доказів. При розгляді справи в Комісії США з міжнародної торгівлі сторони мають право на належне повідомлення, перехресний допит, подання доказів, подання заперечень і клопотань, висунення аргументів, а також інші права, які мають суттєве значення для забезпечення справедливого слухання справи.

Не дивлячись на низку прийнятих законів в Україні стосовно захисту авторських прав, все ж таки процес формування інституту інтелектуальної власності пов'язаний з низкою проблем, що позначається на розвитку науково-технологічного потенціалу та стримує становлення нової інноваційної моделі вітчизняної економікикраїн, оскільки закони не забезпечують ефективний правовий захист інтелектуальної власності.

На нашу думку, для вирішення перелічених проблем, слід удосконалити національну систему охорони та захисту прав інтелектуальної власності з урахуванням міжнародно-визнаних норм і принципів, впровадження дієвого механізму реалізації цих норм та запобігання несанкціонованому використанню об'єктів інтелектуальної власності, запровадження державної програми підтримки винахідництва, новаторства та творчої інтелектуальної праці, а також інформаційне забезпечення діяльності у сфері інтелектуальної власності, розвиток патентно-інформаційної бази.

1. Цивільний кодекс України від 16 січня 2003 року № 435-IV // Відомості Верховної Ради України. – 2003. – №№ 40-44. – Ст.356.

2. Про авторське право і суміжні права: Закон України від 23 грудня 1993 року № 3792-XII // Відомості Верховної Ради України. – 1994. – № 13. – Ст.64.

3. Авторське право у США – його закон і захист // [Електронний ресурс]: Режим доступу: http://yurporada.kiev.ua/uk/novini-ta-ch-obgovorennya/avtorskoe-pravo-v-ssha.html.

Мирошниченко Володимир Олексійович
к.т.н., доц., доцент кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

МЕТОДИ БОРОТЬБИ З НЕГАТИВНИМ ЗМІСТОМ У МЕРЕЖІ ІНТЕРНЕТ: МІЖНАРОДНИЙ АСПЕКТ

Сучасний вік – вік інформації. Тепер у першій половині XXI століття роль інформації в житті людини має вирішальне значення: чим більше навичок і знань вона має, тим вище ціниться як фахівець і працівник. Велика кількість даних активно використовується у виробництві, в науковій діяльності, вони є незамінними у прогнозуванні. Так, у США в галузі інформаційної промисловості працює більше 50% всіх працівників і службовців. З часом ці масштаби тільки зростатимуть, як і обсяги створеної інформації. Загалом, за оцінками вчених, кількість інформації в усьому світі подвоюється принаймні раз на два роки.

Такі великі обсяги даних не тільки надають широкі можливості, але також висувають і нові завдання. Зокрема, деяка інформація може бути шкідли-

вою або взагалі небезпечною, відтак необхідно адекватно реагувати на такі виклики.

Можна сміливо стверджувати, що інформаційна небезпека перетворилася на один з найбільш небезпечних видів загроз, що спричинило збільшення важливості сфери інформаційної безпеки. Свідченням цього є постійне обговорення проблем інформаційної безпеки як науковою спільнотою, так і на офіційних зустрічах на найвищому політичному рівні.

У зарубіжній літературі прийнято розподіл негативного змісту на дві категорії: незаконна та шкідлива. Перша – інформація, заборонена законом. Друга – інша суспільно небезпечна інформація, яка не заборонена кримінальним чи адміністративним законодавством, але для якої встановлено певні обмеження щодо її розповсюдження. І якщо з першою категорією все досить чітко та відносно організовано, то щодо другої спостерігаються великі відмінності між країнами та загальна невизначеність.

Інформаційна безпека, в її широкому тлумаченні, розуміється як така, що передбачає захист від негативної інформації аудиторії засобів масової інформації та користувачів комп'ютерних ігор, протидію маніпуляції громадською свідомістю засобами масової інформації та Інтернет-ресурсами, захист користувачів Інтернету від ризиків вмісту та зв'язку, боротьбу з кіберзлочинністю та іншими руйнівними діями в кібер-просторі, протидію інформаційній війні.

