УДК 343.9.01

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНЦЯ

CRIMINOLOGICAL CHARACTERISTICS OF THE CEBERCRIMINALS

Ткачова О.В.,
к.ю.н., доцент кафедри
кримінології та кримінально-виконавчого права
Національний юридичний університет імені Ярослава Мудрого

Науменко К.В.,
студентка факультету адвокатури
Національний юридичний університет імені Ярослава Мудрого

У статті розглядаються основні ознаки кіберзлочинців, а також наводиться їх класифікація та відмінні риси. На основі їхніх особливостей сформовані ключові ознаки кіберзлочинця, які допоможуть полегшити правоохоронним органам роботу з пошуку і розкриття злочинів, скоєних кіберзлочинцями.
Ключові слова: кіберзлочинність, психологія кіберзлочинності, комп'ютерні злочини, інформаційні злочини, боротьба з кіберзлочинністю.

В статье рассматриваются основные признаки киберпреступников, а также приводится их классификация и отличительные характеристики. На основе их особенностей, сформированы ключевые признаки киберпреступника, которые помогут облегчить правоохранительным органам работу по поиску и раскрытию преступлений, совершаемых киберпреступниками.
Ключевые слова: киберпреступность, психология киберпреступности, компьютерные преступления, информационные преступления, борьба с киберпреступностью.

The article analyses the main features of cybercriminals, as well as their classification and distinctive characteristics. Based on these characteristics, key signs of cybercrime are formed that will help to facilitate the work of law enforcement agencies in the search for and disclosure of crimes committed by cybercriminals. The social danger of cybercriminals, the nature of their activities, ways of interaction with people and with each other, as well as the features of thinking and the psychological attitude to the victim are considered. The authors note the high level of latency of cybercriminals and the need for active actions to disclose cybercrime. Also, specific ways of preventing cybercrime are given. The article points out that the most dangerous cybercriminal, worthy of attention and close scientific study, is a man with superhigh intellectual abilities, an extremely high level of planning and preparation for crime, extensive knowledge in the field of computer security. Such a criminal has a high degree of public danger. The most serious computer attacks are committed by groups of cybercriminals, so you need to monitor their communication. At the scientific level, the authors propose further research of cybercriminals according to the criterion of their passivity or activity, as well as the types of crimes that they are commit. Attention is drawn to the fact that science needs further research on these criminals at the scientific and practical levels in order to create a universal portrait of a cybercrime. A clear statement of the internal and external characteristics of the crime subject allows you to predict his actions, think just like him, and know in advance the next steps of the cybercriminal. Understanding the portrait of a cybercrime facilitates its identification, allows you to suspend committed crimes and planned cybercrime. The result of research and disclosure of crimes will be a decrease in the level of latency of cybercrime. The article discusses the need for common actions of specialists in the field of computer security, psychologists and criminologists, in order to achieve the greatest effectiveness in research. Sharing experience and cooperation at the global level, further strengthening the protection of data, access and funds – should become a common practice throughout the world. The results of this study have a practical importance for identifying the problem of avoiding criminal liability by cybercriminals and disclosing cybercrime.
Key words: cybercrimes, psychology of cybercrimes, computer crimes, information crimes, combating cybercrime.

Тотальна технологізація суспільства, що не може за своїми темпами бути стримана владою держав чи міжнародної спільноти, призвела до зростання кількості кіберзлочинів. Це обумовлює потребу вивчення особи кіберзлочинця з метою наступного попередження злочинів у цій сфері, яка наразі є недостатньо вивченою та мало відомою. Надвисокий рівень латентності кіберзлочинів вказує на прогалину у вивченні даної особи злочинця, тому автори даної статті поставили собі за мету максимальне розкриття портрета особи-кіберзлочинця. Наслідком такого вивчення є більш глибоке уявлення про фізичні, соціальні, емоційно-психологічні прояви даного суб'єкта, що полегшуватиме його наступну ідентифікацію та розкриття злочинів у мережевому просторі.

