УДК 343.543

Шеломенцев Володимир Петрович — головний науковий співробітник Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук

Організована кіберзлочинність: до визначення поняття

Стаття присвячена визначенню поняття організованої кіберзлочинності. Розглядаються характерні риси організованої злочинної діяльності у кіберпросторі.

Ключові слова: кіберпростір, кібернетичні комп'ютерні системи, мережа Інтернет, кіберзлочини, організоване злочинне кіберугруповання.

Процеси глобалізації та інформатизації всіх галузей людської діяльності впливають і на таку сферу, як злочинна діяльність — з'являються нові види й способи злочинних посягань, злочинність освоює середовище комп'ютерних мереж, змінюються форми прояву організованої злочинності.

Криміналізація суспільства обумовлює поширення організованої злочинності у середовищі глобальних інформаційних мереж, які давно вже перетворилися в електронний аналог суспільного життя. В той же час, аналіз діяльності правоохоронних органів у глобальних інформаційних мережах (зокрема у мережі Інтернет) свідчить, що організаційно-правове забезпечення протидії організованій кіберзлочинності в Україні не відповідає вимогам сьогодення через відсутність науково-обґрунтованих методів боротьби з даним видом злочинності.

Тому важливою умовою підвищення ефективності протидії організованій злочинності у середовищі глобальних інформаційних мереж стає знання специфіки злочинних процесів, пов'язаних з його функціонуванням.

Окремі питання організованої злочинності у середовищі глобальних інформаційних мереж розглядалися у працях вітчизняних і зарубіжних науковців: В. М. Бутузова, О. Ф. Долженкова, В. Д. Гавловського, М. В. Гуцалюка, В. С. Цимбалюка, Л. Шеллі, Ф. Уільямса та інших.

Однак, основну увагу дослідників було зосереджено на проявах традиційної організованої злочинності у середовищі глобальних інформаційних мереж.

У той же час, поширення глобальних інформаційних мереж та розвиток системи суспільних відносин в їх середовищі призвели до появи такого феномену, як кіберзлочинність.

У науковій літературі висвітлювалися лише окремі аспекти організованих форм кіберзлочинності, відмічається відсутність визначення поняття організованої кіберзлочинності, яке має важливе теоретичне і практичне значення для подальшого вдосконалення правотворчої та правозастосовної діяльності.

Зважаючи на вищенаведене, в даній статті ставиться за мету визначити поняття організованої кіберзлочинності та розглянути характерні риси організованої злочинної діяльності у кіберпросторі.

Розглядаючи організовану кіберзлочинність як підвид загальної організованої злочинності, доцільно взяти за основу традиційне визначення організованої злочинності у чинному законодавстві України — це сукупність злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань [1].

При цьому відмітними ознаками організованої кіберзлочинності є: сукупність злочинів певного виду — кіберзлочинів; специфічне середовище діяльності особливих організованих злочинних угруповань — кіберпростір; особливі форми організованих злочинних угруповань у зазначеному середовищі — кіберугруповання.

Отже, логічним буде визначити організовану кіберзлочинність як сукупність кіберзлочинів, що вчиняються у зв'язку зі створенням та діяльністю у кіберпросторі організованих злочинних угруповань (кіберугруповань).

Таким чином, для визначення організованої кіберзлочинності необхідно розглянути не тільки поняття "кіберпростору", але й характерні риси кіберзлочинів та організованих злочинних кіберугруповань.

Фахівці вважають, що префікс "кібер-" (cyber) використовується для того, щоб надати певному слову значення чогось, що відноситься до комп'ютерів, Інтернету та цифрових технологій [2]. Однак, на нашу думку, даний префікс є скороченням прикметника "кібернетичний", який вказує на такий, що створений на основі принципів, методів кібернетики [3, с. 427].

Кібернетику, узагальнюючи її тлумачення у словниках та енциклопедії [4, с. 259; 5, с. 226; 6, с. 75], можна розглядати як науку про загальні закономірності процесів управління та перетворення інформації у кібернетичних системах.

При цьому, під кібернетичною системою розуміють сукупність пов'язаних один з одним об'єктів (елементів системи), здатних сприймати, зберігати, переробляти інформацію, а також обмінюватися інформацією [4, с. 265]. Також необхідно відмітити, що кібернетичну систему можна визнати тотожною комп'ютерній системі, визначення якої подане у Конвенції про кіберзлочинність [7] — будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, у відповідності до певної програми, виконує автоматичну обробку даних.

