8. Iakoiu bude nova ukrainska shkola // Shkola: Informatsiino-metodychnyi zhurnal. – 2017. – № 2. – S. 2-8.

Шевченко А. Ф. Проблемы реализации управленческой функции учителя в условиях информационно-образовательного пространства.

Статья посвящена проблемам реализации основной функции учителя в условиях информационно-образовательного пространства. В контексте управленческого подхода к организации профессиональной деятельности, основными факторами его эффективности являются: информация, виртуальная реальность, индивидуальный социокультурный опыт, информационно-педагогическая поддержка. Их анализ дает основание утверждать, что педагогическая деятельность в условиях такого пространства представляет собой систему действий, операций и коммуникаций, направленных на создание условий для самореализации растущей личности. И все это справедливо как для реального, так и виртуального восприятия окружающей среды в процессе усвоения педагогически адаптированного социального опыта, позволяя человеку активно функционировать в современном информационном обществе. Вместе с тем, рассмотрение такой функции в контексте целостности педагогического процесса и субъектности участников образовательного взаимодействия актуализировало ряд противоречий, побуждающих к дальнейшим исследованиям и поискам.

***Ключевые слова**: информационно-образовательное пространство, виртуальная реальность, педагогическая деятельность, управленческая функция учителя.*

Shevchenko A. F. Problems realization of management functions teacher in the information-educational space.

The article is devoted to the problem of realization of the main function of the teacher in the conditions of informational and educational space. In the context of a managerial approach to the organization of professional activities, the main factors of its effectiveness are: information, virtual reality, individual socio-cultural experience, information and pedagogical support. Their analysis gives grounds to assert that pedagogical activity in conditions of such space is a system of actions, operations and communications aimed at creating conditions for the self-realization of a growing personality. And all this is true both for real and virtual perception of the environment in the process of learning pedagogically adapted social experience, allowing a person to actively function in a modern information society. At the same time, consideration of such a function in the context of the integrity of the pedagogical process and the subjectivity of the participants in the educational interaction has actualized a number of contradictions, prompting for further research and searches.

***Keywords:** information-educational space, virtual reality, pedagogical activity, the management function of the teacher.*

УДК 378.016: 004.92.056.55(045)

Матвійчук-Юдіна О. В.

ФОРМУВАННЯ КОМПЕТЕНТНОСТІ ЗІ СТЕГАНОГРАФІЇ У БАКАЛАВРІВ СПЕЦІАЛЬНОСТІ "КІБЕРБЕЗПЕКА" З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "КОМП'ЮТЕРНА ГРАФІКА"

В статті визначено та проаналізовано головні аспекти проектної роботи з

комп'ютерної графіки, що охоплює основні чинники формування компетентності з теорії стеганорафії у студентів кваліфікаційного рівня бакалавр спеціальності 125 "Кібербепека" при вивченні навчальної дисципліни "Комп'ютерна графіка". Розроблено та впроваджено методику надання початкових практичних знань, умінь і навичок для формування компетентності з технології стеганографії у бакалаврів спеціальності "Кібербепека". Деталізовано і впроваджено моделі реалізації стеганографічних методів формування відкритого повідомлення та його вбудовування в файл-контейнер. Досліджено та охарактеризовано графічне представлення і розташування відкритого інформаційного повідомлення у вигляді декількох цифрових графічних файлів. Наведено приклади по представленню і вбудовуванню відкритого інформаційного повідомлення у вигляді безпосередньо тексту в стегано-контейнер.

Ключові слова: *стеганографія, комп'ютерна графіка, стеганографічні методи, компетентності бакалаврів кібербезпеки.*

В попередніх дослідженнях автора, детально розглядались питання формування певного переліку фахових компетентностейу студентів кваліфікаційного рівня бакалавр спеціальності 125 "Кібербепека" з навчальної дисципліни"Комп'ютерна графіка" та приведення їх у відповідність вимогам ринку праці і системі міжнародних стандартів [1].