Попередньо характеристика такого суб'єкта вже надавалася наступними вченими: А. Н. Косенковим, Г. А. Чорним, Л. В. Борисовою, О. М. Кравцовою, С. М. Лозовою, О. А. Севідовим та іншими. Так, А. Н. Косенков та Г. А. Чорний зазначають, що особам кіберзлочинців притаманні такі ознаки, як: відсутність відчуття нанесення шкоди через подовження ланцюгу злочинець-жертва на злочинець-мережа-жертва; зменшене відчуття страху чи дискомфорту; віра у свою геніальність; відчуття подвоєної реальності [1]. Л. В. Борисова стверджує, що кіберзлочинці є поширеною групою, яка включає у себе як високоінтелектуальних представників, так і дилетантів, а також осіб абсолютно різного роду професії [2, с. 76–80]. О. М. Кравцова зазначає про переважну наявність вищої освіти у таких осіб, статусу не одружених, схильності до авантюризму, що не сприяє зміцненню їхніх сімейних стосунків і поділяє всіх кіберзлочинців на три групи: А) тих, що вчиняють кіберзлочини у зв'язку із професійною діяльністю; Б) з метою незаконного збагачення; В) з особистих некорисливих мотивів [3, с. 46–53]. С. М. Лозова зауважує про прояви делінквентної поведінки, ескапізму та адикції у кіберзлочинців [4]. Делінквентна поведінка співвідноситься як частина та ціле із девіантною поведінкою і проявляється як загальна асоціальна спрямованість та схильність до порушення правил людського співжиття та вчинення правопорушень. У свою чергу, ескапізм проявляється у кіберзлочинців як втеча від дійсності, прагнення піти від реальності, від загальноприйнятих норм суспільного життя у світ ілюзій та псевдодіяльності. Натомість, особа, яка захоплена чимось у реальному житті навряд чи зможе стати сильним спеціалістом у галузі ІТ-технологій, оскільки вона не матиме на це достатньо сил та внутрішньої мотивації. Адикція, яка залежність від мережевого світу у кіберзлочинця, може мати навіть прояв хворобливого стану, коли потяг до проведення усього часу у комп'ютерному просторі призводить до нехтування усіма іншими проявами матеріального та соціального життя.

У загальному вигляді під кіберзлочинами міжнародна спільнота розуміє: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання

пристроями, пов'язані із комп'ютерами підробки та шахрайство, всі види забезпечення обігу та використання дитячої порнографії за допомогою комп'ютерної мережі, а так само порушення авторських та суміжних прав [5]. Як ми бачимо, ООН розуміє під явищем кіберзлочинності будь-які злочини, що вчиняються у комп'ютерній мережі або за допомогою неї і не має на увазі виключно складні кіберзлочини вищого порядку, що потребують для їхнього вчинення надвисоких інтелектуальних здібностей чи довготривалого планування. На нашу ж думку, при характеристиці особи кіберзлочинця слід виходити із розмежування наявних видів кіберзлочинів за формою прояву злочинного діяння на активні та пасивні. До активних науковці відносять: кібертероризм, погрозу фізичної розправи, кіберпереслідування та кіберсталкінг. До групи пасивних: кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство та поширення спаму і вірусних програм [6]. Останні поділяються на підвиди: хакери (hackers); кракери (crackers): «вандали», «жартівники», «зломщики»; кардери (carders); фішери (fishers); спамери (spammers); фрікер (phone + break = phreak); кіберкруки (cybercrooks); комп'ютерні пірати [7]. В ідеалі особу кіберзлочинця треба характеризувати щодо кожного окремого різновиду злочинів у кожній із груп, оскільки специфіка вчинення, мотивація та рівень професіоналізму у сфері комп'ютерних технологій та комп'ютерної безпеки значно відрізняється для кожного із них. Так, наприклад, поширення спаму та вірусних програм досить рідко вчиняється особами високого рівня професіоналізму, здебільшого цей вид притаманний неповнолітнім особам з метою розваг чи звичайної цікавості. Даний вид злочину може бути вчинений особами взагалі без знань принципів комп'ютерної безпеки, лише шляхом слідування крокам, розписаним на форумах та сайтах хакерів та крекерів. Цей вид у більшості є примітивним (так званий загальний кіберзлочинний тип) [1] та не є небезпечним, бо частіш за все жертвою такого злочину для підлітка може стали лише посередній сайт із низьким чи взагалі відсутнім рівнем захисту. У виключних випадках цей злочин може бути вчинено особами надвисокого рівня професіоналізму у злочинних цілях, яким і слід приділяти увагу. Ми бачимо, що особи злочинця зовсім різні щодо навіть одного виду злочину, що вже казати про загальну характеристику активних та пасивних груп чи кіберзлочинця у цілому.

