***Список використаних джерел***

1. Міжнародний стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity): [Електроний ресурс]. – Режим доступа: https://webstore.iec.ch/preview/info_isoiec27032 %7 Bed1.0 %7Den.pdf.
2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – С. 10.
3. Правовий захист інформації: навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса: Фенікс, 2015. – С. 32- 44.
4. Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України: Проект Закону України від 06.03.2013 р.: [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/1_doc2.nsf/link1/JG1WZ00I.html. – Назва з екрану.
5. Стратегія кібербезпеки України: Затверджено Указом Президента України від 15.03.2016 р. № 96/2016 // Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.

***КОЗІН О. Б.***

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат фізико-математичних наук, доцент

## МЕХАНІЗМИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ В МЕРЕЖІ ІНТЕРНЕТ

Сьогоднішній день можна охарактеризувати постійним збільшенням ролі цифрової інформації у нашому житті. Кількість цієї інформації швидко зростає, її значення також відповідно зростає і збільшується необхідність її захисту. З розвитком Інтернету все більшої актуальності набуває проблема порушення авторських прав в Мережі. Дедалі актуальнішою проблемою постає забезпечення цілісності цифрової інформації, її захист та розробка механізмів, за допомогою яких можна захистити порушені права її авторів або її власників.

Через поганий захист та неприйняття запобіжних заходів, автори творів не можуть відслідкувати порушника та покарати його.

Відомо певне коло технічних механізмів захисту прав авторів цифрових даних, які використовують у світі. Технічні засоби захисту авторських прав цифрових даних можна розподілити на засоби обмеження доступу к цім даним, засоби їх ідентифікації, засоби криптографічних перетворень та інші. Деякі з засобів ідентифікації ми розглянемо окремо.

Міжнародні засоби ідентифікації об'єктів цифрової інтелектуальної власності це цифрові водяні знаки (Digital watermark), цифрові марки, ідентифікаційні коди ISBN, ISAN та інші.

Також існують ще різні спеціальні програмні коди, які дозволяють не тільки простежити рух твору, а також порушити цілісність твору, якщо його використовують не так, як регламентує замовник.

Одна з найпоширеніших систем захисту — є система «цифрових водяних знаків», яки широко застосовуються в Інтернет у творах (зображеннях, текстах і т. д.). Якщо користувач розглядає цифровий твір за допомогою екрану монітора, то він може не бачити різниці між кодованим і некодованим зображенням. Кодовані позначення — рік видання, значок копірайту, прізвище власника, його логотип. Також цифрові знаки можуть містити іншу інформацію, котра допомагає встановити авторські права на даний цифровий контент. При використані спеціального програмного засобу можна зрозуміти та довести, що файли містять певну інформацію, яка вказує на особу, що її написала.

Найчастіше невидимі цифрові знаки уводять у цифрові твори для захисту в Інтернеті проти тиражування в системах цифрових фотографій паспортів, посвідчень, кредитних карт тощо. Ще один зразок прихованих цифрових водяних знаків — пояснення до цифрових фото з додатковими відомостями. Деякі формати цифрових даних несуть у собі допоміжні відомості (метадані), але цифрові знаки відрізняються від них тим, що ця інформація закодована прямо у самому сигналі. Невидимі знаки аналізуються спеціальним декодером, він і виносить рішення про їх коректність.

Усі засоби, які захищають авторські права методом вбудовуванням цифрових водяних знаків, можна умовно розбити на два класи. Засоби, які маскують інформацію в частотної області та засоби, які маскують інформацію в просторовій області самого зображення. Засоби другого класу вбудовують інформацію в первинну область даних. Це робить їх нестійкими до різних перетворень, особливо до стиснення з втратами (наприклад JPEG-стиснення). Також це може призвести до знищення вбудованого цифрового знаку. Більш стійкими до спотворень являються засоби першого класу. Найвідомішими засобами першого класу є засоби, які базуються на дискретному косинусу перетворенні, дискретному перетворенні Фур'є, перетвореннях Хаара, Добеші та інших [1, с. 3].

Вдосконалення процесу організації прихованого каналу зв'язку привело до появи і розвитку методів організації прихованого каналу зв'язку з одночасною перевіркою автентичності та цілісності інформації [2, с. 1]. Розроблені методи забезпечують можливість ефективної автентифікації та декодування додаткової інформації як при наявності контейнера, так і без нього.

З метою фіксації авторських прав для графічних зображень потрібно вдосконалювати методи першого класу та вбудовувати, як видиме

так і приховане підписування файлів. Такі «посилання» будуть служити безперечним доказом правовласника. Крім того вони можуть вказувати на походження незаконного копіювання. Ці методи будуть достатньо ефективною мірою для захисту прав інтелектуальної власності. Ці посилання можуть по різному розташовуватись у файлі, кодуватись і служити захистом проти кримінальних злочинів, наприклад, таких як підміна власника, або відмова від авторських прав, та інших.

Аналізуючи досвід зарубіжних країн, ми можемо також вдосконалити вже існуючи законодавчі норми та створити власні методи захисту ринка цифрової власності. Наприклад, це будуть центри, які займаються отриманням ліцензій для використання цифрових творів. Вони визначають що і кому належить, тобто фіксують об'єкти інтелектуальної власності. Вони матимуть дозвіл авторів (власників) на обмін, продаж або інші операції з цими об'єктами. Вони також, з дозволу і автора і держави, будуть здійснювати різноманітні операції з цифровою інформацією на міждержавному рівні.

Стрімкий розвиток Інтернету та масові порушення авторських прав цифрових даних в Інтернеті значно ускладнює захист авторського права в Мережі. Розвиток нових технічних засобів вимагає їх удосконалення, та поєднання з правовою базою, тобто їх легалізації на державному рівні. Далі повинна бути міжнародна співпраця і, як наслідок, транскордонне визнання законності цих механізмів. Це буде один із ефективних шляхів захисту авторського права в мережі Інтернет. Він буде поєднувати права нових технічних засобів захисту, і дійсно дасть надійних захист цифрової інтелектуальної власності у світі.

### *Список використаних джерел*


1. Козин А. Б. Использование информационніх технологий для защиті авторського права. / Козин А. Б., Козина М. А. // Сборник научных трудов SWorld. – 2013. – Том 7. – Выпуск 4. – С. 85- 87.
2. Kozina M. O. Discrete Fourier transform as a basis for steganography method / M. O. Kozina – Праці Одеського політехнічного університету. – 2014. – Вип.2(44). – С. 118- 126.