5 балів
- f. 6 балів
- g. 7 балів
- h. 8 балів
- i. 9 балів
- j. 10 балів

2. На скільки захищено Ви почуваєтеся, використовуючи електронні засоби зв'язку?

Виберіть одну відповідь

- a. повністю довіряю електронним засобам зв'язку
- b. вважаю, що електронні засоби зв'язку мають хороший захист
- c. вважаю, що електронні засоби зв'язку мають хороший захист, проте почуваюся незахищено їх використовуючи
- d. вважаю, що електронні засоби зв'язку мають поганий захист, проте мене це не хвилює
- e. вважаю, що електронні засоби зв'язку мають поганий захист
- f. взагалі не довіряю електронним засобам зв'язку

3. Виберіть зображення, яке, на Вашу думку, найбільше відповідає почуттю Вашого комфорту при роботі з електронними засобами зв'язку.

Виберіть одну відповідь

a. 

b. 

c. 

d. 

e. 

f. 

g. 

Таким чином, було виміряно 3 змінних із загальною назвою "рівень комфорту", "довіра" та "графічний комфорт". Для запитання 1 використовувалася метрична десятибальна шкала від 1 до 10 (1 бал відповідав найнижчому рівню комфорту, 10 - найвищому). Для запитання 2 була використана шестибальна метрична шкала від 1 до 6 (1 – мінімальний рівень довіри, 6 – максимальний рівень довіри). Для запитання 3 була використана графічна шкала у вигляді схематичних емоційних зображень обличчя, яка була переведена у метричну семибальну шкалу від 1 до 7 (1 – найнижчий рівень комфорту, 7 – найвищий рівень комфорту). Змінні "рівень комфорту", "довіра", "графічний комфорт" були позначені відповідно x_1, y_1, z_1.

3. Теоретична частина. Теоретична частина була спланована так, щоб викликати зацікавлення учасників предметом тренінгу і, разом з тим, подати їм базові поняття необхідні при роботі з засобами криптографії. Стимулювання інтересу слухачів реалізовувалося здійсненням екскурсу в історію криптографії; наводилися цікаві факти використання крипто-захисту, демонструвалися слайди. В якості основних понять розглядалися такі поняття як крипто-система, основні можливості криптосистем, симетричні та асиметричні системи, цифровий сертифікат, публічний та приватний ключ тощо []. Для глибшого розуміння поданого матеріалу використовувалися аналогії та приклади. Так криптосистема асоціювалася зі

звичайним замком (не зважаючи на те, що механізми замків можуть бути однакові, секрети, а відповідно й ключі у них різні). Симетричні системи розглядалися на прикладі шифрованих каналів супутникового телебачення (переглядати канал може лише той, хто володіє ключем). Для пояснення роботи асиметричних систем була використана аналогія з замком, який може зачинятися без ключа (будь-хто, навіть протяг, може замкнути двері), натомість, щоб відчинити його потрібен ключ.

4. Практична частина. Передбачала виконання таких завдань:
    a. Створення учасниками тренінгу електронних цифрових сертифікатів. Для створення сертифікатів використовувалося програмне забезпечення поштового клієнта "The Bat!". Порядок створення сертифікату демонструвався з допомогою мульти-медійної презентації, а також був доступний в інформаційній системі MOODLE Національного університету "Острозька академія" у курсі "Криптографія" (приклад див. Рис. 1).