Більш за все деякі спільні та відмінні риси кіберзлочинця буде доречно представити у вигляді наступної таблиці.

Критерій	**Спільне**	**Відмінне**	
		Активний кіберзлочинець	Пасивний кіберзлочинець
Фізіологічна характеристика	– Можливі аутистичні розлади, як, наприклад, синдром Аспергера – вік більшості від 21-40 років – ескапізм, адикція, делінквентна поведінка	– фізичний стан частіше незадовільний, часто надмірна вага – статева приналежність: майже завжди чоловіки	Даний критерій майже не можливий до застосування. Фізичне обличчя не можливо визначити. Це може бути як чоловік, так і жінка, будь-якого віку, фізичної статури та як з наявністю фізичних вад, так і з їхньою відсутністю
2. Психо-емоційна складова	– високі та надвисокі Інтелектуальні здібності – посидючість – здатність чекати роками результат власних дій (оскільки час від винайдення уразливих елементів системи та проникнення у неї до моменту використання проникнення на власну користь може скласти не один рік) – бажання поглузувати з уразливості систем, певним чином самоствердитися – почуття вищості та самолюбства – скритність	– більший ступінь емоційної уразливості, імпульсивність – здатні піти за емоціями через певну неврівноваженість – високі розумові здібності у поєднанні із порівняно низьким рівнем самоконтролю – нездатність до довгострокового планування дій	– здатність до самоорганізації – високі вольові показники – здатність до самодисцип- ліни – надвисокий самоконтроль – керуються суто логікою, їх майже неможливо спровокувати на емоційний збій (це – людина-машина) – багата фантазія та скритність – винахідливість – зацікавленість сферою діяльності та постійне вивчення нових методів проникнення у комп'ютерні системи – лідерські здібності
3. Мотивація та тип	– наявна корислива мета майже й всіх злочинах – отримати гроші, (вплив на процеси на фінансових ринках, біржах); отримати ігрові засоби чи викликати інші суспільні процеси (інфляції, девальвації тощо).	– домінуючий мотив і тип – насильницький	– домінуючий мотив і тип - корисливий – доволі часто зустрічається загальна цікавість та так званий "спортивний інтерес"
4. Соціальна модель поведінки	– часто виявляються працівниками корпорацій, комп'ютерну безпеку і вторгнення до яких здійснюють (слід починати шукати «серед своїх») – переважно через те, що порушити безпеку системи, з якої ти знайомий, набагато легше, аніж декілька років занурюватися у нову – часто хаотичні у побуті -використання професійного жаргону	– боягузтво у поєднанні з бажанням протиставити себе загальній масі суспільства – схильність до інтроверсії та недовірі суспільству – соціальна дезадаптація долається активністю у мережі	– як інтроверти, так і екстраверти – модель поведінки не простежується, бо можуть бути і компанійськими, і усамітненими – можуть бути спеціалістами декількох не обов'язково суміжних галузей (наприклад, програміст-бухгалтер, хакер-чиновник тощо) – прискіпливі до деталей, перепитують та роблять зауваження(програмування вимагає доведення коду до ідеалу та відсутності будь-яких помилок, що і обумовлює їхній максималізм та ідеалізм в усьому)
5. Групова злочинна діяльність	Зустрічається в обох видах, проте із різною частотою	– зустрічається вкрай рідко через загальну схильність особи до інтроверсії -можлива переважно у таких видах злочинів, як кібертероризм	– зустрічаються доволі часто кримінальні організації, які є найбільш ефективним та надпрорахованим способом діяльності, що рідко зали- шає жертві та правоохорон- ним органам шанси до від- найдення злочинця, проте зовсім не виключаються випадки «вдалого» скоєння злочину і одноосібно

Як ми бачимо, є доволі суттєва різниця у портреті особи кіберзлочинця залежно від форми прояву її злочинної поведінки. Слід підсумувати, що, на нашу думку, категорія активних злочинців більш легка для вивчення, оскільки їм притаманна більша кількість характерних ознак звичайного злочинця у насильницькому типі злочину, а саме: певна психо-емоційна неврівноваженість, яка й породжує цілі переслідування чи домагання осіб через мережу Інтернет (всі прояви кіберсталкінгу), погроз розправи та насильницьких дій щодо окремої особи чи груп осіб (може мати місце погроза насильством щодо великих груп населення).