У якості кібернетичної комп'ютерної системи можна розглядати як автономний комп'ютер з периферійними виконуючими пристроями, так і комп'ютерні мережі. Елементами кібернетичної комп'ютерної системи є: інформація у формі, придатній для автоматизованої обробки (комп'ютерні дані); носії інформації; програмно-технічні засоби автоматизованої обробки даних та засоби телекомунікацій; засоби забезпечення нормального функціонування системи (спеціальні приміщення, пристрої живлення, кондиціонування, заземлення тощо); телекомунікаційні канали; методи автоматизованої обробки даних та телекомунікацій; персонал, що забезпечує виконання автоматизованої обробки даних.

Функціонування такої системи дозволяє її користувачам отримувати доступ до обчислювальних та інформаційних ресурсів системи, виробляти електронні інформаційні продукти, обмінюватись електронними повідомленнями, а також за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо).

Таким чином, кіберпростір (кібернетичний простір) можна визначити як штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління та обробки інформації.

Кіберпростір у його найбільш повному розумінні реалізується (симулюється) на основі регіональних і глобальних комп'ютерних мереж (у першу чергу, — це мережа Інтернет), на основі локальних інформаційних мереж можна говорити про реалізацію лише окремих сегментів кіберпростору. В автономному комп'ютері буде відсутньою така ознака кіберпростору, як інформаційна взаємодія між користувачами в режимі реального часу.

Аналіз характерних рис кіберпростору вказує на доцільність його розгляду як середовища вчинення злочинів, з позицій: кібернетичного середовища, утвореного у результаті функціонування кібернетичних комп'ютерних систем управління та обробки інформації; інформаційного середовища як складової частини загального інформаційного простору, в якому інформаційні процеси реалізуються на основі принципів, методів і засобів автоматизованої обробки інформації; електронного середовища, що функціонує на основі принципів, методів і засобів обробки інформації в електронній (цифровій) формі, а також передбачає необхідність відповідних програмно-апаратних засобів для сприйняття людиною такої інформації та телекомунікаційних засобів для її отримання або розповсюдження; віртуального середовища, в якому за допомогою технічно-програмних засобів (візуально-тактильно-звукова симуляція реальності), можливе створення ефекту присутності користувача в іншому, відмінному від реального, штучному світі; мережного середовища, реалізованого на основі інформаційно-телекомунікаційних мереж і, як цілісний об'єкт, утворений носіями інформації у цих мережах (у тому числі сигналами, що передаються канала-

ми зв'язку); комунікаційного середовища, створеного з використанням технологій комп'ютерного зв'язку; системи суспільних відносин, сформованої в процесі спільної діяльності щодо використання інформаційних і телекомунікаційних ресурсів кіберпростору відносно стійкої системи зв'язків та відносин між його користувачами; особливого психологічного середовища, що характеризується практично необмеженою свободою та анонімністю й забезпечує користувачам кіберпростору можливість комунікації саме з тим фрагментом реальності, який є найбільш близьким для їх індивідуальностей.

Науковці відмічають, що слово "кіберпростір" служить вдалим містком між словами "Інтернет" та "кібернетика", насамперед тому, що в ньому "точно відбито характер взаємозв'язку Мережі та цієї науки" [8]. Тому поняття кіберзлочинності часто пов'язують саме зі злочинністю у комп'ютерних мережах і, насамперед, в Інтернеті [9, с. 10].

Зважаючи на вищезазначене, під кіберзлочинами (кібернетичними злочинами) пропонується розуміти злочини, пов'язані з протиправним використанням кібернетичних комп'ютерних систем.

До протиправного використання кібернетичних комп'ютерних мереж у загальному вигляді можна віднести: несанкціоноване отримання прав керування такою системою (наприклад, використання шкідливого програмного забезпечення спотворення інформації про стан об'єкту в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку тощо) та її нерегламентоване використання (наприклад, для спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), а також створення та використання у злочинних цілях однієї кібернетичної комп'ютерної системи проти іншої (наприклад, створення мережі зомбованих комп'ютерів для здійснення атак на веб-сайти, створення несанкціонованого автоматизованого робочого місця у системі електронного переказу коштів тощо).

У кіберпросторі комп'ютерних систем, реалізованих на основі комп'ютерних мереж (зокрема, мережі Інтернет), можуть вчинятися злочинні посягання на суспільні відносини в різних галузях людської діяльності, пов'язаних як з використанням інформаційних об'єктів, так й інформаційною взаємодією суб'єктів діяльності в електронній цифровій формі (несанкціоноване втручання у роботу окремих сегментів комп'ютерних мереж, перехоплення комп'ютерних даних, шахрайство, вимагання, шпіонаж, фіктивне підприємництво, терористичний акт, хуліганство, розголошення державної таємниці, пропаганда війни тощо).

Дослідниками відмічається, що висока соціальна небезпека Інтернет-злочинності випливає, насамперед, із суспільних відносин, яким вона загрожує, а також з її транснаціонального та організованого характеру [10, с. 4].