Розглядаючи методи боротьби з інформацією з негативним змістом, слід почати з визначення цього терміна. За негативним змістом розуміється інформація, яка шкідливо впливає на свідомість окремої людини та (або) суспільну свідомість або інформацію, поширення якої порушує права або законні інтереси користувачів. Обидва формулювання є надзвичайно розпливчасті, тому на практиці "захист від негативного змісту" розуміється як захист від кількох принципово різних типів інформації.

Найбільшу підтримку в світі має боротьба з дитячою порнографією – остання заборонена у 77% країн – членів ОБСЄ. Наступною є заборона на заклики до насильства – поширення ненависті на етнічну, релігійну, расову відмінність, обґрунтування злочинів проти людяності, заклики до війни та матеріали екстремістських організацій. До цього ж можна віднести інформацію з негативним змістом наклепу, соціально небезпечної реклами, повідомлення про паніку терористичних нападів, а також інформацію, що суперечить поняттю моральних та етичних стандартів конкретних країн. Окремо можна згадати ресурси, які порушують економічні інтереси конкретних країн.

Основним і майже єдиним способом боротьби з негативним вмістом є його блокування. Технічно він може бути реалізований у точці доступу (на комп'ютері користувача), в мережі (на рівні постачальника) та інфраструктурним шляхом (через глобальні служби інфраструктури та безпосередньо через співпрацю з власниками серверів). Що стосується правових та економічних методів боротьби, то вилучення негативного контенту з мережі також може бути досягнуте таким чином:

– повідомлення постачальника послуг і закриття сайту;
– видалення посилання з пошукової системи;
– виключення сайту від контекстної реклами;
– відкликання домену та послуг платіжної платформи.

Боротьба з негативним контентом йде в активній співпраці з провайдерами, постачальниками платіжних і пошукових сервісів, власниками серверів та простими користувачами мережі, які допомагають виявити сайти з негативним змістом.

На даний момент блокування будь-якого вмісту в мережі пов'язано зі значними труднощами. По-перше, немає способу, який гарантує повне блокування ресурсу, а також методів, які не вимагають витрат і не знижують продуктивність мережі. Багато засобів блокування запобігають доступ не лише до вмісту, який необхідно видалити, але й до всього сегменту мережі в цілому, що порушує права інших користувачів мережі і, як наслідок, викликає публічний протест. Це призводить до суттєвого зниження ефективності блокування контенту. Поява і розвиток хмарних технологій взагалі заперечують можливість блокування вмісту контенту – інформація може легко змінити фізичне розташування і, як і раніше, залишиться доступною.

Розробка і впровадження сучасних протоколів передачі інформації призводить до збільшення безпечних з'єднань в Інтернеті, але, як наслідок, також і до проблем з аналізом вмісту контенту. Крім того, можна створити віртуальні приватні мережі, трафік яких передається через зашифроване тунельне з'єднання, що в принципі робить його аналіз неможливим. Поширення цих технологій робить блокування менш ефективним та, до того ж, у даний час заборона доступу найчастіше легко долається технічно компетентним користувачем.

Така тенденція і далі буде продовжуватися і зростати з розширенням і розвитком Інтернету, розробкою хмарних технологій та технологій для безпечної передачі даних.

Проблемою також є те, що Інтернет є глобальним та міжнародним, тому будь-які спроби впливати на його розвиток вимагають міжнародного співробітництва.

У міжнародних актах у галузі прав людини неможливо охопити всі можливі типи негативного змісту, не всі країни, які можуть бути його джерелом, бажають брати участь у їх реалізації, що дає багато можливостей потенційним правопорушникам.

