Голушко В. В.,
студентка 5 курсу,
1 групи, Інституту прокуратури
та кримінальної юстиції
Національного юридичного університету
імені Ярослава Мудрого

ПОЗИТИВНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ

Ключові слова: кіберзлочин, кібербезпека, інформаційні технології, кіберзлочинність.
Key words: cybercrime, cyber security, information technologies, cybercriminality.
Анотація: Розглянуто питання кіберзлочинності в Україні та висвітлені позитивні аспекти кіберзлочинності.
Abstract: The issue of cybercrime in Ukraine. There are positive aspects of cybercrime represented.

Злочини у сфері комп'ютерної інформації мають динамічний характер. В результаті швидкого розвитку нових технологій не менш швидкими темпами з'являються нові форми комп'ютерної злочинності [1].

Не існує загальноприйнятого визначення кіберзлочинності. У різних країнах в це поняття вкладають різний сенс. За визначенням ООН кіберзлочинність – має на увазі будь-який злочин, який може бути здійснений з використанням комп'ютерної системи або мережі, в рамках або проти комп'ютерної системи або мережі. Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, здійснений в електронному середовищі. Злочин, здійснений в кіберпросторі – це протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні дії, здійснені за допомогою комп'ютерів, комп'ютерних мереж і программ.

На сьогодні законодавством України поняття "кіберзлочинність" безпосередньо не визначено. Європейська Конвенція про кіберзлочинність також не надає конкретного формулювання, хоча і визначає низку суспільно небезпечних діянь, які повинні мати статус кіберзлочинів на рівні національного законодавства. До них відноситься сукупність злочинів з використанням комп'ютерних систем і технологій, таких як незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання в дані, правопорушення, пов'язані з дитячою порнографією, що в цілому відповідає положенням Конвенції про кіберзлочинність.

Статистика свідчить, що наша країна є одним з лідерів за кількістю кібератак у всьому світі. Україна виявилася у цій сфері на четвертому місці після Росії, Тайваню і Німеччини [2].

За статистичною інформацією Генеральної прокуратури кількість злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку зростає. Серед цих злочинів, найбільш поширеними є такі злочини, як несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ) та несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 ККУ). Статистична інформація за останні 5 років проілюстрована у таблиці 1.

Таблиця 1 Співвідношення кількості зареєстрованих (облікованих) злочинів та кількості засуджених осіб за період 2013-2017рр.(станом на 01.11.2017)

		2013	2014	2015	2016	2017(станом на 01.11.2017)
ст. 36	Кількість зареєстрованих злочинів	408	344	432	494	1698

	Кількість засуджених осіб	113	135	74	164	391
ст. 361-1	Кількість зареєстрованих злочинів	12	10	21	15	34
	Кількість засуджених осіб	4	6	3	1	7
ст. 361-2	Кількість зареєстрованих злочинів	20	11	59	28	60
	Кількість засуджених осіб	10	5	43	13	42
ст. 362	Кількість зареєстрованих злочинів	152	73	75	311	632
	Кількість засуджених осіб	129	54	42	226	445
ст. 363	Кількість зареєстрованих злочинів	2	4	9	15	8
	Кількість засуджених осіб	0	1	0	1	1
ст. 363-1	Кількість зареєстрованих злочинів	1	1	2	2	5
	Кількість засуджених осіб	0	0	0	0	0

Сучасний стан розвитку телекомунікаційних, інформаційних та комп'ютерних технологій обумовлює появу та швидкий розвиток суспільних відносин з приводу їх використання. Це вимагає їх правову регламентацію, яка відповідала б інтересам суб'єктів таких відносин та економічній доцільності використання предметів, що уособлюють в собі подібні технології. Більше того, інформаційні технології та комп'ютерні мережі на сьогодні являють собою важливу галузь економіки, розвиток якої виходить за межі економіки однієї країни і характеризується наявністю усталених міжнародних зв'язків.

Разом з цим, інформаційний простір став місцем та в той же час й безпосередньо інструментом злочину. Головним інструментом злочинця стає лише комп'ютер та доступ до інформаційно-комунікаційних систем, де він за допомогою комп'ютерних вірусів та інших незаконних технічних засобів одержує доступ до баз даних, банківських рахунків, автоматизованих систем управління.

При цьому, кіберзлочинність набуває все більшого світового масштабу, новітні технології перетворюють реальних злочинців на анонімних, а легкість швидкого збагачення зваблює все більше людей долучитися до цієї злочинної діяльності[3].

Проте кіберзлочинність має як негативну, так і позитивну сторону. Тож розглянемо деякі позитивні аспекти кіберзлочинності.

