УДК 004.932.2

ІГОР ЯКОВІВ,
АНДРІЙ ДАВИДЮК,
ІГОР КУЛИКІВСЬКИЙ

СИСТЕМА ЗАБЕЗПЕЧЕННЯ АВТОРСТВА ЦИФРОВОГО ФОТОЗНІМКУ

В умовах ведення інформаційно-психологічної війни проти України зростає необхідність у створенні нових засобів забезпечення достовірності і підтвердження авторства інформації на цифрових носіях. У маніпулятивних матеріалах, що стосуються різних сфер нашого життя і розповсюджуються в Інтернет, часто використовуються чужі цифрові фотознімки з контекстом, який викривляє реальні події відповідно до мети зацікавленої в успішній маніпуляції сторони. Механізми оперативного підтвердження (встановлення) авторства дозволяють правильно оцінити достовірність таких матеріалів як у соціальній, так і у технічній сферах. У статті представлений один з можливих способів підтвердження авторства на цифрові фотознімки. Цей підхід також можливо застосовувати в рамках процедур судової експертизи й інших сферах використання цифрових фотознімків (фотостоки, соціальні мережі, веб ресурси з використанням фотографічного контенту).

Ключові слова: захист авторства, цифровий фотознімок, інформаційно-функціональний аналіз, унікальна цифрова послідовність, порівняння цифрових знімків, показник подібності, інформаційна безпека.

Вступ. В умовах широкого розповсюдження інформаційних технологій методи традиційного захисту об’єктів інтелектуальної власності не завжди є ефективними. Літературні, аудіовізуальні, музичні, фотографічні твори, комп’ютерні програми та інші об’єкти авторського права, відтворені у цифровій формі, все частіше стають об’єктами правопорушень [1].

Основу традиційних механізмів забезпечення авторського права (патентування, експертна оцінка, порівняння та інші) забезпечує паперовий документообіг. Наслідком такої реалізації інформаційних процесів стають значні часові втрати і високий рівень появи суб’єктивної помилки. Розробка механізмів, що полягають в застосуванні сучасних інформаційних технологій, дозволяють значно підвищити якість зазначених процедур [2]. Доцільно зазначити, що такий підхід важливий не тільки для сфери цивільно-правових відносин. В умовах інтенсивного інформаційно-психологічного протистояння [3], яке нав’язане Україні гібридною війною, наявність засобів оперативної перевірки автентичності авторства інформаційних матеріалів різного характеру в Internet дозволяє значно зменшити можливості маніпулятивного впливу.

Аналіз відомих підходів щодо захисту авторства цифрових фотознімків. З метою визначення сутності інформаційних процесів забезпечення авторських прав в Internet проведено аналіз ряду праць, що присвячених даній проблемі [4-7]. Найбільш поширений на сьогодні підхід щодо захисту авторських прав на цифровий фотознімок заснований на попередній процедурі патентування і наступному судовому розгляді (в разі виявлення факту порушення, тобто компрометації). Для аналізу і формалізованого представлення цих інформаційних процесів застосовано атрибутивно-трансфертний підхід до сутності інформації та методи системного аналізу [8]. Порядок дій із захисту авторських прав на цифровий фотознімок у вигляді інформаційно-функціональної структури представлений на рис.1.

У рамках традиційного підходу можна виділити наступні етапи:

1) патентування цифрового фотознімку (ЦФ), де
   1.1 – Подання заявки та цифрового фотознімку до органу патентування;
   1.2 – Отримання авторського свідоцтва з зазначенням персональних даних автора (ПДА).

2) розповсюдження ЦФ в Internet і визначення факту його компрометації (ЦФ* – скомпрометований знімок), де
   2.1 – завантаження автором свого цифрового фотознімку до мережі Інтернет;
   2.2 – завантаження автором скомпрометованого цифрового фотознімку (ЦФ*) з мережі Інтернет.
3) судовий розгляд (СР – судове рішення).

