

І.О. Біла,
студ. III курсу, спеціальність “Право”,
Одеський національний університет імені І.І. Мечникова

Науковий керівник: д.ю.н., проф. кафедри кримінального права, кримінального процесу та криміналістики О.А. Чуваков

СУЧАСНИЙ СТАН КРИМІНАЛЬНОЇ ЗЛОЧИННОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розвиток інформаційних технологій, відкритий доступ до Інтернету, “безвізове подолання кордонів”, довільний ступінь анонімності, відсутність цензури створюють різноманітні можливості (підґрунтя) для вчинення нових видів злочинів, а також звичайних традиційних злочинів, але більш ефективними способами. *Актуальність даної теми* полягає у тому, що для виявлення та розкриття злочинів, які вчиняються за допомогою сучасних інформаційних технологій, законодавець іде на шляху створення і прийняття ряду базових нормативних актів у галузі інформаційних (комп’ютерних) відносин, яких на сьогодні, на жаль, є недостатньо для ефективного вирішення даної проблеми. Тому, сьогодні, *необхідно* проаналізувати сучасний стан злочинності, вияснити причини його виникнення та знайти шляхи попередження вчиненню правопорушень у сфері інформаційних технологій.

Слід зазначити, що вперше склади злочинів у сфері інформаційних технологій (комп’ютерних злочинів) були викладені на Конференції американської асоціації адвокатів у Далласі ще 1979 року. Пізніше, Організація Об’єднаних Націй (далі – ООН), опублікувала Керівництво ООН з попередження злочинів, пов’язаних із застосуванням комп’ютерів, і боротьбі з ними (1994 р.). У даному Керівництві ООН надала класифікацію “звичайних видів” комп’ютерних злочинів, до яких віднесла: шахрайство шляхом маніпуляцій на комп’ютері, комп’ютерну підробку, несанкціонований доступ до комп’ютерних систем і послуг, несанкціоноване копіювання комп’ютерних програм, які охороняються законом тощо [1].

Кримінальна відповідальність за комп’ютерні злочини в Україні була передбачено з 1994 року. На сьогодні Особлива частина Кримінального кодексу України (далі – КК України) містить Розділ XVI, який присвячується злочинам у сфері використання електронно-об-

числювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [2, ст.ст. 361–363-1]. Крім того, аби забезпечити ефективність боротьби зі злочинами у цій сфері та здійснити адаптацію до норм міжнародного законодавства, Україна у 2001 році приєдналася до Конвенції про кіберзлочинність, а у 2006 році – ратифікувала Додатковий протокол до неї.

Слід зазначити, що кримінальне законодавство, як і ряд актів інших галузей права, охороняє законні процеси збору, обробки, накопичення, зберігання, пошуку, розповсюдження інформації, у тому числі комп'ютерної [3, с. 348].

Стосовно *сучасного стану кримінальної злочинності* в галузі інформаційних технологій, який склався в Україні, то можна сказати, що у нашій державі кількість “комп'ютерних злочинів” не є значною у порівнянні з такими країнами, як США, Великобританія, Німеччина, Китай тощо, де показники даних злочинів сягають небачених масштабів, але є наявний напрям до її росту.

Аналізуючи відомості про кількість зареєстрованих кримінальних правопорушень у цій сфері з 2005 року по сьогодні, можна побачити тенденцію до збільшення кількості “комп'ютерних злочинів”. Про це свідчать офіційні дані Державної служби статистики України щодо кількості злочинів, зареєстрованих органами внутрішніх справ, за статтями 361–363 КК України. Так, за 2005 рік офіційно було зареєстровано 62 правопорушення; 2008 році – 169; за 2009 рік – 201, а виходячи за підсумками 2010 року – 165 правопорушень у цій сфері. Слід звернути увагу, що за ст. 361-1, 361-2 та 363-1 КК України протягом зазначених років не було порушено жодної кримінальної справи [4, с. 3-4].

Відповідно до статистичної інформації про стан злочинності та результати прокурорсько-слідчої діяльності, а саме Єдиного звіту про кримінальні правопорушення, стосовно загальної відомості про кількість зареєстрованих кримінальних правопорушень у сфері використання електронно-обчислюваних машин (комп'ютерів), систем і комп'ютерних мереж з 2013 року по березень 2019 року (табл. 1), можна зробити висновок, що кількість вчинюваних правопорушень у цій сфері стрімко зростає з кожним наступним роком [5].

На думку експертів, збільшення кількості вчинюваних злочинів, зумовлено особливостями механізму віртуального простору, а саме у тому, що злочинці не бачать своїх жертв, яких “вони обрали для нападу”. Тим самим, винні особи мають впевненість в анонімності та відсутності безпосередньої небезпеки виявлення і переслідування. Як свідчить практика, отримавши опір технічної системи захисту щодо

Табл. 1. Загальні відомості про кількість зареєстрованих кримінальних правопорушень від 01.01.2013 по 11.03.2019 роки¹

		Обліковано кримінальних правопорушень за звітний період							
		2013 р. (січень- грудень)	2014 р. (січень- грудень)	2015 р. (січень- грудень)	2016 р. (січень- грудень)	2017 р. (січень- грудень)	2018 р. (січень- грудень)	2019 р. (січень- березень)	
За видами правопорушень	Ст. 361 КК України	408	344	432	494	1795	1023	216-...	
	Ст. 361-1 КК України	12	10	21	15	35	134	24-...	
	Ст. 361-2 КК України	20	11	59	28	64	52	12-...	
	Ст. 362 КК України	152	73	75	311	670	1070	157-...	
	Ст. 363 КК України	2	4	9	15	6	12	1-...	
	Ст. 363-1 КК України	1	1	2	2	3	10	1-...	
	Усього кримінальних правопорушень	595	443	598	865	2573	2301	411-...	