Формулювання, що використовується в міжнародних договорах та законах конкретних країн для опису контролю над Інтернетом, дозволяють подвійну інтерпретацію, що призводить до випадкових або навіть свідомих зловживань. Поняттям "екстремістський вміст" можуть охоплюватися і тексти відомих терористичних асоціацій, таких як "Ісламська держава", і програми конкурентів нинішньої правлячої партії будь-якої авторитарної країни; заклик суворо покарати злочинців може бути прирівняний до "заклику до насильства"; "інформація, шкідлива для благополуччя дитини" може тлумачитися в самих широких межах залежно від визначення "шкоди" та наукових або псевдонаукових джерел, на підставі яких вплив інформації на дітей оцінюється. Організації, що займаються боротьбою зі шкідливими інформаційними явищами, звинувачуються у спробах запровадити цензуру, у порушенні свободи слова та публічного діалогу, у власних політичних інтересах. І слід визнати, не завжди ці обвинувачення є необґрунтованими. З іншого боку, законодавство тоталітарних і просто консервативних режимів майже завжди містить посилання на цензуру інформаційних джерел.

Дуже важко знайти критерії відбору, ефективні, корисні для суспільства, не порушуючи ніяких прав і свобод. У більшості поставлених питань рішення цих проблем ще не знайдені.

Крім того, існують суперечності законодавства різних країн, які роблять взаємодію з вирішення деяких проблем неможливими. Самі терміни, що використовуються – "негативний зміст", "інформація, яка шкодить добробуту дітей", є дуже розмитими та можуть мати взаємовиключні тлумачення. У багатьох європейських країнах "нетрадиційні відносини" розглядаються як різновид норми, тож інформацію про них не заборонено. Законодавство деяких країн з авторитарним режимом правління передбачає кримінальну відповідальність за розповсюдження новин про ситуацію в цих країнах за кордоном, але навряд чи будь-які демократичні країни захочуть допомагати правоохоронним органам у виявленні порушників цієї заборони та вилученні зробленого ними контенту.

Загалом, складність впливу на ресурси Інтернету силами однієї країни призводить до пом'якшення політики контролю над негативним змістом, якщо не законодавчо, то фактично.

Слід також усвідомити, що можна боротися з негативним змістом, забороняючи або обмежуючи розповсюдження негативного контенту, а можна поширювати корисний вміст та спрощувати доступ до нього. Звичайно, одне не виключає іншого, але другий спосіб здається більш перспективним у багатьох сферах: замість просіювання гігантських обсягів даних у пошуках шкідливих потрібно буде лише забезпечити легкість пошуку корисних даних, що суперечать негативним. Наразі процес розробки ефективних заходів впливу тільки розпочався.

Перепьолкін Сергій Михайлович
к.ю.н., доц., доцент кафедри
теорії та історії держави і права
Дніпропетровського державного
університету внутрішніх справ

ЄВРОПЕЙСЬКИЙ ПОЛІЦЕЙСЬКИЙ ОФІС (ЄВРОПОЛ)

Історію діяльності ЄВРОПОЛ умовно можна розділити на два періоди:

1. ЄВРОПОЛ як міжнародна міжурядова організація держав – членів Конвенції про заснування Європейського поліцейського офісу (використовуються також терміни «відомство», «управління») від 26 липня 1995 р.;

2. ЄВРОПОЛ як Агентство Європейського Союзу (далі – ЄС).

Як міжнародна міжурядова організація, заснована Австрією, Бельгією, Великобританією, Грецією, Данією, Ірландією, Іспанією, Італією, Люксембургом, Нідерландами, Німеччиною, Португалією, Фінляндією, Францією та Швецією, ЄВРОПОЛ фактично розпочав діяльність з 1липня 1999 р., хоча Конвенція про його заснування набрала чинності з 1 жовтня 1998 р., та проіснував до 31 грудня 2009 р.

З 1 січня 2010 р. ЄВРОПОЛ, після набрання чинності Рішення Ради ЄС