

ЗМІСТ**ТЕХНІЧНІ НАУКИ****Федухин А.В., Муха А.А.**Прогнозирование остаточного ресурса
опор контактной сети железных дорог.....73**ВІЙСЬКОВІ НАУКИ****Турчин В.М., Бондаренко С.В., Павленко А.М.**Деякі аспекти підготовки офіцерів запасу
в Національній академії
Національної гвардії України.....78**ФІЛОСОФСЬКІ НАУКИ****Ярмоліцька Н.В., Москальчук М.М.**Історико-філософські та соціально-політичні
дослідження в Київській світоглядно-
гносеологічній школі в період
радянської доби (60–90 рр. ХХ ст.)..... 83**ПЕДАГОГІЧНІ НАУКИ****Онопрієнко О.М., Онопрієнко О.В.**Педагогічні засоби
патріотичного виховання студентів.....91**Павліщева Я.О.**Засоби ефективного розвитку комунікативних
навичок на заняттях з іноземної мови.....94**Порядченко Л.А., Телегуз А.О.**Організаційно-методичні основи формування
читацької компетентності учнів 3 класу
засобами доповненої реальності.....100**Shevchenko Maryna**Interactive debate club techniques during distance
learning with physical education students.....106**ФІЛОЛОГІЧНІ НАУКИ****Карпіна О.С., Молька Н.Е.**Драма Б. Шоу «Свята Іоанна» як художнє
втілення концепції «нової жінки»..... 110**Левченко В.М., Перхач Р.-Ю.Т.**Медична термінологія як об'єкт
лінгвістичного дослідження.....115**ІСТОРИЧНІ НАУКИ****Бондарчук М.О.**Криміногенна ситуація в Україні
в період НЕПу.....119**Пуйда Р.Б.**Атеїзм в Українській РСР
у другій половині 1960-х –
першій половині 80-х роках ХХ ст.:
теорія, пропаганда, протидія
(на прикладі Івано-Франківської області).....128**ПОЛІТИЧНІ НАУКИ****Дяків В.Б.**Перехід від централізованої
до децентралізованої держави
в контексті загальноєвропейських
політичних тенденцій: на прикладі
Великобританії, Німеччини та Франції.....133**ДЕРЖАВНЕ УПРАВЛІННЯ****Пак Н.Т., Воронець Є.С.**Громадський контроль діяльності
органів публічної влади:
сутність та механізми здійснення..... 138**ЮРИДИЧНІ НАУКИ****Гриньчак В.М., Ткаченко В.П.**Порушення прав на об'єкти
інтелектуальної власності
у глобальній мережі інтернет.....143**Улибіна Л.Ю., Гарбуз М.В.**Особливості класифікації
декоративної косметики для губ
при проведенні судової
товарознавчої експертизи148**ЕКОНОМІЧНІ НАУКИ****Литвиненко І.С.**Аналіз теоретичних підходів до визначення
поняття «діджитал економіка».....152**Пугачевська К.Й., Лисенко Е.Р.**Адаптивне управління підприємством
в умовах невизначеності.....158

CONTENTS

ENGINEERING SCIENCES

- Fedukhin Alexandr, Mukha Artem**
Prediction of the residual life
of railroad catenary poles.....73

MILITARY SCIENCES

- Turchin Vladimir, Bondarenko Sergey,
Pavlenko Anatoliy**
Some aspects of training reserve officers
in the National Academy
of the National Guard of Ukraine.....78

PHILOSOPHICAL SCIENCES

- Yarmolitska Nataliia, Moskalchuk Maryna**
The history-philosophical
and social-political researches
in Kyiv worldview-epistemology school
in period during the Soviet era (60–90's XX).....83

PEDAGOGICAL SCIENCES

- Onoprienko Olga, Onoprienko Alexander**
Pedagogical means
of patriotic education of students.....91
- Pavlishcheva Yana**
The means of communicative skills
development at foreign language classes.....94
- Poriadchenko Lesya, Telehuz Anastasiia**
Organizational and methodological
fundamentals of formation
of reading competence of 3th grade students
by means of activated reality.....100
- Shevchenko Maryna**
Interactive debate club
techniques during distance learning
with physical education students.....106