Запропоновано новий підхід формування компетентностей фахівців з ІТ та їх безпеки, через систему міжнародних стандартів, світові моделі промисловості, а також спираючись напідґрунтя базових властивостей інформаційної системи, в тому числі:

– захист ресурсів інформаційної системи;

– висвітлення інформації та даних.

До освітніх розділів та лекційного матеріалу, що безпосередньо стосується захисту інформаційних ресурсів і даних для комп'ютерної графіки можна віднести такі теми, як:

– стеганографія (процес приховування критичних відеоданих);

– компресія або стиск інформаційного відео потоку;

– голографічний захист інформаційних ресурсів;

– різні класи та види рекламної діяльності підприємств, організацій різних форм власності,

– інфографіка різних класів тощо.

Деталізація формування підходів та переліку компетентностей фахівців з кібербезпеки з предмету "Комп'ютерна графіка" представлена в дослідженнях автора [1; 2; 3].

На базі вище зазначених досліджень внесено корекції щодо навчальних програм та запропонованоновий перелік фахових компетентностей з підготовки бакалаврів спеціальності 125 "Кібербезпека" у відповідності до розробленої методики формування компетентностей з предмету "Комп'ютерна графіка".

Як приклад, формування спеціальних компетентностей фахівців кваліфікаційного рівня бакалавр, автор пропонує розглянути розроблені приклади лабораторнихробіт для формування компетентностей за новою

моделлю, а саме:

– здатність забезпечувати процес приховування критичної відеоінформації в ІКС (стеганографія);

– здатність забезпечувати процеси голографічного захисту інформаційних ресурсів ІКС (голографія);

– здатність до розробки, забезпечення та підтримки різних класів та видів систем інфографіки [2].

Компетентність зістеганографії – здатність забезпечувати процес приховування інформації в графічне повідомлення в ІКС.

Дослідження в контексті що безпосередньо присвячені проблемі викладання комп'ютерної графіки варті праці таких сучасних провідних вітчизняних вчених, як С. Горобця, В. Мироненка, М. Новожилової, Н. Федотової та ін., проблеми в сфері стеганографіїнадають ознаки, тлумачення основних понять в комп'ютерній графіці, і окреслюють компетентності в стеганографії та в стеганоаналізі,праці таких зарубіжних науковців, як: В. Дьяконова, Д. Кіровського, М. Пейнадо, А. Фебіана, А. Г. Коробейникова, С. С. Кувшинова, С. Ю. Блинова, А. В. Леймана, С. И. Нестеровата ін.

Метою досліджень є: розробити та впровадити методику надання початкових практичних знань, умінь і навичок з метою формування компетентності з теорії стеганорафії у студентів кваліфікаційного рівня бакалавр спеціальності 125 "Кібербепека" з предмету "Комп'ютерна графіка".

Результати дослідження.

Стеганографія – тайнопис (з грецької: steganos – таємниця, секрет; graphy – запис). Стеганографічні технології та методи кібернетичного захисту інформаційних (корисних) повідомлень, можна реалізувати за допомогою різних систем і їх властивостей, а саме – технічних, фізичних тощо [4].

Прихування корисного повідомлення методами стеганографії значно зменшує ймовірність або зовсім унеможливлює виявлення самого факту передачі інформації. Стеганографія це наука, яка вивчає способи і методи прихування конфіденційних повідомлень.

Стеганографія *– це наука, яка ґрунтується на технологіях, методах і моделях приховування факту вбудовування корисного інформаційного повідомлення* (*відкритого тексту*) *в інше повідомлення (контейнер)з метою забезпечення конфіденційності передачі даних* [5].

Технології, сукупність методів і моделей стеганографії призначені для запобігання вилученню корисної інформації з інформаційного потоку несанкціонованим або не авторизованим користувачем [4].

