УДК 343.9.01:004(477)

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ

Черніков Б.Ю.
Національний юридичний університет імені Ярослава Мудрого

У статті розглянуто поняття та ознаки кіберзлочинності. Приділено увагу регулюванню зазначеного питання у міжнародних нормативно-правових актах. Проаналізовано запропоновані науковцями способи вчинення даних злочинів. Надана характеристика особистості кіберзлочинця. Виявлені, описані та проаналізовані соціально-демографічні, кримінально-правові та морально-психологічні риси осіб, засуджених за вчинення кіберзлочинів. Досліджено типи кіберзлочинців.

Ключові слова: кіберзлочинність, способи вчинення кіберзлочинів, психологічні риси осіб, культурно-психологічні фактори кіберзлочинності, латентність кіберзлочинів.

Постановка проблеми. У другій половині минулого століття розвиток суспільних та економічних відносин призвело до значного збільшення інформації, що потребує оброблення, внаслідок чого виникла необхідність у пошуку нових більш ефективних засобі зберігання, обліку, пошуку та обробки цієї інформації, оскільки попередні форми користування інформацією вже не задовольняють потреби суспільства.

Запровадження у сферу управління та інші сфери суспільного життя електронно-обчислюваної техніки дозволило успішно вирішити це завдання, сприяло стрімкому розвитку наукової думки та успішному вирішенню багатьох технічних та соціальних проблем. Однак, це досягнення людства стало використовуватися не лише у корисних для суспільства цілях.

Фактичний розвиток науково-технічного прогресу, пов'язаний із запровадженням сучасних інформаційних технологій, призвело до появи нових видів злочинів, зокрема, до несанкціонованого втручання у роботу ЕОМ, систем і комп'ютерних мереж, викраденню, присвоєнню, вимаганню комп'ютерної інформації, небезпечному антисуспільному явищу, яке отримало назву – кіберзлочинність.

Аналіз останніх досліджень і публікацій. Вивченню питання кібербезпеки та кіберзлочинності в різних аспектах присвячені наукові праці К. Бєлякова, В. Білоус, В. Бутузова, А. Войціховського, О. Волеводза, Д. Гавловського, В. Голубєва, В. Гуславського, М. Литвинова, Е. Рижкова, В. Розовського, Т. Тропиної, В. Цимбалюк, О. Юхно.

Виділення невирішених раніше частин загальної проблеми. Питання кіберзлочинності потребує нового теоретичного аналізу через стрімке впровадження та використання мережі Інтернет та інформаційних технологій у повсякденному житті.

Мета статті. Головною метою статті є дослідження такого явища як кіберзлочинність та осіб, які приймають у ньому участь, їх соціально-демографічні та морально-психологічні риси.

Виклад основного матеріалу. Поняття «кіберзлочинність» часто вживається поряд із поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених термінів поняття «кіберзлочинність» є найширшим та охоплює найбільше коло злочинних посягань у віртуальному середовищі, також його використання регулює міжнародне законодавство [1, с. 173].

Основними ознаками кіберзлочинності є те, що: 1) кіберзлочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху локальними і глобальними комп'ютерними мережами, зберігаються в пам'яті будь-якого фізичного або віртуального пристроїв, спеціально призначених для їх зберігання, переробки та передачі. Крім того, кіберзлочини можуть вчинятися за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може бути як засобом вчинення, так і предметом злочину [2, с. 332]; 2) кіберзлочинність має інтелектуальний характер – здійснення кіберзлочину вимагає певного набору знань, крім того інтелектуальність серед кіберзлочинців пропагується субкультурою хакерів, що дає їм стимул до розумового саморозвитку; 3) кіберзлочини, на відміну від інтелектуальних злочинів, доступні людям невисоких соціальних і вікових можливостей; 4) кіберзлочини є анонімними та неперсоніфікованими; 5) злочинця та жертву можуть розділяти тисячі кілометрів (віддаленість кіберзлочинів); 6) збиток від кіберзлочину часто здається жертві незначним порівняно з процедурою розслідування, яка здатна забрати час, але не гарантує притягнення до відповідальності винного та компенсації збитку (висока латентність кіберзлочинності) [3, с. 8].

23 листопада 2001 року Рада Європи прийняла Конвенцію про кіберзлочинність [4], яка поділяє злочини в кіберпросторі на чотири групи. До першої групи (злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем) належать: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5).

Також до цієї групи злочинів належить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не тільки комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених у статтях 2-5 Конвенції, а і паролі, коди доступу та їх аналоги, за допомогою яких можна увійти до комп'ютерної системи в цілому або до будь-якої її частини (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовуються тільки в тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

До другої групи належать злочини, пов'язані з використанням комп'ютерних засобів: фальсифікація та шахрайство з використанням Інтернет-технологій (статті 7, 8 Конвенцій). Третю групу складають злочини, пов'язані з контентом (змістом) даних. До четвертої групи увійшли порушення авторського та суміжних прав.

Одним із важливих елементів кримінологічної характеристики кіберзлочинності є способи її вчинення. Так, Н. Г. Шурухнов поділяє способи неправомірного доступу до комп'ютерної інформації на такі три групи: способи безпосереднього доступу; способи віддаленого доступу; комплексні способи [5, с. 103-110].

