Плетньова Т. Р.,
студентка 5 курсу,
8 групи, факультету адвокатури
Національного юридичного університету
імені Ярослава Мудрого

ДЕТЕРМІНАЦІЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Ключові слова: кіберзлочинність, кібербезпека, детермінанти
Keywords: cybercrime, cyber security, determinants
Анотація: Стаття присвячена аналізу специфічних (правових, політичних, економічних та психологічних) детермінант кіберзлочинності в Україні.
Abstract: The article is devoted to the analysis of specific (legal, political, economic and psychological) determinants of cybercrime in Ukraine.

Сучасне інформаційне суспільство охоплює всі сфери життєдіяльності людини і держави. А неминучим наслідком глобалізації інформаційних процесів є зростання кількості злочинів, що здійснюються в цій галузі. За оцінками Інтерполу, темпи зростання злочинності, наприклад, у глобальній мережі Інтернет, є найшвидшими на планеті [1, с. 9]. Сьогодні жертвами злочинців, що орудують у віртуальному просторі стають не лише люди, але і цілі держави. Боротьба з кіберзлочинністю не може бути ефективною без встановлення її детермінант, а тому актуальності набуває питання детермінації кіберзлочинності в Україні.

Якщо звернутися до загального кримінологічного поділу детермінант кіберзлочинності, можна виділити наступні групи: політичні, економічні, соціальні, технологічні, психологічні тощо. І хоча детермінанти кіберзлочинності в Україні безумовно мають свою специфіку, доречним вважається розглядати їх не розрізнено, а в межах наступних груп: політичні, правові, економічні та психологічні детермінанти.

У групі правових детермінант, одразу необхідно звернути увагу на недосконаліть правового регулювання державної політики у сфері кібербезпеки. Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 5 березня 2016 року №96/2016 передбачається створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Документ також передбачає комплекс заходів, спрямованих на боротьбу із кіберзагрозами, поглиблення міжнародного співробітництва у цій сфері, забезпечення захисту державних електронних інформаційних ресурсів та інформаційної інфраструктури [2]. Однак, слушно зазначається, що в Україні цей документ хоча і називається стратегією, проте визначені в ньому основні засади кібербезпеки у світовій практиці не зовсім вважаються стратегічними. Головним атрибутом у закордонних стратегіях передбачається перелік конкретних проектів забезпечення кібербезпеки із кінцевим терміном їх реалізації, з виділеним фінансуванням і, що найголовніше, конкретними відповідальними. У нас це нагадує більше концепцію – напрями, куди треба рухатися зі своїми тактиками дій, власним, а не державним, фінансуванням і без будь-якої відповідальності [3, с. 330].

Також до правових детермінант кіберзлочинності в Україні необхідно відносити недосконаліть організації системи органів, що розслідують кібернетичні злочини і притягають суб'єктів їх вчинення до відповідальності, а також некомпетентність посадових осіб цих органів. Наприклад, в Україні простий кіберзлочин – «зламування» сайту, наприклад, сторінки у соцмережі, організована групова злочинна діяльність, наприклад, атака на Інтернет-банкінг це справа кіберполіції. Однак, відімкненням електростанції від міської мережі вже займається СБУ як кібертероризмом. Коли ж відбуваються кібератаки по всій країні, які супроводжуються військовою агресією, повноважним органом є Збройні сили України [3, с. 331]. І хоча Стратегією визначено, що це не поодинокі суб'єкти, а система органів, однак, система передбачає наявність чіткої ієрархії і підпорядкованості, а вище наведені суб'єкти нехай і відносяться до однієї гілки влади, все ж таки залишаються окремими відомчими одиницями [4, с. 82].

З точки зору політичних процесів і чинників, які сьогодні відбуваються в Україні, необхідно підкреслити особливе значення загострення міждержавних відносин України з Російською Федерацією, зумовленою агресією зі сторони останньої. Ці явища є чинниками активізації численних кіберзлочинів, що вчиняються спецслужбами РФ, які активно використовують як своїх хакерів, так і з інших країн для економічної дестабілізації ідейних супротивників. В Росії за останнє десятиліття спостерігається дуже високий рівень інтеграції хакерів з військовими організаціями, державними і приватними структурами, позаяк там задіяні різні інтереси та обертаються чималі кошти[4, с. 331]. У цьому контексті, також вказується на існування такого протиправного феномену сучасності, як «кібервійна», яка розглядається не лише як різного роду шпигунство, а й боротьбу держав в Інтернет-просторі за свідомість і настрої громадян [5, с. 179].