Стеганографічним контейнером *називається графічне повідомлення*, *в яке буде розміщено* (*приховано*) *корисну інформацію або конфіденційні дані (відкритий текст).* Будь-який файл чи потік даних може

бути *цифровим контейнером*, якщо контейнер не містить корисного інформаційного повідомлення, то його називають порожнім. Контейнер, що містить корисні дані називається – *заповненим стеганограмою*, або стеганоконтейнером [4, 5].

Цифрові методи стеганографіївикористовують для приховування даних властивості інформаційного контейнера, а саме:

– файл-контейнер, який не потребує абсолютної точності якісної обробки даних, може бути змінений з втратою якості чи розміру, але без втрати безпосередньо функціональності самого файлу;

– відсутність спеціального інструментарію або нездатності органів чуття людини надійно розрізняти незначні зміни в файл-контейнерах, що є наслідком вбудовування корисного повідомлення [6].

За типом контейнерів розрізняють методи, що використовують текстові, аудіо, графічні чи відеосередовища. Кожний виділений клас зорієнтовано на максимальне використання особливостей відповідного середовища та його властивостей. Наприклад, графічні методи використовують особливості людського зору, такі як чутливість до контрасту, розміру, форми, кольору, місцеположення або загальної якості цифрового зображення.

За способом вбудовування інформації (в контейнер) методи поділяються на форматні та неформатні.

Форматні базуються на особливостях формату зберігання даних, які являють собою файл-контейнер. У рамках таких методів формат зберігання порожнього контейнера аналізується з метою відшукання тих службових полів у заголовку файлу, зміна яких у конкретних умовах не вплине на функціональність контейнера. Це можуть бути службові поля, які не використовуються сучасними програмами, не повністю заповнені поля коментарів тощо.

Неформатні ґрунтуються на вбудовуванні інформації безпосередньо у данні порожнього файла-контейнера. Зазначені не форматні методи, також поділяються на два класи процедур різних типів [6].

На даний час існує декілька най поширених підходів, щодо приховування корисного інформаційного повідомлення або відкритого тексту в файл-контейнер:

– пряме вбудовування відкритого тексту (зображення, тексту, даних, тощо) в файл-контейнер;

– не пряме приховування відкритого тексту, тобто реалізація покрокового процесу з виконанням попередніх процедур трансформації відкритого тексту за встановленим алгоритмом чи функцією (стик тексту, зображення чи шифрування даних).

Стиснення даних – це процедура трансформації даних за встановленими правилами, алгоритмами або функціями, яка проводиться з метою зменшення обсягу інформації (розміру файла) [7]. Стиснення буває

без втрат (коли можливе відновлення вихідних даних без спотворень), або з втратами (відновлення можливе з незначними спотвореннями чи з контрольованими втратами). Стиснення без втрат використовується при обробці та збереженні ПЗ і критичних даних. Стиснення з втратами зазвичай застосовується для зменшення об'єму звукової, фото, та відеоінформації. Зрозуміло, що стеганографія використовує тільки методи стиску без втрат інформації з урахуванням відтворення повної ідентичної копії вбудованого відкритого тексту.

Методи і графічні проекти надбання вмінь і навичок стеганографії.

Авторами розроблено та впроваджено приклади практичного виконання, розглянутих вище підходів до стеганографічного захисту інформації при розміщенні в контейнері відкритого повідомлення, а саме з процедурою попередньої трансформації базового інформаційного повідомлення на тлі операції стиснення. Операції стиснення можна виконувати, як приклад, спираючись на прикладне ПЗ архівації даних без втрат інформації типу PKZI компанії PkWareабо інше ПЗтипу WinZip (файлові архіватори і компресори фірми Corel) [5].

Під архівацією даних будемо розуміти процес стиснення даних, що представлені у вигляді зображення або тексту (корисного інформаційного повідомлення). Зрозуміло, різни класи даних, а саме інформаційне повідомлення у вигляді контрастного, штучного чи монохромного зображення може бути скомпресоване різними типами архіваторів з різним ступенем стиску та якості. Однак в запропонованих прикладах, будемо рекомендувати використовувати оптимальний архіватор, як для текстів, так і для фото зображень.