PHILOLOGICAL SCIENCES

- Karpina Olena, Molka Natalia**
B. Shaw's drama «Saint Joan» as an artistic
embodiment of the concept of «new woman».....110

- Levchenko Vita, Perhach Roksolana-Justina**
Medical terminology as an object
of linguistic research.....115

HISTORICAL SCIENCES

- Bondarchuk Mykola**
The criminal situation
in Ukraine during the NEP.....119

- Puyda Roman**
Atheism in the Ukrainian SSR
in the second half of the 1960s – first half
of the 1980s: theory, propaganda, counterfeit
(on the example of Ivano-Frankivsk region).....128

POLITICAL SCIENCES

- Diakiv Vitalii**
Transition from a centralized to a decentralized
state in the context of pan-European political
trends: examples from the United Kingdom,
Germany and France.....133

STATE ADMINISTRATION

- Pak Natalia, Voronets Elizaveta**
Public control of activities of public authorities:
essence and mechanisms of implementation.....138

LAW SCIENCES

- Grynychak Valentyna, Tkachenko Valentyna**
Violation of intellectual property rights
on the global internet.....143
- Ulybina Lionella, Harbuz Mariia**
Features of classification
decorative cosmetics for lips
when carrying out ship product expertise.....148

ECONOMIC SCIENCES

- Lytvynenko Inna**
Analysis of theoretical approaches
to the definition of «digital economy».....152
- Pugachevska Kateryna, Lysenko Erika**
Adaptive management of the enterprise
in the conditions of uncertainty.....158

ЮРИДИЧНІ НАУКИ

DOI: <https://doi.org/10.32839/2304-5809/2021-9-97-29>

УДК 004.63

Гриньчак В.М., Ткаченко В.П.Одеський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

ПОРУШЕННЯ ПРАВ НА ОБ'ЄКТИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У ГЛОБАЛЬНІЙ МЕРЕЖІ ІНТЕРНЕТ

Анотація. Досліджено проблематику порушення захисту прав споживачів у вигляді збільшення продажу контрафактних товарів через інтернет-магазини в період карантинних обмежень пов'язаних вірусом COVID 19. Проаналізовано негативний вплив анонімного придбання доменних імен на хостингах, анонімні продажі на онлайн торговельних майданчиках. Розглянуто незаконне використання торговельних марок в межах українського законодавства. Врахування людського фактору при здійсненні онлайн-покупки, а саме неухважність споживачів при виборі сайтів, що мають схожість з сайтами оригінальних брендів назвою доменного імені, оформленням сторінок та товарів. Розглянуто основні різновиди кіберзлочинів у глобальній мережі Інтернет у сфері права інтелектуальної власності такі як онлайн-шахрайство, інтернет-фішинг, піратство, пропозиція, реклама та продаж контрафактної продукції.

Ключові слова: право інтелектуальної власності, контрафакт, інтернет шахрайство, інтернет-фішинг, кіберсквоттинг.

Grynchak Valentyna, Tkachenko ValentynaOdesa Scientific Research Forensic Center
of the Ministry of Internal Affairs of Ukraine

