УДК 342.5:002.6

БЄЛЄВЦЕВА В.В., *доктор юридичних наук, старший науковий співробітник*,
завідувач сектору інформаційного правопорядку
НДІ інформатики і права НАПрН України

УДОСКОНАЛЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ОБІГУ КОМП’ЮТЕРНОЇ ІНФОРМАЦІЇ

Анотація. *Розглянуто окремі аспекти міжнародного співробітництва щодо протидії правопорушенням у сфері комп’ютерної інформації. Наведені підходи до удосконалення національного законодавства з питань відповідальності за правопорушення у сфері комп’ютерної інформації, а також напрями міжнародної співпраці щодо протидії кіберправопорушенням.*

Ключові слова: *інформація, комп’ютерна інформація, кіберправопорушення, відповідальність, протиправні дії у сфері комп’ютерної інформації.*

Аннотация. *Рассмотрены отдельные аспекты международного сотрудничества в области противодействия правонарушениям в сфере компьютерной информации. Приведены подходы к усовершенствованию национального законодательства по вопросам ответственности за правонарушение в сфере компьютерной информации, а также направления международного сотрудничества в области противодействия киберправонарушениям.*

Ключевые слова: *информация, компьютерная информация, киберправонарушения, ответственность, противоправные действия в сфере компьютерной информации.*

Summary. *The article considers some aspects of international cooperation in area of counteraction to offences in the field of computer information. In conclusions the author of the article brings approach of improvement to the national legislation regarding responsibility for offence in the field of computer information, and also directions of international cooperation in area of counteraction to cyber offences.*

Keywords: *information, computer information, cyber offences, responsibility, illegal actions in the field of computer information.*

Постановка проблеми. Сучасний розвиток держави та суспільства стає більш залежним від використання та роботи комп’ютерних систем для автоматичної обробки інформації. Особливої актуальності проблеми удосконалення правового регулювання комп’ютерної інформації набувають у зв’язку з інтенсивним процесом модернізації комп’ютерних систем, що призводить до появи нових можливостей вчинення правопорушень в інформаційній сфері.

В усьому світі комп’ютерні технології та мережа Інтернет досить швидко входять до повсякденного життя. За оцінкою незалежних експертів кількість користувачів Інтернет в Україні на кінець 2015 року складає не менш 58 %. За матеріалами Кабінету Міністрів України, біля 17 % користувачів мережі Інтернет здійснили купівлю-продаж через мережу Інтернет, а більш третини українців користувачів соціальних мереж здійснили придбання в он-лайн-режимі за допомогою соціальних мереж. Не дивлячись на те, що переважна більшість операцій в мережі Інтернет здійснюються із законними цілями, усесвітня мережа дедалі частіше використовується для запровадження шахрайських схем.

У 2014 році Управління по боротьбі з кіберзлочинністю МВС України зареєструвало 4800 злочинів у сфері ІТ, у 2015 році – 6025 [1].

У таких державах, як США, Великобританія, Японія, Канада, Німеччина державні уряди усвідомили характер загрози від комп’ютерних правопорушень, і створили більш менш ефективну систему законодавства і правоохоронних органів для боротьби з ними. Боротьба з такого роду правопорушеннями базується на розумінні необхідності тісної взаємодії і співпраці на усіх рівнях державної влади і приватного сектора економіки [2].

Глибоке дослідження проблем комп’ютерних технологій неможливе без залучення фахівців різних галузей знань – кібернетики, математики, інформатики, радіотехніки, електроніки, зв’язку тощо. Найважче фахівцям юридичної науки, оскільки необхідно як дати своєчасну і належну правову оцінку існуючим правопорушенням у сфері комп’ютерної інформації, так і підготувати норми закону до появи нових форм комп'ютерних правопорушень. Одночасно важливо не тільки професійно сформулювати закон, але і розробити механізм його реалізації.

За час дії статей Кодексу України про адміністративні правопорушення (далі – КУпАП) та Кримінального кодексу України (далі – КК України) правопорушення у сфері комп’ютерної інформації як в теорії, так і в практиці їх застосування виявилися істотні суперечності, причинами яких, є: недоліки правової конструкції норм про правопорушення у сфері комп’ютерної інформації, невірне уявлення правоохоронних органів про значення і роль досліджуваних норм у забезпеченні захисту та охорони суспільних стосунків, помилки у теоретичному і практичному тлумаченні деяких правових термінів і положень ст. 188^{39} ; 212^{2} – 212^{6} КУпАП та ст. 361-363^{1} КК України.

Метою статті є визначення напрямів оновлення законодавства України з питань відповідальності за правопорушення у сфері обігу комп’ютерної інформації.