Архіватор *ZIP* – з англ. *Zone Improvement Plan* ("зональний план покращення") – найбільш популярний та поширений в світі метод архівації файлів та стиску даних без втрат інформації. Традиційно архіви ZIP, можуть містити один чи кілька файлів чи каталогів з різними класами повідомлень або велику кількість файлів одного типу (текст, зображення, двійкова послідовність, тощо).

Каталоги архівів ZIP,традиційно зберігаються у вигляді стиснених файлів з розширенням .zip, .zipx або .zi. Для створення ZIP – архівів і в подальшому їх декомпресії (розпакування) файлів, що знаходяться в каталогах, можуть бути використані спеціальні утиліти, наприклад, як в нашому випадку термінальні PKzi й PKUnzi[3] або графічні WinZip, WinRAR, 7-Zipта інш.

WinZip файловий *"пакувальник"* фірми Corel для підтримки різних операційних систем, в т.ч. OS Microsoft Windows з урахуванням формату ZIP як базового (підтримуються архівні формати: .jpg, .rar, .iso, .img, тощо) [7].

Перший крок.

Для виконання практичного надбання базових навичок з стеганографії, необхідно створити графічний файл-контейнер, а саме з цифрового

зображення різних форматів (приклад формату .jpg, рис. 1) з метою подальшої реалізації стеганографічногометоду поступової трансформації і вбудовування інформаційного повідомлення у вигляді zip-файлу.

Рис. 1. Файл-контейнер у вигляді графічного файла – plane.jpg

Для деталізації прикладу, можна впровадити дві моделі формування відкритого повідомлення на базі:

– графічного представлення і вбудовування відкритого інформаційного повідомлення у вигляді декількох цифрових графічних файлів;

– представлення і вбудовування відкритого інформаційного повідомлення, безпосередньо, у вигляді тексту.

У першому випадку файл-контейнер це цифрове фотозображення літака *у вигляді графічного файла – plane.jpg* (рис. 1).

Другийий крок.

Для виконання наступного кроку, запропонуємо створити графічне інформаційне повідомлення – відкритий текст (рис. 2 A, B, C) з подальшою архівацією його в єдиний стислий (кодований) файл-архів у вигляді zip-файлу.

Використовуючи ПЗ графічного архіватора WinZIP або WinRAR виберемо необхідні доступні функції та згідно вибраного шляху виберемо і проведемо операцію завантаження і компресію файлів A.jpg,B.jpg,C.jpg.

*Файли A.jpg, B.jpg, C.jpg будемо вважати, як*відкрите інформаційне повідомлення увигляді цифрових зображеньлоготипів Харківського і Київського Університетів та логотипу Технічного ліцею ННТ У “КПІ” (рис. 2).

Рис. 2. Відкрите інформаційне повідомлення у вигляді цифрових зображень логотипів навальних закладів України

Подальшим кроком повинно бути створення єдиного файл-архіву – pict.zip. Для виконання цієї операції запакуємо три різні зображення в *A.jpg B.jpg C.jpg в* архів *pict.zip.*

В даному випадку єдиний архів *pict.zip,* ще являє собою інформаційне повідомлення у вигляді так званого – "відкритого тексту", бо він ще не вбудований у файл-контейнер. Однак, зображення логотипів, вже пройшли перші трансформації у вигляді компресії (кодування) та ці кроки вносять доповнення до назви повідомлення – "кодований (стислий) відкритий текст".

Сучасне ПЗ архіваторів має додаткову функцію при компресії даних – шифрування. При виконанні операції стиску даних, з'являється додаткове повідомлення з пропозицією зашифрувати ваші данні різними типами шифраторів.

