Овчар Алла Сергіївна

студентка 4-го курсу Інституту кримінальної юстиції
Національного університету «Одеська юридична академія»

КІБЕРЗЛОЧИННІСТЬ: КРИМІНОЛОГІЧНА СУТНІСТЬ ТА ДЕТЕРМІНАЦІЯ

Стрімке проникнення в повсякденне життя комп'ютерної техніки та комп'ютерних технологій, що сприяє розвитку інформаційних, телекомунікаційних та інформаційно-телекомунікаційних мереж, поставили перед суспільством питання про необхідність захисту від протиправних посягань як особистої інформації, так і найбільш важливих сегментів національної безпеки – фінансового, економічного та інформаційного. Сьогодні складно собі уявити сферу діяльності, в якій не використовується комп'ютерна техніка, комп'ютерні та телекомунікаційні мережі. Жоден складний технологічний процес не може існувати без високих (інформаційних) технологій, соціальні мережі з кожним роком залучають мільйони користувачів, кожен з яких довіряє мережі частину свого особистого життя. Однак і ця сфера «віртуальних» суспільних відносин не позбавлена вразливості. У ній, за рахунок знеособленості користувачів, часто знаходять відображення найбільш негативні прояви особистості, внаслідок необізнаності користувачів про існуючі можливості мережі, вона проста і доступна для злочинних посягань. Це, перш за все, викликано тим, що глобальні цифрові технології відкривають нові можливості для діяльності злочинців, сприяють поширенню злочинів у сфері порушення прав інтелектуальної власності, створюють умови для поширення продукції порнографічного характеру, матеріалів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість і дискримінацію, спрощують можливість придбання і збуту наркотичних і психотропних засобів, зброї тощо.

Під кіберзлочинністю слід розуміти відносно масове соціально-правове явище, яке охоплює сукупність суспільно небезпечних діянь, передбачених КК України, Конвенцією про кіберзлочинність та Додатковим протоколом до неї з урахуванням застережень, зроблених Верховною Радою України, в яких інформаційно-телекомунікаційна система або її елементи є засобом вчинення злочину.

Соціальна обумовленість кіберзлочинності детермінується політико-правовими, економічними, організаційно-управлінськими, ідеологічними та соціально-психологічними факторами. Розглядаючи політико-правові чинники, слід визнати, що її поява і стрімке зростання більшою мірою обумовлені відсутністю адміністративно-територіальних та інших кордонів (особливо в глобальних мережах), а також єдиного

підходу до розгляду питань поширення інформації та захисту прав і свобод окремих громадян, різними поглядами національного законодавця про те, які дії є кіберзлочинами і вимагають кримінально-правової заборони. Економічні чинники детермінації кіберзлочинності пов'язані перш за все з процесом глобалізації світової економіки і глобалізації в цілому. Група організаційно-управлінських факторів пов'язана, перш за все, з недоліками соціального контролю: ігнорування користувачами елементарних вимог інформаційної безпеки, низька підготовленість правоохоронних органів до боротьби з кіберзлочинністю і неналежна їх технічна оснащеність, відсутність кваліфікованих кадрів.

Істотний вплив на поширеність кіберзлочинів справляють і соціально-психологічні чинники. В умовах кіберпростору істотно змінюється психологічний зміст взаємозв'язків злочинець – предмет злочину, а також злочинець – потерпілий, які з прямих перетворюються в непрямі: злочинець – електронний пристрій (мережа) – потерпілий (предмет злочину), що веде до усунення матеріальної складової, як дій людини, так і соціальної взаємодії.

Щодо масовості кіберзлочинів слід зазначити, що кіберзлочинність має свою специфіку, пов'язану, перш за все, з латентністю даного злочину і відсутністю відокремленого статистичного обліку злочинів, віднесених до категорії кіберзлочинів Конвенцією про кіберзлочинність. Так, відповідно до статистичних даних, розміщених на офіційному сайті Генеральної прокуратури України, кількість врахованих правопорушень, що мають ознаки злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ XVI КК України) становив лише 0,1% в 2016 р. і 0,08% в 2017 році. Разом з цим, статистичні показники не відображають реальної картини кіберзлочинності, так як не враховують: комп'ютерне шахрайство (ст. 8 Конвенції), злочини, пов'язані з дитячою порнографією (ст. 9 Конвенції), порушення, пов'язані з порушеннями авторського права і суміжних прав (ст. 10 Конвенції), а також можливість здійснення «традиційних» злочинів з використанням інформаційно-телекомунікаційних мереж. Згідно з дослідженнями, проведеними в липні 2013 р американським Центром стратегічних і міжнародних досліджень та компанією McAfee, щорічні втрати світової економіки від кіберзлочинів досягли вже 500 мільярдів доларів [1].

Вищевказане дозволяє зробити висновок про те, що кіберзлочинність являє собою особливий вид злочинності, являє масове соціально-правове явище, що охоплює сукупність суспільно небезпечних діянь, передбачених КК України, Конвенцією про кіберзлочинність та Додатковим протоколом до неї з урахуванням застережень, зроблених Верховною Радою України, в яких інформаційно-телекомунікаційна система або її елементи є засобом вчинення злочину. При цьому їй притаманні всі ознаки «традиційної» злочинності (соціальна обумовле-

ність, відносна масовість, негативний кримінально-правовий характер і ін.), які мають свою специфіку. З огляду на існуючі особливості, пов'язані з протидією кіберзлочинності на національному рівні, комплексність проблеми, яка зачіпає сферу спеціальних знань, необхідно направляти нормотворчість законодавця на імплементацію норм міжнародного права в практику протидії цим злочинним проявам.

Список використаних джерел

1. Кримінальний кодекс України від 05.04.2001 №2341-III. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2341-14/card6#Public.
2. Конвенція про кіберзлочинність // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71. Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_575.
3. Кримінологія : підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін. ; за ред. В. В. Голіни, Б. М. Головкіна. – Х. : Право, 2014. – 440 с.
4. Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності / Є. Д. Скулиш // Інформація і право. – 2014. – № 1. – С. 93-100.
5. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру / І. В. Гринчак // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. – 2015. – № 12. – С. 93-98.
6. Марков В. В. Щодо питання стосовно зарубіжного досвіду протидії кіберзлочинності / В. В. Марков Національний юридичний журнал: теорія і практика. – 2015. – С. 187-191.
7. Коліса Я. Ю. Взаємодія служб у боротьбі з кіберзлочинністю / Я. Ю. Коліса // Криміналістичний вісник. – 2015. – № 1. – С. 99-8.
8. Номоконов В. А. Киберпреступность: угрозы, прогнозы, проблемы борьбы / В. А. Номоконов, Т. Л. Тропина // Information Technology and Security. – 2013. – № 1 (3). – С. 88.

Науковий керівник: к.ю.н., доцент Чернишов Г. М.

Панасюк В. В.

Національний університет «Одеська юридична академія»
студент 4 курсу Інституту кримінальної юстиції

ПРОБЛЕМИ ПРОКУРОРСЬКОГО НАГЛЯДУ ЩОДО ПОРЯДКУ ВИКОНАННЯ ПОКАРАНЬ

Останнім часом спостерігається стрімка зміна законодавства у правоохоронній сфері. Органи прокуратури, без сумніву, найбільш піддалися реформуванню. Спостерігається відхід функцій, які були