доброякісність, достовірність), але й являють собою достатню та узгоджену сукупність для того, щоб сформувати у правоохоронця внутрішнє переконання (тобто таке, яке склалося без будь-якого зовнішнього впливу, наприклад, телефонного права та ін.) про те, що певне проміжне або тим більше остаточне процесуальне рішення у провадженні може бути прийнято. У такому випадку будь-які суб'єктивні відомості, тобто такі, які отримані від особистісного джерела, «об'єктивізуються» такого роду переконанням правоохоронця, який буде впевнений у тому, що й шляхом суб'єктивних відомостей у сукупності з іншими відомостями встановлена власне об'єктивна істина і тільки на її основі вирішується певне провадження. Інакше необхідно прямо визнати існування ситуацій з вирішення певних кримінальних проваджень не на доказах, а на припущеннях.

У такому аспекті виглядає необґрунтованим акцент уваги в ч. 1 ст. 62 Конституції України на тому, що «обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом, а також на припущеннях» [1], коли нібито виправдання особи може ґрунтуватися і на доказах, одержаних незаконним шляхом, і на припущеннях. Усі суб'єкти кримінального, як і будь-якого іншого провадження, доказування повинні прагнути до встановлення об'єктивної істини у процесі і мати у цьому відношенні рівні права, свободи, інтереси і нести рівні обов'язки. Цьому суперечить й існуючий різний обсяг обов'язків, наприклад, особистісних джерел кримінальних відомостей, насамперед, свідка, потерпілого і переслідуваної особи, давати достовірні показання і т.д.

Література

1. Конституція України від 28 черв. 1996 р. № 254к/96-ВР. URL: http://zakon2. rada.gov.ua/laws/show/ 254к/96-вр (дата звернення: 14.01.2021).

2. Кримінальний процесуальний кодекс України від 13 квіт. 2012 р. № 4651-VI. URL: http://zakon4.rada.gov.ua/laws/show (дата звернення: 14.01.2021).

3. Спасович В.Д. О теории судебно-уголовных доказательств в связи с судоустройством и судопроизводством. Москва: ЛексЭст, 2001. 112 с.

УДК 343.14:004(043.2)

Леонов Б.Д., д.ю.н., с.н.с.,
Серьогін В.С., науковий співробітник,
Український науково-дослідний інститут спеціальної техніки
та судових експертиз Служби безпеки України, м. Київ, Україна

КРИМІНАЛЬНО-ПРАВОВА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ

На стан кіберзлочинності істотно впливає бурхливий розвиток інформаційних технологій та розширення сфери їх застосування.

На думку експертів ОБСЕ, кіберзлочинність, пов'язана з використанням інформаційних технологій, комп'ютерних систем та мереж, здатна створити такий хаос, який за масштабом наближується до економічної кризи. У 2008 році щорічна шкода від кіберзлочинності оцінювалася приблизно у 100 млрд. доларів [1]. Сьогодні збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн. на рік, а за негативним сценарієм у 2021 році вони сягатимуть $ 2 трлн [2].

Революційний стрибок у сучасних інформаційних технологіях на початку XXI століття можна порівняти з появою у 1945 р. ядерної зброї, небезпечний руйнівний потенціал якого зумовив впровадження правових підстав її застосування.

Масштаб та рівень суспільно небезпечних наслідків кіберзлочинності обумовлюють необхідність впровадження адекватних підходів щодо удосконалення кримінально-правового забезпечення протидії кіберзлочинності.

Як на міжнародному, так і національному рівні кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами. До цього часу не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці.

Кримінально-правова політика у сфері забезпечення інформаційної безпеки в основному здійснюється за напрямками, що випливають з міжнародних зобов'язань України. Втім боротьба з кіберзлочинністю залишається недостатньо ефективною. Це свідчить про необхідність удосконалення всієї системи кримінально-правового забезпечення охорони інформаційної безпеки України з урахуванням її міжнародних зобов'язань.