Третій крок

Останнім кроком вбудовування кодованого відкритого тексту у вигляді файлу *pict.zip*, повинно бути використання прикладного програмного забезпечення, що може реалізувати різні методи стеганографії придатні за функціональними можливостями до розміщення скомпресованих *.zip* файлів у графічний файл-контейнер.

Для того, щоб приховати стислі зображення трьох логотипів *pict.zip* з архіву у графічний файл *plane.jpg*, скористаємось прикладним програмним продуктам, а також вкажемо безпосередні шляхи знаходження файлів:

– кодованого відкритого тексту pict.zip (з шифруванням або ні);

– фалу-контейнеру plane.jpg;

– місце подальшого розташування заповненого фалу-контейнеру з стеганограмою або стеганоконтейнера secret_file.jpg.

В подальшому необхідно виконати зворотні процедури вилучення кодованого відкритого тексту та декомпресії графічного інформаційного повідомлення. Файл-контейнер *з стеганограмою*не повинен відрізнятись на погляд людини експерта від рис. 1, а також в подальшому вилучені відкриті повідомлення логотипів не повинні бути спотворені.

Додатковим прикладом вбудовування інформаційного повідомлення,

може бути використання ПЗ для приховання текстової інформації в файл формату PNG або інших типах форматів.

Висновки та перспективи подальших досліджень.

В роботі розроблено та впроваджено методику надання початкових практичних знань, умінь і навичок для формування компетентності з теорії стеганорафії у студентів кваліфікаційного рівня бакалавр спеціальності 125 “Кібербепека” з предмету “Комп’ютерна графіка”.

На базі розроблених прикладів деталізовано і впроваджено моделі реалізації стеганографічних методів формування відкритого повідомлення та його вбудовування в файл-контейнер на базі:

– графічного представлення і розташування відкритого інформаційного повідомлення у вигляді декількох цифрових графічних файлів;

– представлення і вбудовування відкритого інформаційного повідомлення у вигляді безпосередньо тексту в стегано-контейнер.

Використана література:

1. *Матвійчук-Юдіна О. В.* Індустріальна модель як основа формування професійних компетентностей фахівців з кібербезпеки / О. В. Матвійчук-Юдіна // Збірник наук. праць Уманського державного пед. унів. ім. Павла Тичини. – 2017. – Вип. № 2. – С. 247-254.
2. *Матвійчук-Юдіна О. В.* Ключові компетентності фахівців спеціальності “Кібербезпека” з предмету “Комп’ютерна графіка” згідно індустріальної моделі промисловості / О. В. Матвійчук-Юдіна // Вісник Житомирського державного університету. – 2017. – № 4(90). – С. 93-98.
3. *Матвійчук-Юдіна О. В.* Властивості інформаційної системи відповідно міжнародних стандартів – основа формування компетентностей майбутніх ІТ-фахівців з предмету “Компютерна графіка” / О. В. Матвійчук-Юдіна // РІВНЕ Проблеми інженерно-педагогічної освіти : збірник наукових праць. – 2017. – № 48-49. – С. 268-277.
4. *Конахович Г. Ф.* Компютерная стеганография. Теория и практика / Г. Ф. Конахович, Ф. Ю. Пузыренко. – Київ : “МК-Пресс”, 2006. – 288 с.
5. *Ватолин Д.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин // ДИАЛОГ-МИФИ. – Москва, 2012. – 384 с.
6. *Сэломон Д.* Сжатие данных, изображений и звука / Д. Сэломон // Техносфера–М. – 2006. – 386 с.
7. *Грибунин В. Г.* Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // Солон-Пресс. – Москва, 2002. – 272 с.