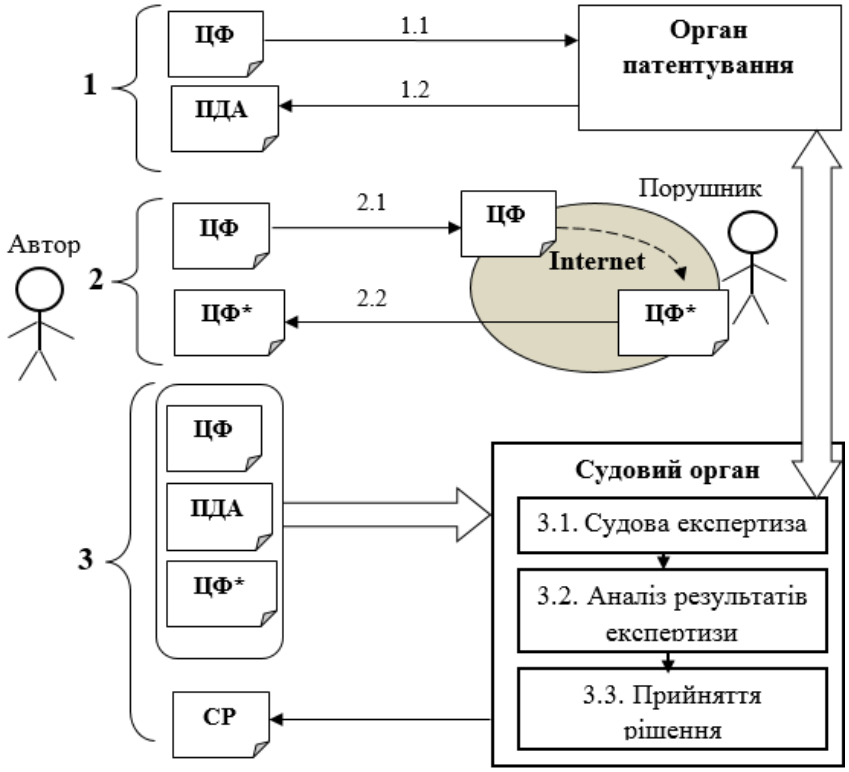

Рисунок 1– Сутність інформаційного процесу за традиційним підходом до захисту авторського права на цифровий фотознімок

Під час судової експертизи (див. п. 3.1 на рис. 1) визначається автентичність патенту. У разі наявності графічних змін до ЦФ* відносно авторського знімку (масштабування, зміна контрастності, зміна кольору, обрізка та інші) необхідна процедура перевірки подібності двох знімків.

Недоліки традиційного підходу:

– заснований на паперовому документообігу. Значні часові втрати;

– значний рівень суб'єктивної помилки під час перевірки подібності;

– неможливість застосування поза судової сфери, що важливо в аспекті протидії масштабним інформаційно-психологічним впливам.

Крім заходів захисту в цивільно-правовій сфері були досліджені засоби забезпечення авторства на основі інформаційних технологій.

Для забезпечення вирішення проблеми захисту цілісності, накладення маркеру авторства та конфіденційності текстових та бінарних файлів широко використовується електронно-цифровий підпис (*Digital Signature, DS*). Організація розповсюдження відкритого (*Public key*) та закритого ключів (*Private key*) здійснюється через інфраструктуру відкритих ключів (*Public key infrastructure, PKI*), до якої належить ієрархія довірчих центрів сертифікації. Такий підхід передбачає обов'язковий супровід *ЦФ* при поширенні цифровим підписом *DS*. Це ефективно при обміні інформацією в рамках довірчих відносин. У рамках реалізації розглянутої загрози порушник може знищити цифровий підпис.

Також однією з рекомендацій щодо захисту свого авторського права є не передавання вихідних файлів цифрових фотознімків в форматі **.RAW* та файлів *AdobePhotoshop (*.psd)*. Але за достатніх умінь та елементарних засобів ці підходи легко скомпрометувати [9].

Ще одним із підходів до захисту цифрових фотознімків є накладання цифрового водяного знаку (*Digital Water Mark, DWM*) для виявлення факту несанкціонованого редагування і підтвердження авторства [4], але даний засіб не є стійким до внесення змін у фото (масштабування, зміна кольорів, тощо).