VIOLATION OF INTELLECTUAL PROPERTY RIGHTS ON THE GLOBAL INTERNET

Summary. The World Wide Web has more than 4.5 billion users, which means that more than 60% of the world's population using Internet. Intellectual property rights are important for the functioning of the Internet. The entire global network system also based on those rights. IT technologies allow the widespread use of intellectual property in the Internet environment, works, drawings that fill the content of Internet resources, computer programs – almost all the intellectual achievements and ideas which transmitted by the human brain. Therefore, it is impossible to operate on the Internet without solving the problems of protection of the intellectual property rights. The criminal elements sphere of interests is widely spreading on the technology of "mobile tracking", which allows monitoring the activities of any enterprises, organizations, institutions and individuals, interception of telecommunications traffic, hacker attacks. Another very attractive "piece of the cake" for the cybercrimes is online shopping and social networks. Growth of: Internet phishing, online fraud, piracy, an increase in the number of counterfeit products through the illegal use of trademarks, appellations of origin and logotypes has reflected on the consumers market. Scammers making the fake official websites for sales, owners of intellectual property rights suffer significant economic losses and reputational losses, consumers trying to buy questionable stuff from an unlicensed seller and do not receive the promised quality level, service and support. Identification by unique address and domain name system is the main characteristic of the logical level of the Internet. Acquisition of a domain name for the purpose of its dishonest use or in order to prevent its conscientious use by another person is called a term – cybersquatting. A domain name has the value, it is a company asset and also can be bought or sold. Seizure of a domain for the purpose of selling or preventing its use may be an offence of intellectual property rights or other means of individualization, unfair competition that causes harm. Most Internet users see only the top level of the Internet and the content level, which includes content transmitted over the network, web pages, mp3 files, e-mails, streaming videos, and applications that work on or submit to the network. The main characteristic of this level is the active participation of Internet users in creating content. The growing of the Internet has led to an unprecedented increase of questions how to protect intellectual property rights on the Internet. Anonymity is one of the features of the Internet that provides an unmanaged infrastructure through websites, e-mails, chat rooms, encryption tools, anonymous servers, etc. that support anonymity. General question about location of criminals is the main issue to establish the identity of the offender.

Keywords: intellectual property law, counterfeiting, Internet phishing, online fraud, cybersquatting.

Постановка проблеми. Права інтелектуальної власності мають вагомe значення для функціонування Інтернету. Вся глобальна система мереж базується зокрема і на цих правах. ІТ-технології (особливо розвиток цифрового простору) дозволяють широко використовувати інтелектуальну власність в Інтернет-середовищі, твори, малюнки, які наповнюють зміст Ін-

тернет-ресурсів, комп'ютерні програми – майже всі інтелектуальні здобутки та ідеї, що транслює людський мозок. Таким чином, неможливо діяти в Інтернеті без розв'язання проблем захисту прав на об'єкти інтелектуальної власності.

Огляд останніх досліджень і публікацій. Сьогодні ми не можемо уявити життя без Інтернету, оскільки ми не можемо уявити життя без Інтернету, оскільки ми не можемо уявити життя без Інтернету, оскільки ми не можемо уявити життя без Інтернету, оскільки ми не можемо уявити життя без Інтернету.

ють такі важливі інфраструктури, як охорона здоров'я та освіта, енергетика, транспорт, банківська справа та фінанси. Дійсно, наразі глобальна мережа Інтернету налічує понад 4,5 млрд користувачів, що означає, що понад 60% населення світу має підключення до Інтернету. Ця цифра продовжує зростати щороку.

Відомо, що інтелектуальна діяльність, інтелектуальний продукт, а також їх види розкриваються в якості двох категорій:

1) ринок інтелектуальних прав дозволяє його учасникам видобувати більші доходи, його можна розглядати як економічну категорію;

2) юридичну категорію, коли власник об'єктів інтелектуальної власності має право використовувати, розпоряджатися, передавати права на них іншим особам для використання, шляхом укладення договору-поступки, продавати права, забороняти третім особам здійснювати такі ж дії без його (власника прав) згоди.

Законодавчо визначені об'єкти інтелектуальної власності ст. 420 Цивільного кодексу України, перелік яких включає: «літературні та художні твори; комп'ютерні програми; компіляції даних (бази даних); виконання; фонограми, відеограми, передачі (програми) організацій мовлення; наукові відкриття; винаходи, корисні моделі, промислові зразки; компонування (топографії) інтегральних мікросхем; раціоналізаторські пропозиції; сорти рослин, породи тварин; комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення; комерційні таємниці» [1].

У сфері інтересів кримінальних елементів виступає технологія «мобільний трекінг», що дозволяє здійснювати стеження за діяльністю будь-яких підприємств, організацій, установ і окремих осіб, перехоплення телекомунікаційного трафіку, хакерські атаки. Цифрові засоби в теперішній час стали провідними у веденні промислового шпигунства. І це не надумана проблема – шкода, яку завдають промисловим шпигунством державі, юридичним і приватним особам може бути колосальною.