Найголовнішим аспектом є розвиток нових технологій. Методи вчинення кіберзлочинів щодня вдосконалюються і стають дедалі складнішими. Відповідно реагують і правоохоронці. З цим явищем нерозривно пов'язаний розвиток комп'ютерних технологій, поява новітніх систем захисту та боротьби з кіберзлочинністю. Кіберзлочини спонукають світ до розвитку.

Із появою кіберзлочинів постала гостра потреба в законодавчій регламентації питання існування кіберпростору і злочинів з використанням інформаційних технологій. Поява і вдосконалення законодавста також є позитивною рисою для розвитку країни як правової держави.

Для ефективної протидії злочинам у сфері комп'ютерних технологій створюються нові правоохоронні органи. Сьогодні кіберзлочинам протидіє Департамент кіберполіції Національної поліції України, проте незабаром будуть створені окремі правоохоронні органи по боротьбі з кіберзлочинністю. Створення нових органів тягне за собою появу робочих місць.

Позитивним аспектом кіберзлочинності є також підготовка фахівців для боротьби з кіберзлочинністю. Серед молодих людей які прагнуть стати правоохоронцями багато тих, хто захоплюється комп'ютерним програмуванням, нині вони можуть поєднувати це і стати професіоналами у боротьбі з кіберзлочинністю. У Харківському національному університеті внутрішніх справ на підставі наказу МВС України від 20.11.2012 № 1062 функціонує факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми. На факультеті здійснюється підготовка фахівців за напрямами підготовки «Системи технічного захисту інформації» та «Правознавство» спеціалізації «боротьба з кіберзлочинністю» та «боротьба

з торгівлею людьми»[4].

Ще одним позитивним аспектом кіберзлочинності є співпраця з кіберзлочинцями. Кіберзлочинці, як і звичайні злочинці, часто на крок попереду правоохоронних органів, тому вони можуть ефективно та швидко викрити кіберзлочин. Не можна ігнорувати цей важливий аспект як співпраця, за допомоги кіберзлочинців ми зможемо вдосконалити системи захисту і запобігти вчиненню низки нових кіберзлочинів.

Поява кіберзлочинів зумовила появу нового простору для досліджень науковцями. Нові явища завжди тягнуть за собою інтерес людей пов'язаних з наукою. Недосліджені питання викликають неабияку зацікавленість і прагнення висвітлити питання неповторно. Кіберзлочинність це відносно нове явище, тому зараз багато науковців займаються саме проблемами кіберзлочинності.

Підсумовуючи вищевикладене можна сказати, що усі явища мають дві сторони, як позитивну, так і негативну. Не можна уявити суспільство без злочинності, вона існувала, існує і буде існувати. Негативні явища необхідні суспільству не менш ніж позитивні. Злочинці спонукають світ рухатись вперед, не залишаючись на місці ні хвилини. Як кажуть: «Не має лиха без добра».

Список використаних джерел:

1. Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів.
2. Орлов О. В., Онищенко Ю. М. Державна політика підготовки кадрів з попередження кіберзлочинності в Україні.
3. Методичні рекомендації «Кіберзлочинність в Україні: сучасні тенденції та напрями протидії» Головне територіальне управління юстиції у Житомирській області.
4. Демедюк С. В., Марков В. В. Підготовка та підвищення кваліфікації працівників у сфері боротьби з кіберзлочинністю.
5. Головкін Б. М. Поняття, предмет, система кримінології та її завдання на сучасному етапі розвитку / Б. М. Головкін // Питання боротьби зі злочинністю: зб. наук. пр. / редкол. В. І. Борисовна та ін. – Х. : Право, 2014. – Вип. 28. – С. 80-92.
6. Головкін Б. М. Види злочинності / Б. М. Головкін // Журнал східноєвропейського права. – 2015. – №. 18. – С. 14-21

Міністерство освіти і науки України

**Національний юридичний університет
імені Ярослава Мудрого**

ЗЛОЧИННІСТЬ У ГЛОБАЛІЗОВАНОМУ СВІТІ

Матеріали XVI Всеукраїнської кримінологічної конференції для студентів, аспірантів та молодих вчених

(м. Харків, 12 грудня 2017 р.)

За загальною редакцією
професора *А. П. Гетьмана* і професора *Б. М. Головкіна*

Харків
«Право»
2017

УДК 343.9.01:005.44
ББК 67.61я431
З-68

Злочинність у глобалізованому світі : матеріали XVI Всеукр.
З-68 кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. – Харків : Право, 2017. – 420 с.

ISBN 978-966-937-307-6

ISBN 978-966-937-307-6