Проведений аналіз підтверджує актуальну потребу у розробці системи забезпечення авторства цифрових фотознімків (далі – Система) на основі сучасних інформаційних технологій. Така Система надасть можливість:

– підвищити ефективність традиційної системи захисту авторського права на ЦФ в рамках цивільно-правових відносин;

– користувачам Internet проводити оперативну перевірку даних про авторство ЦФ, що важливо в аспекті протидії масштабним інформаційно-психологічним впливам.

Загальний опис роботи розробленої системи забезпечення авторства цифрового фотознімку. На відміну від традиційного захисту всі інформаційні процеси в розробленій Системі реалізуються в електронно-цифровому середовищі інформаційних технологій. Перелік, послідовність і сутність цих процесів відображається інформаційно-функціональною структурою системи (див. рис. 2).

Процес захисту включає наступні етапи:

1) реєстрація автора і формування сертифікату ЦФ;
2) розповсюдження ЦФ в Internet і визначення факту його компрометації (ЦФ* – скомпрометований знімок);
3) верифікація ЦФ (3.1* – взаємодія центру сертифікації і центру верифікації підчас верифікації).

Спочатку автор реєструється в ЦС. Його персональні дані (ПДА) і цифровий фотознімок (ЦФ) застосовуються для формування сертифікату (С). У разі виявлення факту несанкціонованого використання свого фотознімку автор пред'являє ЦФ, С і ЦФ* в центр верифікації (ЦВ). Останній за допомогою ЦС перевіряє автентичність сертифікату, подібність ЦФ* початковому знімку і приймає рішення про його авторство. Основу процедур перевірки сертифікату і подібності складає механізм формування *унікальної цифрової послідовності фотознімку* (*УЦП*).

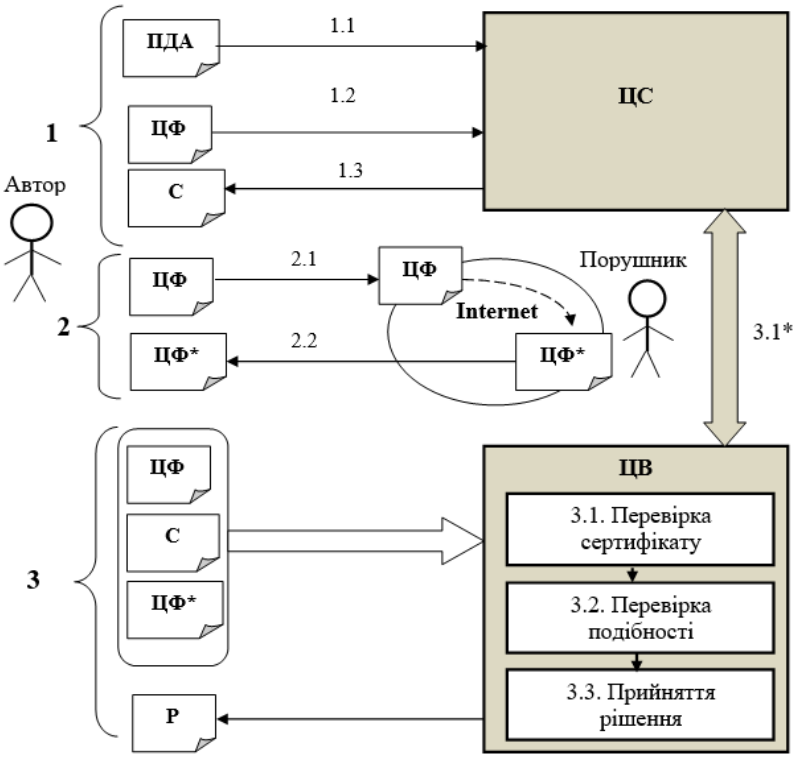

Рисунок 2– Інформаційні процеси запропонованої системи захисту авторського права на цифровий фотознімок

Реєстрація автора і сертифікація цифрового знімку. Сутність інформаційних процесів ЦС на 1 етапі представлена у вигляді інформаційно-функціональної структури на рис. 3.