Відмінності між цими особами є досить глибинними і полягають не лише у мотивації і фізичному прояві. Через те, що пасивного кіберзлочинця ідентифікувати надто складно і його портрет є розмитим, пропонуємо сприймати кіберзлочинця активних видів злочинів як фізичну особу, яка має свій набір характеристик, як і у будь-якому іншому виді злочинів. А особу пасивного кіберзлочинця, навпаки розглядати не як особистість, бо це може взагалі не дати результатів в її пошуку, а як загальне сукупне явище, яке має приблизний набір характеристик, які не можуть бути визнані остаточними чи стовідсотково вірними, оскільки особа кіберзлочинця найвищого рівня (який і є найбільш небезпечним) майже не відома людству.

Крім того, до портрета особистості кіберзлочинця слід додати наступні загальні для всіх них характеристики: філософський склад розуму; дезорганізуючий тип злочинця; особливе відношення до жертви; особливий тип мотивації; специфічна взаємодія з особами свого роду діяльності; обумовленість місця проживання певною місцевістю; необхідна наявність матеріально-технічної забезпеченості; галузі переважної зайнятості для відвернення уваги. Розглянемо кожну ознаку окремо.

Філософський склад розуму. Схильні мати власні погляди на життя, бажано якомога більше відмінні від загальної маси людей, щоб протиставити себе та таким чином самовиразитися. Так само, відмінні цінності життя, наприклад, небажання мати сім'ю та одружуватися як засіб «захисту» своєї психологічної свободи, небажання підлаштовуватися під будь-кого, безкомпромісність та крайній егоцентризм. Філософські концепції у поєднанні із високим інтелектом дають такій особі можливість обґрунтовувати будь-які свої злочинні та асоціальні погляди, позиціювати їх як єдино вірні та не сприймати сторонніх поглядів. Проте, це скоріш є переважним напрямом їхніх думок, аніж аксіомою і не може бути віднесене до всіх представників. Винятком є Євген Богачов, що за показаннями засудженого Сполученими Штатами Америки хакера Олександра Паніна одружений та має двох дітей.

Дезорганізуючий тип злочинця. Полягає у зухвалому відношенні до правопорушення. Особа вважає винною саму жертву, оскільки уразливість систем комп'ютерної безпеки є її прогалиною, а пряме втручання у неї та злам розглядається як своєрідна допомога покращити захист жертви або суцільна відсутність емпатії до неї, оскільки норми співжиття нею ігноруються. Даний тип особи вважає будь-які стандарти адекватної поведінки, визнані суспільством, як нав'язані стереотипи, що заважають кіберзлочинцю, розцінюються як безглузді прояви стадності і нехтуються.

Особливе відношення до жертви. Часто кіберзлочинці пов'язані із жертвами трудовими відносинами. Пов'язаність може проявлятися у займанні як керівних, так і підлеглих посад. Керівники мають доступ до системи і часто розуміються на комп'ютерній безпеці або фінансових операціях. Підлеглі можуть бути «невизнаними геніями», які займають, наприклад, посаду системного адміністратора чи бухгалтера. Це значно полегшує їм вчинення злочину. Особа, яка працює досить довго із певною системою і має доступ до неї, в якийсь момент використовує доступ або виявлену уразливість системи та обертає її на свою користь з різних мотивів. У деяких випадках вибір жертвою компанії, в якій кіберзлочинець працює не пов'язаний з прямим бажанням завдати шкоду саме цій компанії, іноді це бажання «набити руку» на ній, отримати досвід для вчинення наступних більш серйозних діянь.