Серед основних міжнародних нормативно-правових актів щодо протидії кіберзлочинності виділяються: Конвенція ООН проти транснаціональної злочинності 2001 р. (ратифікована із застереженнями і заявами Законом України від 04.02.2004 р. № 1433-IV), Європейська конвенція про взаємну правову допомогу у кримінальних справах 1959 р. (ратифікована із застереженнями і заявами Законом України від 16.01.1998 р. № 4498-ВР, Конвенція про кіберзлочинність 2001 р. (ратифікована із застереженнями і заявами Законом України від 07.09.2005 р. № 2824-IV).

Конвенція про кіберзлочинність 2001 року передбачає встановлення відповідальності за «правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи» тощо.

Ми підтримуємо позицію вчених, на думку яких кримінально-правовий обсяг поняття «кіберзлочинність» визначається рівнем суспільно небезпечних загроз, зміст яких складають як правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних, навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних, так і кримінальне каране втручання у роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, навмисне серйозне перешкоджання їх функціонуванню.

Поряд із поняттям «кіберзлочинність» у кримінально-правовому аспекті вживається поняття «злочини у сфері використання інформаційних технологій». Забезпечення кримінально-правового стимулювання позитивних та мінімізації негативних соціальних наслідків інформатизації передбачає визначення як самостійного об'єкта кримінально-правової охорони системи суспільних відносин, які забезпечують реалізацію інформаційної потреби. Для позначення цієї системи використовують термін «інформаційна безпека», її структуру складають відносини у сфері формування інформаційного ресурсу, забезпечення доступу до інформації, а також відносини у сфері використання інформаційних технологій [3, с. 11; 4]. Суспільна небезпечність злочинів у сфері використання інформаційних технологій головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це і визначає суспільну небезпечність конкретного посягання в сфері використання інформаційних технологій [5].

Водночас слід зазначити, що норми про злочини, які передбачені розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК, не охоплюють увесь спектр злочинних діянь у сфері інформаційної безпеки. Тому більш прийнятною важаться зміна назви розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК на «Злочини у сфері використання інформаційних технологій».

Схожий підхід закладений у законопроекті про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки (реєстр. № 9575 від 09.12.2011), згідно з яким родовим об'єктом злочинів, що розглядаються, є суспільні відносини у сфері інформаційної безпеки, що, на думку його розробників, зумовлює зміну назву розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК на «Злочини у сфері інформаційної

безпеки» [6].

Враховуючи викладене, вважаємо, що під час удосконалення законодавства України про кримінальну відповідальність назву розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК доцільно змінити на «Злочини у сфері використання інформаційних технологій», а його зміст доповнити нормами про злочини проти конфіденційності, цілісності та доступності комп'ютерних даних.

Література

1. Киберпреступность страшнее финансового кризиса. URL: https:www.crime-research.ru/news/03.12.2008/50.

2. Киберпреступники наживаются на самых бедных. URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief.

3. Карчевский Н.В. «Киберпреступление» или преступление в сфере использования информационных технологий? Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). Одеса: ОДУВС, 2016. С. 10-14.

4. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 512 с.

5. Карчевський М.В. Дослідження практики використання національними судами норм про кримінальну відповідальність за злочини в сфері використання комп'ютерної техніки та мереж електрозв'язку. Злочини в сфері використання ІТ. URL: http//www.it-crime.at.ua.

6. Офіційний сайт Верховної Ради України. URL: http://w1.c1.rada.gov.ua/pls/ zweb2/webproc4_1?pf3511=42065.

УДК 343.346.2(043.2)

Лисько Т.Д., к.ю.н.,
Галатенко К.В., Дяченко О.С., здобувачі вищої освіти,
Національний авіаційний університет, м. Київ, Україна

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ ПРОТИ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ ТА ЕКСПЛУАТАЦІЇ ТРАНСПОРТУ: ОКРЕМІ КОНЦЕПТУАЛЬНІ АСПЕКТИ

Останніми роками питання протидії порушенням правил дорожнього руху й експлуатації транспорту привертає все більше громадської уваги та викликає цікавість науковців. Автомобільний транспорт відіграє дедалі більшу роль у суспільному та особистому житті кожної людини, оскільки саме він сприяє задоволенню потреб усього суспільства в перевезенні