Ще одним дуже привабливим шматком у сфері кіберзлочинів є онлайн-шопінг та соціальні мережі.

З досліджень GWI (GlobalWebIndex), приблизно три чверті інтернет-користувачів у віці від 16 до 64 років щомісячно купують щось онлайн. В Україні покупки онлайн за останній рік здійснили понад 60% користувачів Інтернету.

Більша частина респондентів GWI (53%) у віці від 16 до 64 років заявили, що коли вони шукають інформацію про бренди, продукти та послуги, вони в першій черзі звертаються до пошукових систем. Пошук у соціальних мережах використовують близько 43%, здебільшого це користувачі від 16 до 24 років.

Потужним поштовхом до цього стали вірус COVID-19 та пандемія, яку він спричинив. Навіть той, хто звик купувати у реальних магазинах, отримувати інформацію з офіційних ресурсів, був вимушений почати користуватись онлайн-ресурсами.

На споживчому ринку це відобразилось у вигляді:

– зростання: інтернет-фішингу, це фішингові (підроблені) сторінки створені шахраями, які

копіюють офіційні сторінки інтернет-магазинів, виробників, підприємств, банків, платіжних сервісів, і т. д.;

– онлайн-шахрайства – фальшиві інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

– піратства – протиправне поширення об'єктів інтелектуальної власності в Інтернеті;

– збільшенням кількості контрафактної продукції шляхом незаконного використання товарних знаків, найменування місця походження товарів та фірмових знаків.

Виділення невирішених раніше частин загальної проблеми. У власників інтернет-магазинів є переваги завдяки відкритому Інтернет-простору, чим вони можуть зловживати у сфері дотримання вимог щодо захисту прав споживачів продаючи контрафактні товари. Такі порушення трапляються частіше, коли в Україні є ідентичні товари які вже продає офіційний дистриб'ютор або виробник, товари з нанесеними позначеннями тотожними або схожими з зареєстрованими торговельними марками які продає всесвітня мережа Інтернет.

Шахраї копіюють офіційні сторінки у мережі Інтернет з продажу товару та намагаються видати себе в очах споживача за представника або партнера компанії-виробника, використовуючи репутацію бренду на свою користь.

Мета статті. Головною метою цієї роботи є висвітлення проблематики порушення захисту прав споживачів у вигляді збільшення продажу контрафактних товарів через інтернет-магазини, незаконного використання об'єктів інтелектуальної власності в межах українського законодавства та здійснення кіберзлочинів у глобальній мережі Інтернет. Пошук рішення для унеможливлення шахрайських дій порушників, копіювання оригінальних веб-сторінок або їх крадіжок.

Виклад основного матеріалу. Власники прав на об'єкти інтелектуальної власності несуть значні економічні збитки, а також мають місце репутаційні втрати. Пересічні споживачі також страждають, купуючи товар сумнівної якості у неліцензованого продавця та не отримують обіцяний рівень сервісу, обслуговування та підтримки.

Саме використання торговельної марки без дозволу власника є порушенням прав на торговельну марку. Наприклад, позначення нанесене на товар, розміщений на сайті в інтернет-магазині, логотип саме онлайн-магазин, названа доменного імені тощо, тотожні з зареєстрованою торговельною маркою або відрізняються від неї лише окремими елементами. Саме перше зорове сприйняття будь-якого об'єкту впливає на свідомість людини. Відповідним чином у свідомості споживача запам'ятовується і позначення, яке використовується як торговельна марка. Згідно з пунктом 27 статті 1 Закону України «Про захист прав споживачів» до фальсифікованої продукції належить продукція, «...виготовлена з порушенням технології або неправомірним використанням знаку для товарів та послуг, чи копіювання форми, пакування, зовнішнього оформлення, а так само неправомірним відтворенням товару іншої особи. До того ж у пункті 4 статті 6 Розділу II зазначеного Закону зазначається, що «забороняється введення в обіг фальсифікованої продукції» [4].