Наступним фактором детермінації кіберзлочинності є економічний. В Україні, як і в усьому

світі економічні фактори детермінації пов'язані, перш за все, з процесом глобалізації світової економіки. Модернізація сучасного соціуму шляхом впровадження у життя продуктів комп'ютерної техніки та технологій несе з собою цілу низку новоутворень в соціальному бутті. Доступ все більшої кількості користувачів до глобальних інформаційних мереж, розвиток електронної торгівлі, можливість відкриття банківських рахунків через Інтернет і здійснення online-операцій, що не вимагають безпосереднього контакту з контрагентом, поява електронних грошей обумовлюють зростання кіберзлочинів в сфері торгівлі і операцій з кредитними картками, крадіжок персональних даних, паролів доступу[6, с. 114]. За повідомленням начальника департаменту кіберполіції Нацполіції України Сергія Демедюка, протягом 2014–2015 років група кібершахраїв з дванад-

цяти осіб незаконно заволоділа грошовими коштами користувачів інтернету в розмірі 10 млн. гривень. Вони створювали неіснуючі сайти відомих інтернет магазинів в доменних зонах .org, .net. Домени реєструвалися у зарубіжних хостинг-провайдерів. Кіберспекулянти виставляли на цих сайтах фотографії неіснуючих товарів зі сфери електроніки і побутової техніки за цінами, які були на 20–30% дешевше від ринкових пропозицій [7, с. 60].

На формування особи кіберзлочинця також впливають чимало психологічних факторів, зокрема, почуття необмеженої свободи, здатності діяти більш широко порівняно із реальним світом. Одним з криміногенних чинників кіберзлочинності в Україні можна вважати наявність субкультури хакерів і відсутність дієвих заходів, направлених на формування негативного суспільного відношення до кіберзлочинців і їх дій. Характерна для сучасного рівня розвитку інформаційного суспільства в цілому і рівня правового забезпечення діяльності в сфері застосування електронних інформаційних технологій в Україні ситуація, в цілому ж, не сприяє використанню хакерського руху в інтересах суспільного розвитку. Тобто, наша держава, як і більшість країн світу, не знаходить поки що способу використання творчого потенціалу найбільш освічених своїх членів, таких, що найкраще знаються на електронних інформаційних технологіях, що є локомотивом розвитку інформаційного суспільства. У той же час, даним потенціалом усе більш успішно користується професійна злочинність [8, с. 171]. Сучасному українському поколінню невідома настанова про те, що хакери – це не сучасні Робін Гуди і не «борці за свободу», а злочинці. Відсутність соціальної реклами в українських медіа, в рамках проведення широкомасштабних кампаній, а також пропаганди розумного і правомірного використання комп'ютерних технологій, провокує українську молодь, занурену у віртуальне життя, долучатися до субкультури хакерів і ставати на шлях кіберзлочинності [9,с. 336-337].

Отже, у ході нашого дослідження були встановлені наступні детермінанти кіберзлочинності в Україні: відсутність виваженої державної політики у сфері кібербезпеки, низький рівень формування ефективних правоохоронних структур, загострення міждержавних відносин з Російською Федерацією, не захищеність українських Інтернет-банкінгу та online-магазинів, необачне використання українцями електронних грошей, а також активний розвиток хакерської субкультури. Подальший аналіз зазначених факторів, а також вироблення механізмів їх подолання, повинні сприяти становленню кібербезпеки в Укрїіні.

Список використаної літератури:

1. Орлов О. В. Попередження кіберзлочинності – складова частина державної політики в Україні / О. В. Орлов, Ю. М. Онищенко // Теорія та практика державного управління. – 2014. – № 1 (44). – С. 9-16.
2. Стратегія кібербезпеки України : Указ Президента України від 5 березня 2016 року №96/2016 [Електронний ресурс] - Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016.
3. Грицюк Ю. І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання [Електронний ресурс] / Ю. І. Грицюк // Науковий вісник НЛТУ України. – 2016. – Вип. 26.8. – С. 327-337. – Режим доступу: http://nbuv.gov.ua/UJRN/nvnltu_2016_26.
4. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах / О. В. Таволжанський // Журнал східноєвропейського права. – 2016. – №. 31.– С. 80-86 [Електронний ресурс]. – Режим доступу: http://easternlaw.com.ua/wpcontent/uploads/2016/09/tavolzhanskyi_31.pdf.
5. Пивоваров В. В. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання / В. В. Пивоваров, С. Ю. Лисенко // Право і суспільство. – 2016. – № 3(2). – С. 177-182. – Режим доступу: http://nbuv.gov.ua/UJRN/Pis_2016_3%282%29__32.

6. Кривцова М. О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії / М. О. Кривцова // Юридичний науковий електронний журнал. – 2014. – №5. – с.113-116.
7. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності / Н. В. Сметаніна // Міжнародні стандарти з кібербезпеки та їх застосування в Україні : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). – Харків, 2016. – С. 59–61.
8. Горова С. В. Кіберпрофесіонали і кіберзлочинність / С. В. Горова // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2014. – № 2. – С. 170-173. – Режим доступу: http://nbuv.gov.ua/UJRN/boz_2014_2_41.
9. Дзюндзюк Б. В. Особливості субкультури кіберзлочинців [Електронний ресурс] / Б. В. Дзюндзюк // Теорія та практика державного управління. - 2013. - Вип. 2. - С. 333-339. - Режим доступу: http://nbuv.gov.ua/UJRN/Tpdu_2013_2_48.

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

З-68 **Злочинність** у глобалізованому світі : матеріали XVI Всеукр. 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