References:

1. *Matviichuk-Yudina O. V.* Industrialna model yak osnova formuvannia profesiinykh kompetentnostei fakhivtsiv z kiberbezpeky / O. V. Matviichuk-Yudina // Zbirnyk nauk. prats Umanskoho derzhavnoho ped. univ. im. Pavla Tychyny. – 2017. – Vyp. № 2. – C. 247-254.
2. *Matviichuk-Yudina O. V.* Kliuchovi kompetentnosti fakhivtsiv spetsialnosti “Kiberbezpeka” z predmetu “Kompiuterna hrafika” zghidno industrialnoi modeli promyslovosti / O. V. Matviichuk-Yudina // Visnyk Zhytomyrskoho derzhavnoho universytetu. – 2017. – № 4(90). – C. 93-98.
3. *Matviichuk-Yudina O. V.* Vlastyvosti informatsiinoi systemy vidpovidno mizhnarodnykh standartiv – osnova formuvannia kompetentnostei maibutnikh IT-fakhivtsiv z predmetu “Kompiuterna hrafika” / O. V. Matviichuk-Yudina // RIVNE Problemy inzhenerno-pedahohichnoi osvity : zbirnyk naukovykh prats. – 2017. – № 48-49. – C. 268-277.
4. *Konakhovich G. F.* Kompyuternaya steganografiya. Teoriya i praktika / G. F. Konakhovich, F. Yu. Puzyrenko. – Kyiv : “MK-Press”, 2006. – 288 s.
5. *Vatolin D.* Metody szhatiya dannykh. Ustroystvo arkhivatorov, szhatie izobrazheniy i video / D. Vatolin, A. Ratushnyak, M. Smirnov, V. Yukin // DIALOG-MIFI. – Moskva, 2012. – 384 s.

6. *Selomon D.* Szhatie dannykh, izobrazheniy i zvuka / D. Selomon // Tekhnosfera–M. – 2006. – 386 s.
7. *Gribunin V. G.* Tsifrovaya steganografiya / V. G. Gribunin, I. N. Okov, I. V. Turintsev // Solon-Press. – Moskva, 2002. – 272 s.

Матвийчук-Юдина О. В. Формирование компетентности по стеганографии у бакалавров специальности "Кибербезопасность" по учебной дисциплине "компьютерная графика".

В статье обозначены и проанализированы главные аспекты проектной работы по компьютерной графики, которые охватывает основные факторы формирования компетентности по теории стеганорафии у студентов квалификационного уровня бакалавр специальности 125 "Кибербезопасность" при изучении дисциплины "Компьютерная графика". Разработана и внедрена методика предоставления начальных практических знаний, умений и навыков для формирования компетентности по технологии стеганографии у бакалавров специальности "Кибербезопасность". Детализированны и внедрены модели реализации стегано графичних методов формирования открытого сообщения и его встраивания в файл-контейнер. Исследовано и охарактеризовано графическое представление и расположение открытого информационного сообщения в виде нескольких цифровых графических файлов. Приведены примеры по представлению и встраиванию открытого информационного сообщения в виде непосредственно текста в стегано-контейнер.

Ключевые слова: *стеганография, компьютерная графика, стеганографические методы, компетентности бакалавров кибер безопасности.*

Matviychuk-Yudina O. V. Forming of competence on steganografii for the bachelors of speciality "Cyberbuck safety" on educational discipline "computer graphics".

In the article marked and analysed main aspects of project work to on computer graphics, which engulfs basic factors of forming of competence on the theory of steganorafii for the students of qualifying level bachelor of speciality 125 "Cyberbuck safety" at the study of discipline the "Computer graphics". Developed and inculcated method of grant of initial practical knowledges, abilities and skills for forming of competence on technology of steganografii for the bachelors of speciality "Cyberbuck safety". Detals and the models of realization of quilted grafichnikh methods of forming of the opened report and his building are inculcated in a file-container. Investigational and described graphic presentation and location of the opened information message as a few digital graphic files. Examples are resulted on presentation and building of the opened information message as a direct text in stegano-konteyner.

Keywords: *quilted grafiya, computer graphics, quilted graphic methods, to the competence of bachelors cyberbuck of safety.*