Основу роботи *ЦС* становить процедура формування в центрі сертифікації *УЦП*, яка залежить від значення кольорових складових x_r, x_b, x_g кожного пікселя цифрового зображення. Тобто

$$УЦП = F_1(M), \quad (1)$$

де $F_1(.)$ – функція від зображення ЦВ в *УЦП*;

$M = \{(x_r, x_b, x_g)_k\}$ – множина значень кольору всіх пікселів;

$k = 1,..., K$ – поточний номер пікселя, *К* – кількість пікселів в ЦФ $(x_r, x_b, x_g)_k$ – упорядкований набір кольорових складових *k*–го пікселя (*red, blue, green*).

На основі персональних даних автора ПДА і УЦП за допомогою перетворення F_2 формується сертифікат *С*:

$$C = F_2(ПДА, УЦП), \quad (2)$$

Сертифікати і *УЦП* для кожного знімку зберігаються у базі даних (*БД*) (див. рис.3). Цифрові фото зберігаються тільки у автора.

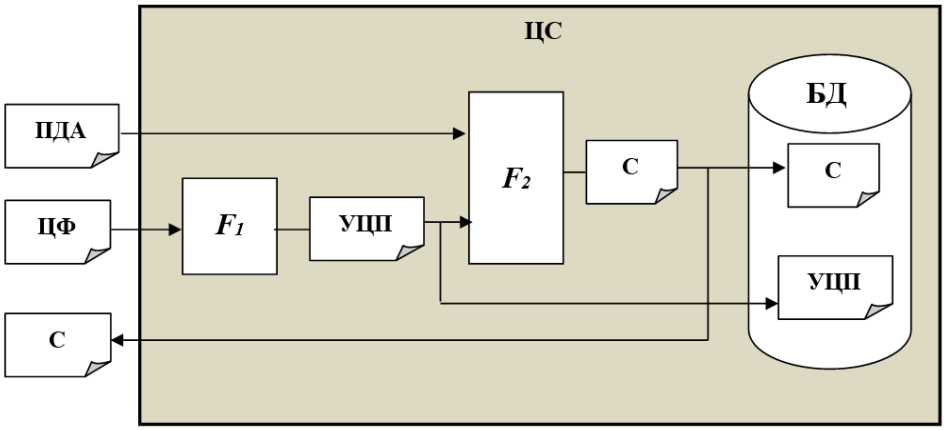

Рисунок 3 – Інформаційні процеси на етапі реєстрації автора і формування сертифікату *ЦФ*

Верифікація цифрового фотознімку. Мета цього етапу – прийняття рішення про авторство *ЦФ* на основі процедур перевірки сертифікату і визначення подібності між *ЦФ* і *ЦФ**. Сутність інформаційних процесів верифікації представлена на рис. 4.

Між *ЦВ* і *ЦС* існують довірчі відносини. Рішення *Р* про авторство *ЦФ* формується на основі порівняння (F_4) унікальних цифрових послідовностей. $УЦП^{(ЦС)}$ – послідовність, яка зберігається в *БД ЦС* і визначається за запитом від *ЦВ*. Цей запит формується (F_3) на підставі сертифіката *С*, який надається автором центру верифікації разом з *ЦФ* і *ЦФ**. $УЦП^{(ЦВ)}$ – цифрова послідовність, яка формується (F_1) на основі оригіналу *ЦФ*, що надав автор центру верифікації. Аналогічно формується унікальна цифрова послідовність від скомпрометованого знімку *УЦП**.

$$P = F_4(УЦП^{(ЦФ)}, УЦП^{(ЦС)}, УЦП^{*}), \quad (3)$$

де *Р* – рішення про авторство;

$УЦП^{(ЦФ)}$ – УЦП від цифрового фотознімку, що надав автор;

$УЦП^{(ЦС)}$ – УЦП , що знаходиться в ЦС, $УЦП^{*} = F_1(ЦФ^{*})$ – УЦП скомпрометованого фотознімку

Правило прийняття рішення про авторство. Розглядається два випадки:

а) авторство підтверджено

$P = 1$, якщо $pp = f_{пор}(УЦП^{(ЦФ)}, УЦП^{(ЦС)}) = 100\%$

$i\ pp = f_{пор}(УЦП^{(ЦФ)}, УЦП^{(ЦФ*)}),\ 70\% < pp < 100\%,$

б) авторство не підтверджено

$\mathrm{P} = 0$, якщо $pp = f_{пор}(УЦП^{(ЦФ)}, УЦП^{(ЦС)}) = 100\%$

$i\ pp = f_{пор}(УЦП^{(ЦФ)}, УЦП^{(ЦФ*)}),\ pp < 70\%,$

де pp – показник подібності;

$f_{пор}(.)$ – функція порівняння.