Згідно з тлумачним словником сучасної української мови [3]:

– «ФАЛЬСИФІКАТ, у, чол. Підроблена річ, яку видають за справжню; підробка».

– «РІЧ 1, речі, жін. 1. Предмет, перев. домашнього вжитку, трудової діяльності і т. ін. // Будь-який предмет взагалі».

– ТОВАР 1, у, чол. 1. тільки одн., ек. Признач. для обміну продуктом праці, що має споживну вартість... 2. Все те, що становить предмет торгівлі. «веб-сайт, -у, чол. Сукупність взаємопов'язаних посиланнями та змістом веб-сторінок, опублікованих та підтримуваних певною особою, групою осіб чи організацією з метою поширення чи обміну інформацією; сайт».

– ПРОДУКЦІЯ, і, жін. Сукупність продуктів, що випускаються окремим підприємством, певною галуззю промисловості, сільського господарства або всім народним господарством країни.

Відповідно до Закону України «Про охорону прав на знаки для товарів і послуг» [2] порушення прав власника свідоцтва. 1. Будь-яке посягання на права власника свідоцтва, передбачені статтею 16 цього Закону, в тому числі вчинення без згоди власника свідоцтва дій, що потребують його згоди, та готування до вчинення таких дій, вважається порушенням прав власника свідоцтва, що тягне за собою відповідальність згідно з чинним законодавством України: використання без згоди власника торговельних марок в доменних іменах є порушенням прав власника свідоцтва, вказаних у пункті 5 статті 16 цього Закону. На вимогу власника торговельної марки використання повинно бути припинено, а порушник має відшкодувати власнику торговельної марки заповдіні збитки. Власник торговельної марки як правило вимагає усунення з товару використане зображення торговельної марки, схоже з нею настільки, що їх можна сплутати.

Останнім часом спостерігається ріст фальсифікованої та контрафактної продукції, багато експертів вважають, що може збільшитися кількість неякісної продукції медичного призначення, в тому числі й неефективні фальсифікати вакцини проти COVID-19. Можна припустити, що злочинці не тільки будуть вкладати значні кошти в їх створення, а й поширювати пропозиції на їх придбання з використанням цифрових технологій (Інтернет, різні онлайн-платформи, соціальні мережі).

У зв'язку з економічними проблемами у населення можливе підвищення попиту на контрафактні товари, що буде впливати на розширення тіньових ринків, розвиток яких спричинить зростання злочинів у сфері недобросовісної конкуренції та незаконного використання інтелектуальної власності. Адже споживач щиро вірить у можливі акції та знижки на оригінальну продукцію, яка по факту є контрафактною.

Інтернет умовно можна поділити на три рівні: фізичний, логічний та інформаційного наповнення.

Фізичний рівень Інтернету з'єднаний з логічним шаром Інтернету, щоб дозволити користувачам спілкуватися або отримувати доступ до послуг.

Логічний рівень Інтернету складається з набору протоколів, таких як Інтернет-протокол (IP) та Протокол управління передачею (TCP), які

обробляють такі речі, як IP-адреси та операції з портами, обмінюючись інформацією з фізичним протоколом та додатком. Зокрема, що стосується комп'ютерів, розташування веб-сайту визначається IP-адресою, яка містить унікальний 32-рядковий номер, розділений крапками, наприклад, 255.255.100.1. Використовуючи ці номери, один комп'ютер може зв'язатися та спілкуватися з будь-яким іншим комп'ютером в Інтернеті та обмінюватися даними. Але, попри те, що Інтернет має «адреси», ці IP-адреси не розкривають географічне розташування користувача, а лише знаходять розташування машини в мережі.