Особливий тип мотивації. Мотивом вчинення кіберзлочину для такої особи може бути багатий спектр варіантів. Для активних кіберзлочинців це переважно насильницька мотивація, що обумовлена психоемоційними розладами сексуального характеру та нав'язливими ідеями (наприклад, помста). Для пасивної категорії – бажання збагатитися, самоствердитися, проявити творчі здібності або звичайна цікавість, поєднана із зухвалістю.

Специфічна взаємодія з особами свого роду діяльності. Асоціальна поведінка, часта відсутність прямого спілкування з людьми компенсується кіберзлочинцями через віртуальну взаємодію. Між собою вони спілкуються через закриті форуми під псевдонімами. Основна мета такого спілкування самоствердження та розповсюдження інформації практичного та теоретичного характеру. Злочинці обмінюються інформацією про те, яким чином вони зламали та якою уразливістю системи скористалися. Поширеним є надання інструкцій для зламу та порад щодо методів проникнення у систему.

Обумовленість місця проживання певною місцевістю. У цілому можна поділити кіберзлочинців за критерієм їхнього місцезнаходження на тих, що працюють із місць позбавлення волі та тих, хто знаходиться «на волі». Перші маючи багато вільного часу, опановують професію під час відбування покарання за якийсь інший злочин (рідше за вчинення саме кіберзлочину). Тут є навички та інтелектуальні здібності, є матеріально-технічна забезпеченість засудженого через власні канали забезпечення (знайомства з контрабандистами; приховані від слідства та суду матеріальні ресурси, що залишилися після попередніх злочинів тощо). Другі здійснюють свою діяльність не з будь-якого місця. Це може бути мегаполіс або курортна зона. Мегаполіс дозволяє переховуватися та змінювати місце перебування, щоб не стати віднайденим (Лос-Анджелес, Гонг-Конг, Шанхай). Також, слід враховувати країни з високим рівнем освіти (переважно Росія, Україна, Великобританія та США). Загалом країни найбільшої локації – це Росія, США, Нідерланди, Франція, Німеччина, Індонезія та Тайвань. Серед детермінант вибору саме цих країн є: політична та економічна нестабільність, комерційні замовлення організаторів злочинів щодо цих країн, де містяться великі матеріальні ресурси; досить вільне законодавство, яке дозволяє кіберзлочинцям у цих країнах переховуватися та залишатися не поміченими; високий рівень освіти у поєднанні із високим рівнем безробіття, а також зменшення фінансування на забезпечення комп'ютерної безпеки. Ці детермінанти існують окремо одна від одної і не обов'язково повинні мати місце у своїй сукупності.

Необхідна наявність матеріально-технічної забезпеченості. Матеріальна забезпеченість не має значення майже завжди. Доступ до мережі та комп'ютер є достатнім матеріальним забезпеченням у більшості випадків. Необхідним є лише ресурс знань та терпіння. Великі матеріальні та технологічні ресурси можуть бути необхідними лише злочинцям, які здійснюють Dos-атаки (Denial of Service) та DDos-атаки (Distributed Denial of Service). Такі атаки коштують дуже дорого, потребують значного матеріального забезпечення (серверів, системні ресурси тощо). Серйозні Dos- та DDos-атаки за своєю вартістю можуть бути профінансовані лише державами. Це дає розуміння, що сам кіберзлочинець буде у такій ситуації скоріше виконавцем, аніж організатором та працюватиме у складі цілої групи (використовується значний людський ресурс).

Галузі переважної зайнятості для відвернення уваги. Тут слід поділяти за двома можливими варіантами: якщо особа щодо жертви має внутрішнє походження (співпра-

цюють), то це як правило програмісти, системні адміністратори, інженери тощо, фінансові директори, головні бухгалтери та провідні економісти компанії. Якщо ж мова йде про зовнішніх злочинців (жертва не відома з особою), то тоді це може бути будь-який рід професії, який займатиме не багато часу і залишатиме можливість у вільний час займатися основним своїм видом діяльності.