¹ Ці дані отримані на підставі власного аналізу Єдиного звіту про кримінальні правопорушення, за Формою № 1 (місячна) затвердженою наказом ГПУ від 23 жовтня 2012 р. № 100 за погодженням з Держстатом України, за кожен окремий рік, починаючи із січня 2013 р.- по березень 2019 р.

несанкціонованого доступу до комп'ютерної системи, злочинці шукають нову інформацію та вдосконалюють свої знання щодо способів і шляхів вчинення злочину. Необхідно зазначити, що мотивами вчинення комп'ютерних злочинів найчастіше виступають користь, хуліганські спонування, але вони можуть бути також вчинені за мотивами інтересу, почуття помсти, не виключний варіант їх здійснення з метою приховання іншого злочину.

Також, слід звернути увагу на те, що при проведенні кримінологічних досліджень, які засновані на опитуванні працівників правоохоронних органів та спеціалістів в галузі інформаційних технологій, зазначили, що за межами статистичних обліків (офіційних даних, зазначених у табл. 1) залишаються до 90% кіберзлочинів [6]. Кіберзлочинність охоплює різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет, а об'єктами кіберзлочинів виступають персональні дані, банківські рахунки, паролі та інша особиста інформація фізичних і юридичних осіб, бізнесу та державного сектору. Поширеними кіберзлочинами на сьогодні є кібершахрайство, протиправний контент (захист інтелектуальної власності), поширення шкідливого програмного забезпечення тощо [7]. Таке явище, а саме високу латентність цих злочинів, пов'язують з небажанням потерпілих подавати заяви до відповідних органів для початку кримінального провадження; недовіреністю працівників правоохоронних органів у розслідуванні цих злочинів через відсутність необхідної практики та засобів боротьби у цій сфері; труднощами в кваліфікації; відсутністю спеціалізованих експертиз для розслідування комп'ютерних злочинів; труднощами збирання доказів; відсутністю комп'ютерної культури, а також обізнаності громадян щодо своїх прав та обов'язків у сфері інформаційних технологій.

Виходячи з вищевикладеного, можна стверджувати, що *рівень кримінальної злочинності* у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку з кожним роком зростає. *Причин* для виникнення такої ситуації в Україні – безліч, основні з них: недосконала нормативно-правова база щодо попередження та протидії злочинам у сфері інформаційних технологій; відсутність у працівників правоохоронних органів необхідної практики та засобів боротьби з даними злочинами; неефективність діяльності правоохоронних органів у здійсненні діяльності по реагуванню на вчинений злочин та подану у зв'язку з цим заяву потерпілого; низький рівень інформатизації українського суспільства тощо. Великого значення у *попередженні, виявленні та боротьбі* з

комп'ютерними злочинами має виявлення і дослідження причин їх вчинення та напрацювання відповідних рекомендацій протидії, зокрема, за участю правоохоронних органів. Крім того, для попередження злочинів необхідно проводити інформаційно-аналітичну роботу, підготовку кадрів для роботи у сфері технічного захисту інформації, а також громадяни України повинні дотримуватися елементарних правил, які встановлені для користувачів, для того, щоб уникнути зайвої можливості стати потерпілим у сфері “комп'ютерних злочинів”.

Список використаної літератури

1. Стрельцов Є.Л., Загіка Г.В. Злочинність у сфері інформаційних технологій. URL: https://studopedia.su/10_65095_zlochinnist-u-sferi-informatsiynih-tehnolo-giy.html (дата звернення:16.03.2019 р).
2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. (зі змін. та доп.). URL:<https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення:16.03.2019 р).
3. Кримінальне право України: Особлива частина: Підручник / За заг. ред. д-ра юрид. наук, проф., засл. діяча науки і техніки України Є.Л. Стрельцова. Харків, 2009. 496 с.
4. Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України: Висновок на проект Закону України від 31 серпня 2012 р. № 11125. URL: <http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=44208&pf35401=237192> (дата звернення: 16.03.2019 р).
5. Статистична інформація про стан злочинності та результати прокурорсько-слідчої діяльності. Єдиний звіт про кримінальні правопорушення за Формою № 1 (місячна) затвердженою наказом ГПУ від 23 жовтня 2012 р. № 100 за погодженням з Держстатом України URL: <https://www.gp.gov.ua/ua/statinfo.html> (дата звернення:16.03.2019 року).
6. Спирина С. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации. URL: <http://www.dissercat.com/content/kriminologicheskie-i-ugolovno-pravovye-problemy-prestuplenii-v-sfere-kompyuternoi-informatsi> (дата звернення: 16.03.2019 року).
7. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: <https://www.gurt.org.ua/articles/34602/> (дата звернення: 16.03.2019 року).