До першої групи належать способи, які в літературі іноді називають "за дурнем" (коли для проникнення у заборонену зону правопорушник, тримаючи в руках предмети – елементи маскування, разом з якоюсь особою проникає до приміщення) та "прибирання сміття" (використання відходів інформаційного процесу – фізичних чи електронних, що залишені користувачем після роботи з комп'ютером) [6, с. 28].

До другої групи способів належать: підключення до телекомунікаційного обладнання, комп'ютерної системи чи мережі; проникнення в комп'ютерні мережі шляхом автоматичного перебирання абонентських номерів із подальшим з'єднанням з тим або іншим комп'ютером; проникнення у комп'ютерну систему з використанням чужих паролів ("непоспішний вибір"); безпосереднє та електромагнітне перехоплення інформації. Останній спосіб ґрунтується на тому, що робота електронних пристроїв (дисплеї, принтери) супроводжується побічними електромагнітними випромінюваннями (так, сигнали з електронно-променевої трубки дисплея можна приймати, записувати й аналізувати на відстані понад 1000 м).

Третю групу утворюють такі способи: уведення в комп'ютерну програму команд, що дають змогу здійснювати незапланові функції ("троянський кінь"); модифікація комп'ютерної програми ("містифікація"); доступ до баз даних і файлів шляхом знаходження слабких місць у системах захисту ("маскарад"); використання помилок і недоліків у комп'ютерній програмі [6, с. 30-32].

Що стосується кримінологічної характеристики особи кіберзлочинця, то має важливе значення, оскільки ефективна, успішна боротьба з кіберзлочинам не можлива без всебічного аналізу образу мислення і особи порушника.

Проведені соціологічні кримінолого-криміналістичні дослідження, зокрема в Австралії, Канаді, США, Німеччині, допомогли розподілити комп'ютерних злочинців на три великі категорії [7]:

1) 11-15 років, вони переважно займаються злочинами з використанням телефонних мереж, кредитних карток та автоматів з видачі готівки;

2) 17-25 років, вони займаються комп'ютерним хакерством;

3) 30-45 років, вони використовують комп'ютери для корисливих цілей та шпигунства.

Так, статистика комп'ютерних злочинів в США за останні 27 років свідчить про те, що більшість (70%) злочинців – це працівники компаній, як мають доступ до ЕОМ. Ця особа, як правило:

- працює компанії не менше 4 років;
- першою приходить і останньою уходить;
- не користується або рідко користується відпустками;
- робить все можливе для завоювання довіри адміністрації, інформує про помилки і проступки інших працівників;
- добре знайома з роботою системи захисту інформації і має ключі від основних замків службових приміщень.

Діапазон рівня спеціалізації освіти правопорушників теж достатньо широкий: від осіб, які володіють мінімальними знаннями користувача, до висококваліфікованих фахівців своєї справи. Крім того, 52% злочинців мають спеціальну підготовку в галузі автоматизованої обробки інформації, 97% – були службовцями державних установ і організацій, які використовували комп'ютерні системи і інформаційні технології, а 30% з них мали безпосереднє відношення до експлуатації засобів комп'ютерної техніки. З дослідницької точки зору цікавим є той факт, що з кожної тисячі комп'ютерних злочинів тільки сім скоєні професійними програмістами. В окремих випадках особи, які вчинили комп'ютерні злочини, взагалі не мали технічного досвіду.

За станом здоров'я ці особи частіше слабо розвинуті, мають певні особливості в фізичній конструкції (худорлявість або зайва вага). Нерухомий спосіб життя часто призводить до серйозних проблем зі здоров'ям. За ознакою зайнятості найбільше в Україні вчиняють злочини працездатні особи, які ніде не працюють і не навчаються (45-50%). Кіберзлочинцям не властивий спеціально-кримінальний рецидив. Його рівень не більше 5%.

Більшість дослідників схиляються до снування такого набору індивідуально-психологічних рис кіберзлочинця: виражені порушення емоційно-вольової сфери; відхилення у психосексуальному розвитку; виражені аутичні прояви у сполученні із соціальним аутсайдерством; користолюбство; мстивість; антигуманна спрямованість; озлобленість; відчуття нерівності чи другорядності; боязкість і лякливість у соціальних та між особистих стосунках; заглибленість у своїх думках, мріях, фантазіях; філософське сприйняття світу; відсутність буттєвих ціннісних орієнтацій; викривлена (збочена) система життєвих цінностей; тотальна недовірливість та виражений цинізм; прагнення уникнути перешкод у подоланні життєвих труднощів. Хоча, для деяких представників може бути характерним активна життєва позиція, нестандартність мислення і поведінки, обережність, уважність. Це може бути

яскрава, мисляча й творча особа, великий професіонал своєї справи, здатний іти на технічний виклик, бажаний працівник.

В залежності від мотивації злочинної поведінки вчені виділяють наступні типи кіберзлочинців.

Корисливий тип. Окрім характерних для звичайного корисного типу злочинця ознак, кіберзлочинці можуть вчиняти злочини для отримання специфічних предметів, що мають особливу цінність у кіберсфері.