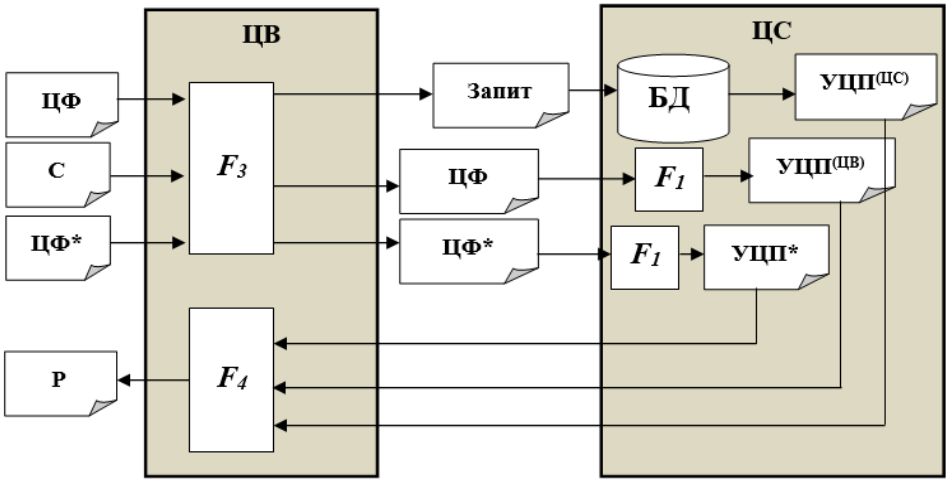

Рисунок 4 – Інформаційні процеси на етапі верифікації

Аналіз способів використання системи забезпечення авторства цифрових фотознімків. Дана система призначена для захисту авторського права на цифровий фотознімок у судовому порядку. За ситуації, коли його автор попередньо зареєстрував своє фото в системі та отримав сертифікат. Потім помітив свій цифровий фотознімок, викладений у відкритому доступі в мережі Інтернет іншою людиною. Автор висуває претензію щодо порушення авторського права та несанкціонованого використання його інтелектуальної власності. Людина, що виклала це фото відмовляється визнавати дану претензію. Автор цифрового фотознімку подає позов до суду.

Розроблена система завдяки інформаційним технологіям пришвидшить час експертизи та знизить імовірність помилки при прийнятті рішення для висновку експертизи. Опис системи в даній роботі буде відповідати саме цій ситуації.

Висновки. На основі запропонованих методів аналізу і порівняння цифрових знімків розроблено принципи функціонування системи забезпечення авторства цифрових фотознімків. Система надає можливість:

– збільшити ефективність наявної системи захисту авторського права на ЦФ в рамках судової експертизи;

– користувачам мережі Internet здійснювати перевірку даних про авторство ЦФ, що важливо в аспекті протидії масштабним інформаційно-психологічним впливам.

Перспективи подальших досліджень:

– оптимізація методів та способів порівняння цифрових фотознімків;

– підвищення стійкості системи до можливих вразливостей.

Результати експериментального дослідження показали, що програмно реалізовані функції (*F1* та *F4*) виконують завдання аналізу та порівняння цифрових фотознімків на предмет подібності. В рамках експерименту порівнювалися авторський знімок і скомпрометовані *ЦФ*, які отримані шляхом застосування різних змін (масштабування, зміна контрастності, зміна кольору, обрізка та інші) до авторського знімку. Результати експерименту підтверджують працездатність запропонованого підходу. Детальніше про проведення експерименту буде розкрито в наступній статті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Н.В. Троцюк, "Особливості адміністративно-правового захисту авторського права в Україні", *Митна справа*, № 2 (2.2), с. 105-110.