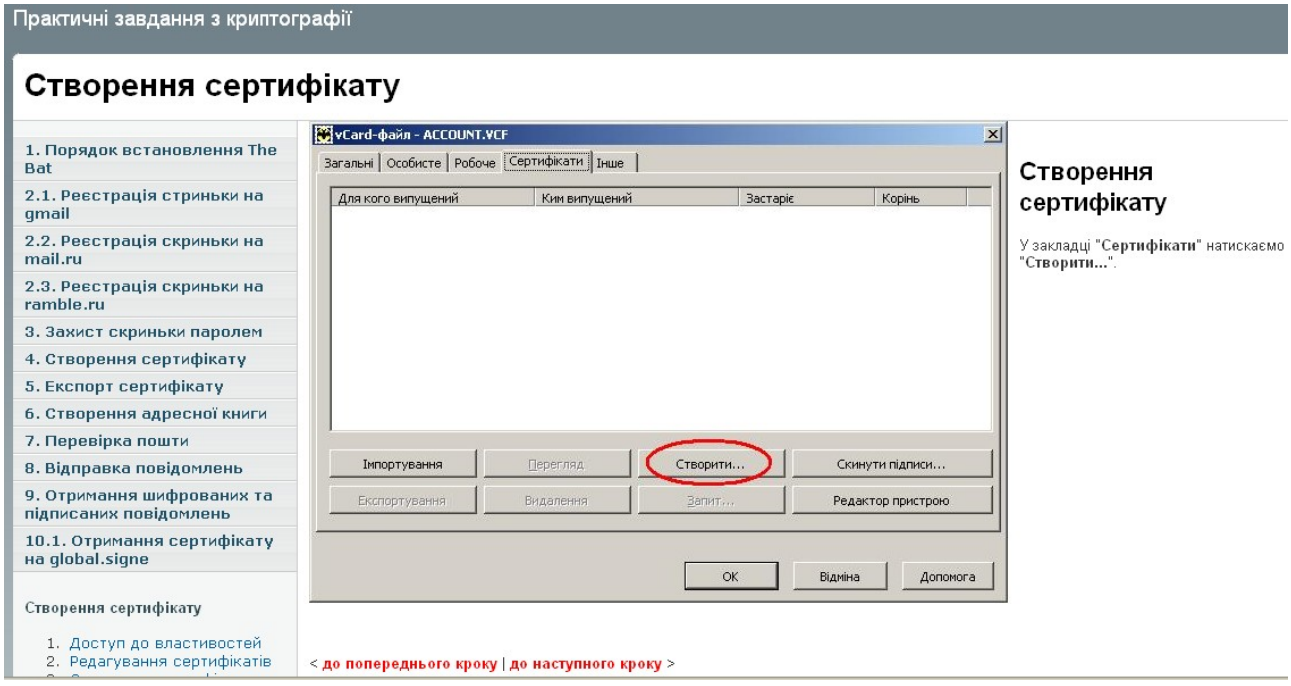

Рис. 1. Фрагмент допомоги на сайті MOODLE НаУОА

    b. Обмін відкритими ключами створених сертифікатів. Учасники розміщували свої відкриті ключі у загальнодоступному каталозі й вносили в адресну книгу відкриті ключі інших учасників.

c. Надсилання підписаних та зашифрованих повідомлень. Учасники розбивалися на пари і надсилали один одному зашифровані та підписані електронні листи. При отриманні зашифрованого й підписаного листа його потрібно було розшифрувати та перевірити справжність цифрового підпису.

d. Отримання учасниками тренінгу пробного цифрового сертифікату від Globalsign. З використанням мережі Інтернет учасники отримували пробний 30-ти денний сертифікат від одного з кореневих центрів сертифікації (так як українські центри сертифікації не надають пробних сертифікатів, було використано Globalsign) і здійснювали надсилання підписаних, а пізніше й зашифрованих електронних листів. Відмінність від попереднього способу полягала у відсутності необхідності обміну відкритими ключами, так як механізм довіри гарантувався Globalsign. Приклад допомоги по отриманню сертифікату див. Рис. 2