Насильницький тип. Не зважаючи на відсутність фізичного контакту, такі насильницькі злочини, як доведення до самогубства або погроза вбивством, можуть бути скоєні за допомогою електронних засобів та мереж. У зв'язку з чисельними самогубствами неповнолітніх, скоєних також під впливом образи або погроз, висловлених за допомогою різноманітних онлайн-сервісів, у США постає питання про можливість кримінальної відповідальності за кіберзалякування та кіберпереслідування для попередження трагічних наслідків.

Сексуальний тип. Для даного типу злочинців характерним є вчинення таких злочинів, як розповсюдження матеріалів порнографічного змісту або предметів, без будь-якої мети, спонукання до дій сексуального характеру, розпусні дії. Ймовірно, що деяких випадках вчинення зазначених дій по відношенню до неповнолітніх матиме місце насильницько-сексуальний тип злочинця.

Соціально дезорганізований тип злочинця, головною метою якого є порушення закріплених законодавчо соціальних норм та здійснення деструктивного впливу на соціум та суспільні відносини.

Ідеологічний або політично мотивований тип. Останнім часом скоєння спеціальних кіберзлочинів стає розповсюдженою формою протесту та полтичної або ідеологічної боротьби. У західних країнах для позначення злочинців спеціального кіберзлочинного типу, які вчиняють злочини з політичних або ідеологічних переконань, використовується термін «хактивіст».

Статусний тип. Злочинці цього типу, вчиняючи злочин, намагаються отримати більш високий неофіційний соціальний статус, здебільше серед представників кіберспільноти.

Дослідницький тип характерний для осіб, які вчиняють спеціальні кіберзлочини. Основою їх мотивацію є вивчення програмних та технічних складових електронних пристроїв та їх мереж, пошук слабких місць, можливостей їх використання та усунення. Зазначені цілі були характерними для перших поколінь мало чисельних хакерів, а також окремих сучасних злочинів, хоча зараз у більшості випадків вони є тільки додатковим мотивом. Злочинці даного типу, в першу чергу, спрямовують свої дії на усунення помилок та розвиток захисту пристроїв та мереж а тому є соціально «корисними». Відповідно до дослідження Орлі Тургеман-Голдшмидт, хакери по-різному пояснюють свою діяльність та цілі, однак, майже всі вони характеризують себе як позитивних девіантів: екстраординарних людей, які розумніші за інших та демонструють незвичайну, кращу поведінку, або, навіть, є носіями суспільних змін. Одним із основних висновків дослідження було те, що хакери не відчувають провини за власні злочинні дії [8].

Отже, кіберзлочинність це міжнародне явище, рівень якого тісно пов'язаний з економічним рівнем розвитку суспільства у різних держаах та регіонах. При цьому Україна має можливість використовувати досвід інших країн, зокрема, дослідження у сфері психофізіологічних властивостей кіберзлочинців з подальшим ефективним запобіганням та викриттям злочинів. А з метою попередження таких злочинів необхідне подальше проведення досліджень соціального та кримінологічного профілю (портрет) типового комп'ютерного злодія.

Список літератури:

1. Іванченко О. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні // Актуальні проблеми вітчизняної юриспруденції. – 2016. – № 3. – С. 172-177.
2. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.
3. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. 12 с.
4. Конвенція про кіберзлочинність від 23 листопада 2011 року.
5. Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. – М.: Щит-М, 1999. – 254 с.
6. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юрид. лит., 1991. – 160 с.
7. Сабадаш В.В. Компьютерная преступность – проблемы латентности.
8. Orly Turgeman-Goldschmidt. Meanings that Hackers Assign to their Being a Hacker. URL: http://www.cyber-crimejournal.com/Orlyijccdec2008.pdf.

Черников Б.Ю.
Национальный юридический университет имени Ярослава Мудрого

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПНОСТИ

Аннотация
В статье рассмотрено понятие и признаки киберпреступности. Уделено внимание регулированию данного вопроса в международных нормативно-правовых актах. Проанализированы предложенные учеными способы совершения данных преступлений. Предоставлена характеристика личности киберпреступника. Выяснены, описаны и проанализированы социально-демографические, криминально-правовые и морально-психологические черты лиц, осужденных за совершение киберпреступлений. Исследовано типы киберпреступников.
Ключевые слова: киберпреступность, способы совершения киберпреступлений, психологические черты лиц, культурно-психологические факторы киберпреступности, латентность киберпреступлений.

Chernikov B.Y.
Yaroslav Mudryi National Law University

CYBERCRIME CRIMINOLOGICAL CHARACTERISTICS

Summary
The article deals with the concepts and features of cybercrime. The attention was paid to the regulation of this issue in international legal acts. The methods of committing these crimes proposed by scientists are analyzed. The characteristic personality cyber criminal. Identified, described and analyzed socio-demographic, criminal and moral-psychological characteristics of person convicted of committing cybercrimes. The types of cybercriminals are investigated.
Keywords: cybercrime, ways of committing cybercrime, psychological traits of people, cultural and psychological factors cybercrime, latency of cybercrime.