[2] Кабінет міністрів України. (2001, Груд. 27). *Постанова КМУ №1756, Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір.* [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/1756-2001-%D0%BF. Дата звернення: Верес. 12, 2016.

[3] Президент України. (2015, Трав. 6). *Указ Президента України № 287, Про Стратегію національної безпеки України.* [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/287/2015. Дата звернення: Верес. 24, 2016.

[4] В.О. Хорошко, О.Д. Азаров, та М.Є. Шелест, *Основи комп'ютерної стеганографії*. Вінниця, Україна: ВДТУ, 2003.

[5] М.В. Гайворонський, та О.М. Новіков, *Безпека інформаційно-комунікаційних систем*. Київ, Україна: Видавнича група BHV, 2009.

[6] Ю.А. Белобокова, и Э.С. Клышинский, "Защита информационного содержания цифровых фотографий методом многократной маркировки цифровыми водяными знаками. [Электронный ресурс]. Доступно: http://samag.ru/archive/article/2671. Дата обращения: Сент., 24, 2016.

[7] Верховна рада України. 8 сесія. (1993, Груд. 23). *Закон № 3792-XII, Про авторське право і суміжні права.* [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/3792-12. Дата звернення: Верес. 24, 2016.

[8] І.Б. Яковів, "Канал зв'язку з позицій атрибутивно-трансферної сутності інформації", Information technology and security, vol. 1, iss. 2, pp. 84-96, 2012.

[9] В. Пацай, "Преимущества и недостатки форматов изображений RAW, JPEG и TIFF". [Электронный ресурс]. Доступно: http://kaddr.com/2014/12/takie-raznye-formaty-raw-jpeg-tiff/. Дата обращения: Сент., 24, 2016.

Стаття надійшла до редакції 28 вересня 2016 року.

REFERENCES

[1] N.V. Trotsiuk, "Features of administrative and legal protection of copyright in Ukraine", *Customs*, no. 2 (2.2), pp. 105-110, 2014.

[2] Cabinet of Ministers of Ukraine. (2001, Dec. 27). Decree of CMU №1756, *On state registration of copyright and agreements concerning copyright to work.* [Online]. Available: http://zakon3.rada.gov.ua/laws/show/1756-2001-%D0%BF. Accessed on: Sept. 12, 2016.

[3] President of Ukraine. (2015, May 6). *Order of the President of Ukraine № 287, About national security strategy of Ukraine.* [Online]. Available: http://zakon3.rada.gov.ua/laws/show/287/2015. Accessed on: Sept. 24, 2016.

[4] V.O. Khoroshko, O.D. Azarov, and M.Ye. Shelest, *Fundamentals of computer steganography*. Vinnytsia, Ukraine: VNTU, 2003.

[5] M.V. Haivoronskyi, and O.M. Novikov, *Information and communication systems security*. Kyiv, Ukraine: Publishing Group BHV, 2009.

[6] Iu.A. Belobokova, and E.S. Klyshinskii, "Protection of the information content of digital photographs using multiple labeling method of digital water marks". [Online]. Available: http://samag.ru/archive/article/2671. Accessed on: Sept. 24, 2016.

[7] Verkhovna Rada of Ukraine. 8th Session. (1993, Dec. 23). *Law of Ukraine № 3792-XII, A*bout authorship and related rights. [Online]. Available: http://zakon3.rada.gov.ua/laws/show/3792-12. Accessed on: Sept. 24, 2016.

[8] I.B. Yakoviv, "The communication channel from the position of attributive-transfer nature of the information", Information technology and security, vol. 1, iss. 2, pp. 84-96, 2012.

[9] V. Patsai, "Advantages and Disadvantages of RAW image formats, JPEG and TIFF". [Online]. Available: http://kaddr.com/2014/12/takie-raznye-formaty-raw-jpeg-tiff/. Accessed on: Sept. 24, 2016.