Також логічний рівень Інтернету забезпечує управління та функціонування системи доменних імен. Щоб потрапити на певний веб-сайт, користувач покладається на доменне ім'я, яке представляє буквено-цифрову мітку, що відповідає IP-адресі (і навпаки). Доменні імена є ієрархічними. Вони включають "доменне ім'я верхнього рівня", яке може бути загальним (наприклад, *.com, *.org, *.net, *.int або *.edu) або конкретним для країни (так звані доменні імена з кодом країни, наприклад, *.fr або *.lt) та доменне ім'я другого рівня (наприклад, whatis, кока-кола). На кожному рівні дерева так званий сервер працює для ведення таблиці всіх імен, зареєстрованих під цим рівнем, і для направлення всіх запитів до сервера імен, зареєстрованого для цього імені.

Загальна група доменів верхнього рівня (gTLD) є відкритою групою (у якій компанії чи приватні особи можуть подати заявку до Network Solutions, Inc. (NSI), яка може зареєструвати доменні імена в цих gTLD домен верхнього рівня з кодом країни (ccTLD). Доменне ім'я країни не обов'язково вказує на те, що правласники цього імені знаходяться в цій країні. Дійсно, багато реєстрів пропонують доменне ім'я верхнього рівня з кодом країни для нерезидентів.

Важливо відзначити, що Радою Інтернет-корпорації з присвоєння імен та номерів (ICANN) ще у 2015 році схвалено одну з найбільших змін у загальній системі імен загальних доменів верхнього рівня, яка дозволила будь-кому по всьому світу зареєструвати домени верхнього рівня в будь-якою мовою або письмом [5]. Наприклад, можна зареєструвати gTLD, які можуть містити такі адреси, як *.google, .coke або навіть *.BBC, або зареєструвати бренди на другому рівні нових gTLD, зареєстрованих іншими (тобто Diet.Coke, відео. MTV).

Крім того, попри те, що компанія з управління кодом країни верхнього рівня несе відповідальність за збереження точності даних, що містяться в базі даних, така компанія не несе юридичної відповідальності за будь-яке можливе порушення третіх сторін право на об'єкти інтелектуальної власності.

Придбання доменного імені з метою його несумлінного використання або з метою не допустити його сумлінного використання іншою особою іменується терміном – кіберсквоттинг. Доменне ім'я є об'єктом купівлі-продажу, і вартість його залежить від різних факторів.

З розвитком так званого «е-бізнесу», у другій половині 1990-х років доменні імена дали істотну надбавку числа клієнтів які впливають на її вартість. Отже, доменне ім'я має вартість, є активом компанії, може купуватися і продаватися. Оціночна вартість найпопулярніших доменних

імен досягає десятків мільйонів доларів. Природно, в таких умовах з'являються охочі заробити на перепродажі доменних імен – кіберсквоттери.

Захоплення домену з метою продажу або перешкоджання його використання може бути порушенням прав на об'єкти інтелектуальної власності чи інший засіб індивідуалізації, недобросовісною конкуренцією, що завдає шкоди.

Ідентифікація за однозначною адресою та системою доменних імен є основною характеристикою логічного рівня Інтернету.

Третій рівень Інтернету – це рівень інформаційного наповнення. Більшість користувачів Інтернету бачать лише верхній рівень, який представляє матеріали, що передаються мережею, веб-сторінки, mp3-файли, електронну пошту, потокове відео, а також прикладні програми, які працюють у мережі або подають її.

Рівень інформаційного наповнення Інтернету – це фактична інформація, доступна програмам, які залежать від логічного рівня, оскільки використовує фізичну мережу для перенесення вмісту від провайдерів до користувачів.

Немає явних суттєвих бар'єрів для входу, і існує незліченна кількість постачальників Інтернет-контенту. Це означає, що будь-який користувач, який володіє комп'ютером та має підключення до Інтернету, може розмішувати на веб-сайті будь-який контент, включаючи вміст, що порушує право інтелектуальної власності. Дійсно, Інтернет є найважливішим носієм для поширення інформації та обміну інформацією. За даними опитування веб-серверів, зараз в Інтернеті доступно понад 883 мільйонів веб-сайтів. Веб-сторінку можна визначити як систему об'єднання сотень мільйонів електронних документів (веб-сторінок) на мільйонах комп'ютерів (веб-сайтів) в Інтернеті, кожен з яких доступний за допомогою унікальної, але змінної назви або Уніфікований локатор ресурсів (URL). Таким чином, веб-сайт – це просто сукупність веб-сторінок, що містять текст, графіку, зображення чи звуки, і створюється за допомогою комп'ютерної мови, яка називається мовою розмітки гіпертексту (HTML). Коли веб-сервер отримує запит з Інтернету, він повертає дані веб-сторінки у файлі на комп'ютер, який здійснює запит.