Виклад основного матеріалу. Захист інформації, що знаходиться в обігу в інформаційних системах та інформаційно-телекомунікаційних мережах, від несанкціонованого доступу, використання, розголошування, поширення, зміни або знищення інформації здійснюється в державі з метою забезпечення: цілісності і достовірності інформації (недопущення неправомірної зміни або знищення інформації); охорони конфіденційності інформації, доступ до якої обмежений законом або відповідно до закону; реалізації права на інформацію (гарантованого доступу до інформації, у випадках, коли такий доступ має бути забезпечений).

Слід зауважити, що основні поняття в законодавстві з питань обігу комп’ютерної інформації були сформульовані досить давно. За цей час науково-технічний прогрес не зупинявся, тому сьогодні з’являються нові терміни та категорії, які вимагають прийняття принципово нових законів. Наприклад, такий феномен як “спам”, що оцінюється у законодавстві багатьох держав як правопорушення у мережі Інтернет, в українському законодавстві не має належного регулювання.

Практика реалізації положень національного законодавства з досліджуваної проблематики свідчить про те, що наявні проблеми протидії правопорушенням у сфері обігу комп’ютерної інформації обумовлені недосконалістю правових норм, суперечністю їх тлумачення, відсутністю науково-методичних рекомендацій та офіційних управлінських роз’яснень щодо кваліфікації цих діянь, наприклад, постанов Верховного Суду України, а також ратифікованих міжнародних угод з питань ефективної спільної боротьби з даними видами правопорушень.

В українському законодавстві відсутній чіткий понятійний апарат, що стосується інформації та інформаційного обміну. Це дає, у свою чергу, можливість маніпулювати поняттями та уникати відповідальності. Якщо розглядати детальніше нормативно-правові акти України, то можна наявно побачити розбіжність в поняттях і відсутність

чітких визначень, особливо в наукових поняттях і технічних термінах у нормативно-правових актах, Держстандартах, технічній літературі тощо.

Державне регулювання у сфері захисту комп’ютерної інформації здійснюється шляхом встановлення вимог щодо захисту самої інформації, щодо власників інформації, користувачів інформації та власників інформаційних систем, користувачів інформаційно-телекомунікаційних мереж, а також відповідальності за несанкціонований доступ до конфіденційної інформації або за інші види правопорушень у сфері захисту інформації і права на інформацію.

З метою ефективної протидії несанкціонованому доступу до комп’ютерної інформації зусиль лише на національному рівні недостатньо. Необхідна розробка, стандартизація та уніфікація законодавства та програмних засобів, що дозволять визначити місцезнаходження та встановити особу, яка протиправно використовує комп’ютерну інформацію засобами комп’ютерних мереж та глобальних телекомунікаційних систем, відповідно до досвіду держав, що підписали Європейську конвенцію про кіберзлочинність [3].

Важливим документом у досліджуваній сфері є прийнята 15 березня 2016 року Стратегія кібербезпеки України [4]. Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Основу національної системи кібербезпеки України становитимуть Міністерство оборони України, Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Також слід акцентувати увагу на вирішенні організаційних проблем виявлення та ідентифікації осіб, які вчиняють протиправні дії у сфері комп’ютерної інформації на міжнародному рівні за допомогою оперативно-розшукових заходів. При цьому, з метою визнання судовими інстанціями різних держав у якості доказів документів передбачити методи фіксації, збору та передачі їх, можливості точного визначення географічного місцезнаходження вузлів мережі Інтернет для того, щоб правоохоронні органи змогли визначити країну походження й тим самим країну процесуальної юрисдикції, у тому числі використовуючи так звану “комп’ютерну розвідку”. З метою впровадження вищевикладених пропозицій видається необхідним доробити існуючі законодавчі акти, а також прийняти нові.

З урахуванням швидкого розвитку глобальних комп’ютерних мереж особливу роль могла б зіграти міжнародна інтегрована база даних кіберправопорушників, в якій фіксувалися б особи, схильні до вчинення протиправних дій у сфері комп’ютерної інформації, характеристика вчинених правопорушень тощо. При цьому необхідно розробити та запровадити закриті канали доступу до комп’ютерної мережі між підрозділами кіберполіції різних держав для повсякденного та екстреного зв’язку. Можливо, міжнародні угоди повинні включати деякі процесуальні санкції.

У зв’язку з цим необхідно розробити комплекс пропозицій до удосконалення правового регулювання протидії кіберправопрушенням. Отже, вважаємо за доцільне навести наші думки з цього приводу.

Використовуваний в українському законодавстві термін “правопорушення у сфері комп’ютерної інформації” певною мірою відповідає змісту Розділу XVI КК України. У світлі необхідних змін і розширення переліку складів даного виду правопорушень, уявляється правильнішим використання терміну “кіберправопорушення” для позначення будь-яких правопорушень, здійснених з використанням комп’ютера. Дане формулювання також відповідає традиційним уявленням про об’єкт посягання, як сферу соціальних відносин, і виводить з чисто технічної в суспільну площину.