При вирішенні питання про притягнення осіб до відповідальності за кіберзлочини, також слід враховувати, що хворобливі стани, на кшталт, синдрому Аспергера, що мають прояв у даних суб'єктів дозволяють їм уникати кримінальної відповідальності за вчинене (випадок із Райаном Клірі з LulzSec). Слід зазначити, що, оскільки такі стани встановлюються правоохоронними органами вже після ідентифікації особи на стадії пред'явлення їй обвинувачення або судового розгляду, то існує імовірність симулювання даних станів з метою ухилення від покарання. Тому, слід більш ретельно перевіряти їх наявність, аби не давати кіберзлочинцю шансів на введення в оману.

Суспільна небезпечність. Жертвами даного виду злочинності є не лише окремі особи чи їхні групи, а установи, організації та цілі держави. Небезпечність виявляється у заподіянні шкоди, яка має матеріальний та моральний вияв. Матеріальна шкода проявляється у прямих збитках, завданих викраденням коштів із рахунків осіб чи установ, у збитках на відновлення нормальної роботи комп'ютерних програм, серверів, систем обслуговування клієнтів. Моральна шкода, у свою чергу, виявляється у стражданнях особи, завданих розголошенням приватної інформації, яка стала відомою внаслідок злому доступу до останньої, у зв'язку зі знищенням чи пошкодженням її майна; приниженням честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи. Особливістю суспільної небезпечності даного виду злочинів є масштаб заподіюваної шкоди, а саме її масовість. За допомогою комп'ютерних технологій можливим є одночасне отримання доступу до конфіденційної інформації та матеріальних ресурсів великої кількості осіб. Одним із прикладів є викрадення коштів з рахунків клієнтів конкретного банку, у системі безпеки якого було віднайдено уразливість. Шкода може бути виражена у: викраденні коштів вузької групи осіб, які володіють ними у великій кількості або викраденні порівняно невеликих сум, проте з рахунків чисельної групи осіб. Тут так само враховуємо пряму (викрадені кошти) та опосередковану (втрата прибутку банківської установи через відтік клієнтів) шкоду, а також більш широке сприйняття поняття жертви, до якої відносимо не лише осіб, що втратили матеріальні цінності, а й тих, що були звільнені через факт злочину, втратили дохід внаслідок банкрутства установи або втрати ділової репутації тощо. Небезпечність так само має прояв у своїй латентності. Через здатність злочинців не бути віднайденими і покараними, загублюватися у мережевому просторі, мають місце не лише зростання привабливості даного виду діянь для осіб зі злочинного світу і, як наслідок, підвищення кількості фактичних злочинів даного виду, а й зростання: кількості жертв, вірогідності заподіяння шкоди кожній особі, переростання загрози у глобальні масштаби (втручання у системи обігу коштів Міжнародного валютного фонду, Банку міжнародних розрахунків, Азійського банку розвитку та інших). Наступним підґрунтям небезпечності цих злочинів є надвисока швидкість розвитку нових технологій та способів атаки серверів, обернення конфіденційної інформації у власних злочинних інтересах та приховування злочинів.