Випадки корисливої мотивації, мабуть, вичерпуються отриманням доходу від реклами, яка розміщена на веб-сайті, що містить популярний, але контрафактний контент (так званий «варез»). Веб-мастер зазвичай отримує дохід зі свого веб-сайта через розміщення на ньому реклами. Дохід тим більше чим вище відвідуваність ресурсу. Розмістити на сайті популярний «варез» – вірний шлях швидко підняти відвідуваність.

При відстеженні правопорушень такого напрямку утворюються такі сліди технічного характеру:

- записи в лог-файлах веб- або FTP-сервера при записі файлів на сервер (upload);
- записи в лог-файлах веб- або FTP-сервера при отриманні файлів споживачами – свідчить про інтерактивну доступність файлів іншим особам;
- сліди на комп'ютері, з якого підозрюваний записував файли на загальнодоступний сервер, локальні копії цих файлів;
- архіви і лог-файли повідомлень електронної пошти та ICQ, в яких підозрюваний повідомляв

іншим користувачам про доступність файлів за певним мережевою адресою.

Крім того, підозрюваний може мати договір з оператором зв'язку, на ресурсі якого проводилося розміщення об'єкту інтелектуальної власності.

Поява Інтернету призвела до безпрецедентного зростання кількості питань про те, як захистити права інтелектуальної власності в Інтернеті. Безперечно, що для запобігання порушенню прав інтелектуальної власності через Інтернет потрібні деякі форми контролю розповсюдження інформації.

Контент-інфраструктурою Інтернету «керують» постачальники послуг Інтернету, відповідальні за доступ до Інтернету, надаючи адреси електронної пошти, а також розмішуючи інформацію, яку користувачі вирішують публікувати в Інтернеті за допомогою так званих послуг розміщення веб-сайтів. Основною характеристикою інформаційного наповнення Інтернету є активна участь користувачів Інтернету у створенні контенту.

Висновки та пропозиції. Питання про місцезнаходження є центральним для з'ясування особи порушника. Багато повідомлень через Інтернет є анонімними, і неможливо з абсолютною впевненістю перевірити особу порушника. Поширеним варіантом анонімності є псевдонім, коли порушник бере участь у спілкуванні під вигаданим ім'ям або кількома вигаданими іменами. Анонімність – одна з характеристик Інтернету, яка забезпечує некеровану інфраструктуру через веб-сайти, електронну пошту, кімнати чату, FTP-сайти, групи новин Usenet, засоби шифрування, повторну розсилку та анонімні сервери, які підтримують анонімність.

Анонімність в Інтернеті не є абсолютним правом, і обмеження щодо використання анонімності можуть бути введені з метою захисту інших основних прав. Зокрема, це очевидно у випадку порушення прав інтелектуальної власності через Інтернет, де анонімні IP-адреси порушників не можуть бути захищені конфіденційністю. Тому провайдер може зіставити відповідну адресу комп'ютера, що використовується в мережі, з унікальним абонентом Інтернету. Знаючи адресу протоколу Інтернету та дату та час підключення, провайдери можуть ідентифікувати підключений комп'ютер, після чого можна зіставити його з обліковим записом користувача Інтернету та його/її фізичною адресою.

Одним із варіантів вирішення питання зменшення кількості порушень використання прав на об'єкти інтелектуальної власності в мережі Інтернет є законодавче посилення відповідальності власників хостингів та веб-серверів за недопущення оренди веб-простору анонімними особами, це зумовило б розмішування інформації на договірних умовах з фізичними та юридичними особами, виключаючи анонімність.