Далі, на законодавчому рівні необхідно закріпити поняття комп’ютерної інформації, використовуване в законодавстві України (наприклад, комп’ютерна інформація – це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватись, змінюватись чи використовуватись за допомогою АЕОМ.

Також слід змінити поняття інформації, закріплене в українському законодавстві. При цьому можливо застосування підходу, використовуваного в міжнародно-правових актах, коли не дається чітке визначення інформації, але перераховується, що для цілей даного акту включається в поняття інформації. Такий підхід спрощує роботу правозастосовчих органів і робить ефективнішою реалізацію положень нормативно-правових актів. Разом з тим, такий підхід не знімає необхідності розроблення загального і прийнятного визначення інформації.

Висновки.

Пропозиції з удосконалення законодавства щодо відповідальності за правопорушення у сфері обігу комп’ютерної інформації можуть бути зведені до наступного:

– у число ознак об’єктивної сторони деяких складів КУпАП та КК України слід включити використання комп’ютерної техніки. Таким чином, включення використання комп’ютерної техніки в число ознак об’єктивної сторони відповідало б і вимогам практики (такі зміни полегшили б кваліфікацію діянь), і підвищеної суспільної небезпеки подібних правопорушень. Як приклад, можна навести склад шахрайства, здійсненого з використанням комп’ютера (у японському законодавстві існує окремий склад комп’ютерного шахрайства), розкрадання, здійсненого шляхом використання комп’ютерної техніки; незаконне отримання інформації, що складає комерційну або банківську таємницю, шляхом перехоплення в засобах зв’язку, незаконного проникнення в комп’ютерну систему або мережу; порушення правил поводження з інформацією (документами, комп’ютерною інформацією), що містить державну таємницю;

– вважаємо за необхідне внесення змін до статей КУпАП та КК України, що встановлюють юридичну відповідальність за ухилення від сплати податків і зборів. Зокрема, слід виділити таку ознаку об’єктивної сторони правопорушень, як ухилення від сплати податків у сфері електронної торгівлі. Підвищена суспільна небезпека даного правопорушення визначається його високою латентністю і зростаючими обігами електронної комерції, оскільки обіг електронної торгівлі в Україні постійно зростає. Офіційна статистика відсутня, проте, на думку експертів, електронні продажі будуть надзвичайно швидко зростати і стануть сегментом ринку, що динамічно розвивається. Правопорушення, пов’язані з ухиленням від сплати податків, з одного боку не відносяться до комп’ютерних правопорушень у вузькому сенсі, а з іншого – вони безпосередньо пов’язані з такою сферою як кіберпростір, комп’ютерні мережі і здійснюються з використанням комп’ютера;

– необхідно доповнити розділ XVI КК України статтями, що передбачають відповідальність за кібератаки на сайти в Інтернеті, за виробництво, продаж, придбання для використання комп’ютерних паролів, кодів доступу або інших даних, за допомогою яких можна отримати доступ до комп’ютерної системи з метою використання їх для вчинення протиправних дій. Слід криміналізувати й дії з виготовлення та збуту спеціальних засобів для неправомірного доступу до комп’ютерної системи або мережі;

– слід передбачити такі заходи з профілактики комп’ютерних правопорушень, як повідомлення приватних компаній про загрозу електронних атак і рекомендації щодо встановлення відповідного програмного забезпечення із захисту від комп’ютерних правопорушень;

– слід також встановити систему податкових пільг для тих підприємств, які вкладають кошти у розробку систем захисту інформації. Очевидно, що в результаті втрат приватних компаній від комп’ютерних правопорушень, шкоди зазнає й держава у цілому. Це виражається в недоотриманих податках, паралізації банківської діяльності тощо.

Підводячи підсумок слід зазначити, що аналіз міжнародно-правового регулювання комп’ютерних правопорушень дозволяє зробити висновок про відсутність належного та ефективного нормативно-правового регулювання комп’ютерних правопорушень і про гостру необхідність його розробки. Специфіка і тенденції розвитку законодавства з питань протидії комп’ютерним правопорушенням вимагають найпильнішої уваги учених різних спеціальностей. Піднімаючи питання забезпечення безпеки комп’ютерної інформації, хотілось привернути увагу до даної проблеми і стимулювати подальше обговорення цієї тематики.

Використана література

1. В Україні зростає кількість кіберзлочинів / “Економічна правда” від 28.03.16 р. – Режим доступу : http://www.epravda.com.ua/news/2016/03/28/587044

2. Информационные технологии : учебник ; под ред. В.В. Трофимова. – М. : Издательство Юрайт ; ИД Юрайт, 2011. – 624 с.

3. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824-IV // Відомості Верхововної Ради України (ВВР). – 2006. – № 5-6. – Ст. 71.

4. Про рішення Ради національної безпеки і оборони України від 27.01.2016 р. “Про Стратегію кібербезпеки України” : Указ Президента України від 15.03.16 р. № 96/206 // Офіційній вісник України. – 2016. – № 23. – С. 69.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~