Запобігання та протидія кіберзлочинності. Головним заходом запобігання є захист комп'ютерних програм, баз даних, рахунків, якомога частіше оновлення даних та способів захисту доступу до серверів і паролів. Щоб не стати жертвою кіберзлочину потрібно постійно оновлювати власні підходи до комп'ютерної безпеки, збільшувати фінансування спеціалістів у даній сфері, проводити масові заходи з ознайомлення населення з діями правопорушників, попереджати про необхідність більш сумлінної поведінки та обережності у розголошенні інформації, яка уможливлює чи полегшує втручання до власності осіб. Розвиток запобігання повинний відбуватися за умови співробітництва всіх країн світу, оскільки глобальний характер шкоди від кіберзлочинів вже давно зробив останні проблемою людства, а не окремої країни. Лише завдяки оперативному обміну досвідом, напрацюваннями, нововиявленою інформацією про злочинні групи та їхні дії, можливо ефективно припиняти злочини. Щодо запобігання, то тут важливим і необхідним є подальше ускладнення процесів ідентифікації користувачів у банківських кабінетах та ускладнення процедур підтвердження особи і збереження відомостей щодо неї. Так само важливою є правова допомога державних та міждержавних правоохоронних органів у розслідуванні кіберзлочинів. Неможливим є запобігання та припинення кіберзлочинів без наявного складу висококваліфікованих працівників правоохоронних органів, які у співробітництві зі спеціалістами у сфері комп'ютерної безпеки вживатимуть заходів із поєднання знань комп'ютерних технологій та практики розслідування і проведення слідчих дій, будуть направляти усі зусилля на виведення кіберзлочинів зі складу латентних та допомагати притягати до відповідальності усіх винних осіб. Надвисокий рівень латентності кіберзлочинів робить вкрай складним стовідсоткове запобігання ним і перетворює роботу правоохоронних органів на процес надолуження сучасних методів злочинних дій, аналіз їхніх механізмів та припинення вже вчинюваних правопорушень. У розрізі цього питання більш доцільно казати саме про припинення вже існуючих злочинних дій як таких, що у багатьох випадках не можуть бути заздалегідь передбачені і попереджені через недостатній рівень підготовки спеціалістів. Припинення полягає у структурному аналізі кола відносин злочинців, їхніх дій, які слід перебудовувати у логічні ланцюги, що дозволяє відстежити хід вчинюваних дій та зрозуміти кінцеву мету. Наступним кроком є заповнення логічного ланцюгу елементами, яких не вистачає особам для досягнення злочинної мети і припинення цих дій до настання негативних наслідків.

Підсумовуючи вище викладене, можна сказати, що особа кіберзлочинця розглядається міжнародним співтовариством у широкому сенсі. Проте, найбільш небезпечний кіберзлочинець, що заслуговує уваги та ретельного вивчення – це особа, що має надвисокі інтелектуальні здібності, ультрависокий рівень спланованості і підготовки злочину, великі знання у галузі комп'ютерної безпеки та приймає участь у вчиненні злочину із великим рівнем суспільної небезпечності. Найбільш серйозні атаки вчиняються групами кіберзлочинців, тому слід відстежувати їхню комунікацію. На науковому ж рівні, пропонуємо надалі розмежовувати кіберзлочинців за критерієм пасивності або активності вчинюваних ними кіберзлочинів. Наголошуємо на потребі подальшого вивчення даних злочинців на науковому та практичному рівні з метою винайдення найбільш універсального портрета особи кіберзлочинця. Чітке уявлення внутрішніх та зовнішніх характеристик суб'єкта злочину дає можливість прогнозувати його дії, мислити як він та усвідомлювати наперед його кроки. Це полегшує його ідентифікацію, дає можливість припиняти вчинювані та попереджувати плановані кіберзлочини. На масштабному рівні це дозволить поступово вивести кіберзлочини із категорії латентних. Щодо заходів запобігання та припинення кіберзлочинів, то тут вкрай важливим є залучення висококваліфікованих спеціалістів, обмін досвідом та співробітництво на глобальному рівні, постійне посилення захисту даних, доступів та коштів.

ЛІТЕРАТУРА

1. Общая характеристика психологии киберпреступника / А. Н. Косенков, Г. А. Черный. Криминологический журнал БГУЭП № 3 (21), III квартал 2012.
2. Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні і психофізіологічні аспекти. Актуальні проблеми держави і права. 2008. Вип. 44.
3. Кравцова М. О. Сучасний кіберзлочинець: кримінологічна характеристика особистості. Митна справа. 2015. Вип. № 4 (100).
4. Лозова С. М. Деякі особливості психічних девіацій кіберзлочинця. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/180/Aktual_p1tan_rozsl_kiberzloch_2013.pdf?sequence=1&isAllowed=y
5. Конвенція про кіберзлочинність. URL: http://zakon0.rada.gov.ua/laws/show/994_575/page
6. Кримінологія: підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін.; за ред. В. В. Голіни, Б. М. Головкіна. Х.: Право, 2014. С. 294.
7. Севідов О. А. Криміналістична класифікація суб'єктів кіберзлочинів та їх особливості. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/180/Aktual_p1tan_rozsl_kiberzloch_2013.pdf?sequence=1&isAllowed=y

УДК 343.615.5 (477)