Особливу увагу необхідно приділити розробці та реалізації заходів організаційного, нормативно-правового та методичного характеру для забезпечення інформаційної безпеки. У їх число: відповідна підготовка спеціалістів, технічна забезпеченість правоохоронних органів новітніми технологіями цифрового світу, розробка методичних рекомендацій щодо протидії сучасним викликам злочинності.

І на кінець треба зазначити про необхідність координації діяльності всіх зацікавлених суб'єктів попереджувальної діяльності за охороною інтелектуальної власності, суспільних організацій правоохоронного напрямку. Велике значення має взаємодія з міжнародними організаціями, адже використання інтелектуальної власності у цифровому форматі, в тому числі

протиправне, не дозволяє вирішувати проблеми, що впливають на такі порушення тільки в межах однієї держави через їх транскордонний характер.

Маємо надію, що рівень безпеки в інтернет-просторі України незабаром значно підвищиться, а популярні шахрайські схеми в мережі будуть зведені нанівець.

Список літератури:

1. Цивільний кодекс України : Закон України станом на 14 жовтня 2008 р. URL: <http://zakon2.rada.gov.ua/laws/show/435-15> (дата звернення: 26.08.2021).
2. Про охорону прав на знаки для товарів і послуг : Закон України від 15 грудня 1993 р. № 3689-XII / Верховна Рада України. URL: <http://zakon2.rada.gov.ua/laws/show/3689-12> (дата звернення: 26.08.2021).
3. Словник української мови (Академічний тлумачний словник 1970–1980) : в 11 томах. URL: <http://sum.in.ua> (дата звернення: 26.08.2021).
4. Про захист прав споживачів : Закон України від 12.05.1991 № 1023-XII, із змінами. URL: <https://zakon.rada.gov.ua/go/1023-12> (дата звернення: 26.08.2021).
5. Uniform Domain Name Dispute Resolution Policy. URL: <https://www.icann.org/resources/pages/policy-2012-02-25-en> (дата звернення: 26.08.2021).
6. GlobalWebIndex. URL: <https://www.gwi.com/> (дата звернення: 26.08.2021).
7. CloudFlare. What is a DDoS Attack? 2018. URL: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> (дата звернення: 26.08.2021).
8. Maras, Marie-Helen. Computer Forensics: Cybercriminals, Laws and Evidence, second edition. Jones and Bartlett. 2014. 413 p.
9. Maras, Marie-Helen. Cybercriminology. Oxford University Press, 2016. 448 p.

References:

1. Tsyvil'nyy kodeks Ukrayiny [The Civil Code of Ukraine]. Available at: <http://zakon2.rada.gov.ua/laws/show/435-15> (accessed 26 August 2021).
2. Law of Ukraine «Pro okhoronu prav na znaky dlya tovariv i posluh» [Law of Ukraine «About protection of the rights to marks for the goods and services»]. Available at: <http://zakon2.rada.gov.ua/laws/show/3689-12> (accessed 26 August 2021).
3. Slovnyk ukrayins'koyi movy (Akademichnyy tлумachnyy slovnyk 1970–1980): v 11 tomakh [Dictionary of the Ukrainian language (Academic Explanatory Dictionary 1970–1980): in 11 volumes]. Available at: <http://sum.in.ua> (accessed 26 August 2021).
4. Law of Ukraine «Pro zakhyst prav spozhyvachiv» [Law of Ukraine «On consumer protection»]. Available at: <https://zakon.rada.gov.ua/go/1023-12> (accessed 26 August 2021).
5. Uniform Domain Name Dispute Resolution Policy. Available at: <https://www.icann.org/resources/pages/policy-2012-02-25-en> (accessed 26 August 2021).
6. GlobalWebIndex. Available at: <https://www.gwi.com/> (accessed 26 August 2021).
7. CloudFlare (2018) What is a DDoS Attack? Available at: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> (accessed 26 August 2021).
8. Maras, Marie-Helen (2014) Computer Forensics: Cybercriminals, Laws and Evidence, second edition. Jones and Bartlett, 413 p.
9. Maras, Marie-Helen (2016) Cybercriminology. Oxford University Press, 448 p.