ИГОРЬ ЯКОВИВ,
АНДРЕЙ ДАВИДЮК,
ИГОРЬ КУЛИКОВСКИЙ

СИСТЕМА ОБЕСПЕЧЕНИЯ АВТОРСТВА ЦИФРОВОГО ФОТОСНИМКА

В условиях ведения информационно-психологической войны против Украины возрастает необходимость в создании новых средств обеспечения достоверности и подтверждения авторства информации на цифровых носителях. В манипулятивных материалах, что касаются разных сфер нашей жизни и распространяются в Интернет, часто используются чужие цифровые фотоснимки с контекстом, которой искажает реальные события в соответствии к цели заинтересованной в успешной манипуляции стороны. Механизмы оперативного подтверждения (установления) авторства позволяют правильно оценить достоверность таких материалов как в социальной, так и технической сферах. В статье представлен один из возможных способов подтверждения авторства на цифровые фотоснимки. Этот подход также можно применять в рамках процедур судебной экспертизы и других сферах использования цифровых фотоснимков (фотостоки, социальные сети, веб ресурсы с использованием фотографического контента).

Ключевые слова: защита авторства, цифровой фотоснимок, информационно-функциональный анализ, уникальная цифровая последовательность, сравнение цифровых снимков, показатель подобия, информационная безопасность.

IHOR YAKOVIV,
ANDRII DAVYDIUK,
IHOR KULYKIVSKYI

THE SYSTEM OF PROVIDING AUTHORSHIP PROTECTION FOR DIGITAL PHOTO

In conditions of information-psychological war against Ukraine, the necessity in creating new means of authenticity and proof of information authorship on digital carrier increases. In manipulative materials which have a connect with different areas of our life and distributed in the Internet, often alien digital photos with the context, which distorts the real events according to interested in successful manipulation side. Mechanisms of operational confirmation (determination) of authorship can properly estimate the reliability of such materials as in social that in technical areas. The article presents one way to confirm digital photos authorship. The idea of this approach has a place in creation of certification and verification centres for digital photo. In the certificationcentre, the digital photo is analyzed and the unique digital sequence is made, this sequence is saved in database of certification centre. In the situation when you want to verify authorship in verification centre of digital photo, the unique digital sequence of digitalphoto, which is verified, is comparedwith data based in database of certification centre and the decision about authorship of digital photo is made. Therefore, in this article the existing approaches for authorship protection are analyzed. The new system of authorship protection, which consists of certification and verification centres, is offered. In addition, information processes, which have a place in centres and rules of decision making about digital photo authorship, are presented. This approach can also be used for the forensics examination procedures and other areas of digital photos application (e.g., photo stocks, social networks, web sources, which use photographic content).

Keywords: protection of authorship, digital photo, information and functional analysis, unique digital sequence, comparison of digital images, similarity index, information security.

Ігор Богданович Яковів, кандидат технічних наук, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: iyakov52@gmail.com.

Андрій Вікторович Давидюк, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.
E-mail: andrey19941904@gmail.com.
Ігор Михайлович Куликівський, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.
E-mail: ikylikovskiy1995@gmail.com.

Игорь Богданович Яковив, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.
Андрей Викторович Давидюк, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.
Игорь Михайлович Куликовский, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Ihor Yakoviv, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.
Andrii Davydiuk, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.
Ihor Kulykivskyi, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

УДК 621.391:004.056.53 (045)

ПЕТРО ПАВЛЕНКО,
МИКОЛА ВІНОГРАДОВ,
СЕРГІЙ ГНАТЮК,
АНДРІЙ ГІЗУН,
ВІКТОР ГНАТЮК

МЕТОД ФОРМУВАННЯ ПРАВИЛ ЕКСТРАПОЛЯЦІЇ ІНЦИДЕНТІВ ДЛЯ МЕРЕЖЕВО-ЦЕНТРИЧНОГО МОНІТОРИНГУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Інциденти можуть порушити штатний режим функціонування інформаційно-телекомунікаційної системи і призвести до значних матеріальних та іміджевих збитків підприємства. Одним із підходів до інцидент-менеджменту є застосування мережево-центричної теорії управління для моніторингу інцидентів, проте не достатньо формалізованим є етап формування множини базових правил. З огляду на це, у цій роботі розроблено метод формування множини правил екстраполяції інцидентів для мережево-центричного моніторингу інформаційно-телекомунікаційних систем, який за рахунок