КРИМІНАЛІЗАЦІЯ ДОМАШНЬОГО НАСИЛЬСТВА В УКРАЇНІ

CRIMINALIZATION OF DOMESTIC VIOLENCE IN UKRAINE

Яїцька Д.І.,
студентка 3 курсу
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена аналізу елементів складу домашнього насильства, криміналізованого Законом України № 2227-VIII від 6 грудня 2017 року. Поштовхом до внесення змін до Кримінального кодексу України стала ратифікація Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу з цими явищами. До цього насильство, вчинюване у сім'ї, жодним чином не виокремлювалося серед інших видів насильства. Автором досліджено особливості елементів складу злочину, передбаченого ст. 126-1 Кримінального кодексу України, а також проаналізовано види насильства, що входять до складу. У статті порівнюється зміст домашнього насильства в українському законодавстві та міжнародних нормативно-правових актах, аналізується практика кваліфікації насильства у сім'ї до внесення змін та оцінюються перспективи застосування нових положень Кримінального кодексу України у майбутньому.

Ключові слова: злочини проти життя і здоров'я особи, домашнє насильство, економічне насильство, насильство стосовно жінок, тілесні ушкодження.

Статья посвящена анализу элементов состава домашнего насилия, криминализованного Законом Украины от 6 декабря 2017 года. Толчком к внесению изменений в Уголовный кодекс Украины стала ратификация Конвенции Совета Европы о предотвращении насилия в отношении женщин и домашнего насилия и борьбе с этими явлениями. До этого насилие, совершаемое в семье, никоим образом не выделялось среди других видов насилия. Автором исследованы особенности элементов состава преступления, предусмотренного ст. 126-1 Уголовного кодекса Украины, а также проанализированы виды насилия, входящих в этот состав. В статье сравнивается содержание домашнего насилия в украинском законодательстве и международных нормативно-правовых актах, анализируется практика квалификации насилия в семье до внесения изменений и оцениваются перспективы применения новых положений Уголовного кодекса Украины в будущем.

Ключевые слова: преступления против жизни и здоровья человека, домашнее насилие, экономическое насилие, насилие в отношении женщин, телесные повреждения.

The article is devoted to the analysis of elements of the composition of domestic violence, criminalized by the Law of Ukraine of December 6, 2017. The impetus for amending the Criminal Code of Ukraine was the ratification of the Council of Europe Convention on the Prevention of Violence Against Women and Domestic Violence and the fight against these phenomena. Prior to that, violence committed in the family, in no way stood out among other types of violence. The author investigates the features of elements of the composition of domestic violence, as well as analyzes the types of violence that are part of the composition. The article compares the content of domestic violence in Ukrainian legislation and international normative and legal acts, analyzes the practice of qualifying domestic violence before introducing changes, and assesses the prospects for applying the new provisions of the Criminal Code of Ukraine in the future.

Prior to the latest changes to the Criminal Code of Ukraine, courts considered criminal offenses committed in connection with the use of violence in the family, depending on the type of violence, the nature of its consequences: 1) physical violence – crimes against the life, health, personal will of the victim; 2) sexual violence – crimes against sexual freedom and sexual inviolability; 3) economic violence – avoiding payments, crimes against property; 4) psychological violence – a variety of threats, including the threat of murder. The court almost never took into account the history of domestic violence and did not take into account that such violence could have existed for years and the committed crime is an episode in long-term mockery of the family.

From now on, economic violence is criminalized. It includes willful deprivation of housing, food, clothing, other property, money and documents, obstruction of obtaining necessary treatment or rehabilitation services, prohibition of work, forced labor, prohibition of study and other economic offenses. Economic violence in the family is expressed in a kind of economic pressure.

Domestic violence as a component of a crime has its own characteristics in relation to the subject. In our opinion, it is necessary to talk about a special victim of a crime. Such victims can be real or former spouses or a person with whom the perpetrator is (was) in family or close relationships.

The article focuses on the interpretation of the actions that are part of the objective side of domestic violence, the characteristics of the subject and the victim, the advantages and disadvantages of changes introduced in the Criminal Code of Ukraine are called.

Key words: crimes against the life and health of the individual, domestic violence, economic violence, violence against women, bodily harm.