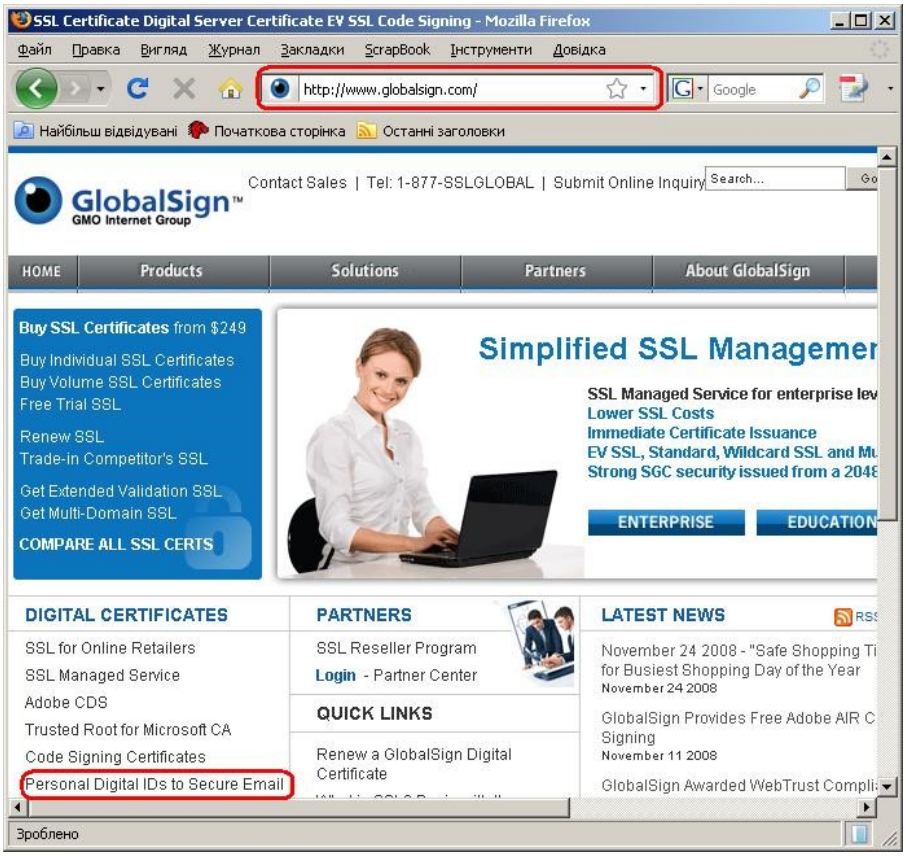

Рис. 2. Приклад допомоги по отриманню цифрового сертифікату від Globalsign

e. Підписування документа MS Word. На цьому етапі кожен учасник тренінгу створював документ MS Word і накладав на нього власний цифровий підпис з допомогою сертифікату, отриманого від Globalsign.

f. Перевірка справжності веб-сайту. Користувачі здійснювали перевірку кількох веб-сайтів через їх цифрові підписи, використовуючи механізми, які надаються типовими програмами для навігації в Інтернет (Internet Explorer, Mozilla Firefox, Opera). Приклад перевірки веб-сайту з допомогою Mozilla Firefox показано нижче (див. Рис. 3).

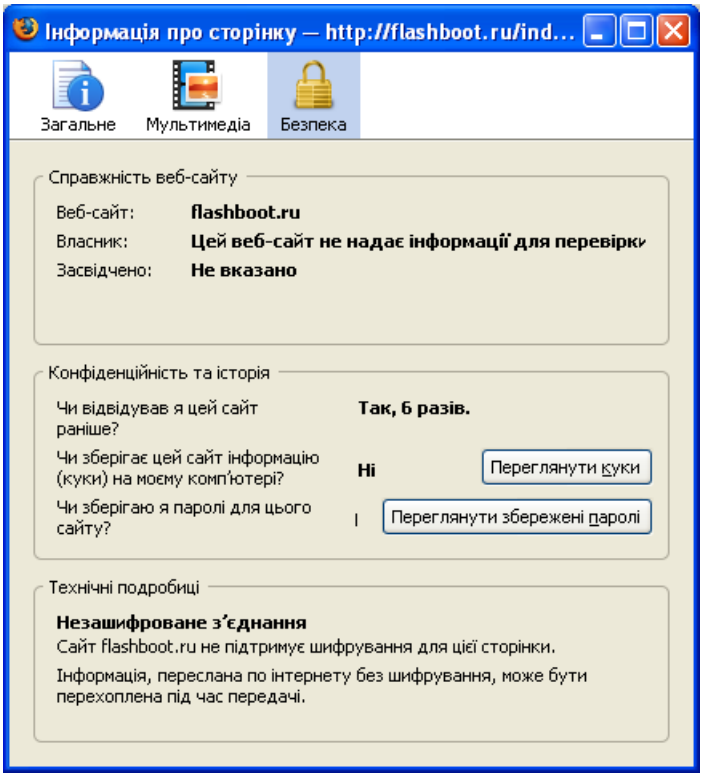

Рис. 3. Перевірка справжності веб-сайту з допомогою Mozilla Firefox

Усі етапи практичної частини демонструвалися з допомогою мультимедійної презентації, а також були (і досі є) доступними в інформаційній системі MOODLE Національного університету "Острозька академія" у курсі "Криптографія".

5. Повторення та узагальнення навчального матеріалу.
6. Заключний етап. Представляв собою повторне опитування і був проведений так само як і другий. Змінні "рівень комфорту", "довіра", "графічний комфорт" були позначені відповідно x_2, y_2, z_2.

В якості наукової гіпотези розглядалося припущення про те, що середнє значення рівня психологічного комфорту групи учасників після проведення тренінгу збільшиться.

В експерименті взяла участь група студентів чисельністю 30 чоловік, що навчалися на факультеті політико-інформаційного менеджменту за спеціальністю "Документознавство та інформаційна діяльність". Так як більшість студентів цієї спеціальності по закінченні навчання працюють на посаді офіс-менеджера, вони і представляли вибірку з генеральної сукупності.

Для перевірки наукової гіпотези були використані параметричні методи порівняння двох вибірок, зокрема критерій t-Ст'юдента для залежних вибірок [, 167].

Для полегшення розрахунків, було використано програмне забезпечення для статистичної обробки результатів досліджень "SPSS 12.0 for Windows" і результати представлено у вигляді таблиці (див. Таблиця 1).

Таблиця 1

Критерій парних вибірок

		Парні різниці					T	ст.св.	Знч. (2-сторон)
		Середнє	Стд. відхилення	Стд. похибка середнього	95% довірчий інтервал різниці середніх				
					Нижня межа	Верхня межа			
Пара 1 "рівень комфорту"	x_1 & x_2	-,900	,995	,182	-1,271	-,529	-4,955	29	,000
Пара 2 "довіра"	y_1 & y_2	-,367	,809	,148	-,669	-,065	-2,483	29	,019
Пара 3 "графічний комфорт"	z_1 & z_2	-,633	,669	,122	-,883	-,384	-5,188	29	,000

Цілком зрозуміло, що для усіх трьох пар потрібно відкинути нульову гіпотезу H_0: $\overline{M}_1 = \overline{M}_2$, так як виконуються нерівноссті $p < 0{,}05$ ($p_x < 0{,}001, p_y < 0{,}05, p_z < 0{,}001$) для кількості ступенів свободи $df = 29$. Тому було прийнято альтернативну гіпотезу. Для пари №1 середні значення рівня психологічного комфорту склали відповідно $M_{x_1} = 5{,}70$, $M_{x_2} = 6{,}60$ (див. Таблиця

2), середнє значення їх різниці – $M_{d_x} = -0{,}900$. Для пари №2 використовувалася шестибальна шкала. Середні значення довіри до електронних засобів зв'язку до та після тренінгу та їх середня різниця мали значення $M_{y_1} = 3{,}53$, $M_{y_2} = 3{,}90$, $M_{d_y} = -0{,}367$ відповідно (див. Таблиця 1, Таблиця 2). І, нарешті, 3 пара, де рівень психологічного комфорту вимірювався з допомогою графічної шкали, дала такі значення для середніх величин: $M_{z_1} = 4{,}37$, $M_{z_2} = 5{,}00$, $M_{d_z} = -0{,}633$.

Таблиця 2

Статистики парних вибірок

		Середнє	N	Стд. відхилення	Стд. похибка середнього
Пара 1 "рівень комфорту" Пара 2 "довіра"	x_1	5,70	30	1,088	,199
	x_2	6,60	30	1,429	,261
Пара 3 "графічний комфорт" Пара 1 "рівень комфорту"	y_1	3,53	30	,937	,171
	y_2	3,90	30	1,062	,194
Пара 2 "довіра" Пара 3 "графічний комфорт"	z_1	4,37	30	,850	,155
	z_2	5,00	30	,830	,152

На основі опрацьованих даних було зроблено висновок, що рівень психологічного комфорту учасників та їх довіра до електронних засобів зв'язку після тренінгу збільшилися статистично достовірно ($p < 0{,}05$).

У якості подальших перспектив досліджень у даному напрямку слід запропонувати вдосконалення та розвиток запропонованої тренінгової системи, пошук оптимальної шкали визначення психологічного комфорту та врахування гендерних особливостей формування комфорту.

Література:

1. Анин Б. Ю. Защита компьютерной информации : практическое пособие / Б. Ю. Анин. — СПб. : BHV-Санкт-Петербург, 2000. — 368 с : ил.
2. Ємець В. Сучасна криптографія : основні поняття / В. Ємець, А. Мельник, Р. Попович. — Львів : БаК, 2003. — 144 с.
3. Коцюк Ю. А. Криптографічні методи захисту інформації та психологічний комфорт користувачів інформаційних систем [Електронний ресурс] / Ю. А. Коцюк // Інформаційні технології і засоби

навчання. — Грудень 2007. — №3. — Умови доступності : http://www.nbuv.gov.ua/e-journals/ITZN/em3/emg.html

4. Коцюк Ю. А. Психологічний комфорт у професійній діяльності менеджера / Ю. А. Коцюк // Збірник наукових праць Інституту психології ім. Г. С. Костюка АПН України / За ред. С. Д. Максименка. Т. VIII, вип. 4. — К., 2006. — С. 160—166.
5. Наследов А. Д. Математические методы психологического исследования : Анализ и интерпретация данных : Учебное пособие / А. Д. Наследов. — [2-е изд., испр. и доп.]. — СПб. : Речь, 2006. — 392 с.

Ключові слова:

Комфорт, інформаційні системи, інформаційна безпека, криптографія, тренінг, цифровий сертифікат,