Хоча у Конвенції Ради Європи про кіберзлочинність (ратифікована Україною у 2005 році) [7] не розкрито поняття кіберзлочину, проте визначено перелік протиправних діянь, за які на національному рівні повинна

встановлюватися кримінальна відповідальність. Тлумачення положень даної Конвенції та Додаткового протоколу до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (ратифікований Україною у 2006 році) [11] дозволяє віднести до кіберзлочинів лише злочинні посягання:

— проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, вчинені з використанням технічних засобів і комп'ютерних даних (незаконний доступ до комп'ютерної системи або її частини без права на це; нелегальне перехоплення технічними засобами передач комп'ютерних даних; навмисне перешкоджання функціонуванню комп'ютерної системи; виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, створених або адаптованих для використання при вчиненні вищезазначених злочинів, а також комп'ютерних паролів, кодів доступу, за допомогою яких можна здобути доступ до комп'ютерної системи або її частини з наміром використання її для вчинення будь-якого вищезазначеного злочину; володіння будь-яким із зазначених предметів з наміром його використання для вчинення будь-якого з вищезазначених злочинів);

— пов'язані з комп'ютерами (комп'ютерна підробка, комп'ютерне шахрайство);

— пов'язані з виробленням, володінням або пропонуванням громадськості чи наданням доступу через комп'ютерні системи, розповсюдженням, передаванням або набуттям за допомогою комп'ютерних систем, інформації, яка за своїм змістом є: дитячою порнографією; матеріалами расистського та ксенофобного характеру; погрозами з расистських та ксенофобних мотивів; образами з расистських та ксенофобних мотивів; запереченням, значною мінімізацією, схваленням або виправданням геноциду чи злочинів проти людства; пособництвом та підбурюванням до вчинення будь-якого з правопорушень расистського та ксенофобного характеру);

— пов'язані з порушенням за допомогою комп'ютерних систем авторських та суміжних прав, учинені свідомо, в комерційних розмірах.

У кіберпросторі виділяють систему суспільних відносин, що виникають у результаті інформаційної взаємодії суб'єктів Інтернет-співтовариства — сформованої в процесі спільної діяльності відносно стійкої системи зв'язків і відносин між користувачами мережного інформаційного простору [12, с. 214]. При цьому, загальна схема інформаційного процесу певного суб'єкта залишається незмінної й у кіберпросторі, проте цей процес супроводжують інші (специфічні) загрози, пов'язані з особливостями існування і передачі інформації в новому середовищі [13].

Дослідники відмічають, що: усі достоїнства кіберпростору залишаються достоїнствами, і не стають недоліками доти, поки не з'являється індивідуум — учасник Інтернет-спілкування, налаштований агресивно, зацікавлений у втручанні в сферу Інтернет-відносин з метою одержання матеріальної вигоди, або з хуліганських спонукань [14]; особливості технологій

мережі Інтернету, що допомогли їй поширитися по всьому світі, у той же час створюють сприятливі можливості для багатьох видів злочинної діяльності [10, с. 3].

Зазначене дозволяє зробити висновок, що наявність системи суспільних відносин [15, с. 60] та особливого психологічного середовища [16; 17] у мережі Інтернет сприяє встановленню у кіберпросторі стійких взаємозв'язків між кримінально орієнтованими особами, що, у свою чергу, призводить до утворення в мережному середовищі їх віртуальних співтовариств (злочинних кібертовариств).

З розвитком глобальних інформаційних мереж (зокрема, мережі Інтернет), а також системи суспільних відносин у кіберпросторі, діяльність злочинних кібертовариств набуває все більш організованого характеру.

Так, правоохоронці Росії відзначають стійку тенденцію до об'єднання хакерів у групи, в тому числі міжнародні, для вчинення великомасштабних злочинів. Причому такі союзи носять, на їхню думку, яскраво виражені ознаки організованих злочинних груп [18]. Вітчизняні дослідники, крім організованих груп хакерів, виділяють також організовані злочинні формування, які використовують для досягнення злочинної мети фахівців у галузі комп'ютерних технологій (програмістів, хакерів та інших) по найму [19, с. 113].

Необхідно відмітити, що членом злочинного кіберугруповання може бути спеціальний суб'єкт — користувач кіберпростору, який з метою вчинення злочинів здійснює у кіберпросторі інформаційну взаємодію з іншими користувачами (членами кіберугруповання).

Аналіз процесів, пов'язаних зі створенням та діяльністю кібертовариств, дозволяє відмітити у них характерні риси, притаманні організованим злочинним угрупованням у реальному світі (ст. 28 КК України [20]), а саме:

— кількісний склад учасників (користувачів мережі);

— попередня зорганізованість цих осіб в об'єднання з метою вчинення злочинів (на основі використання комунікаційних можливостей мережі Інтернет), у тому числі й зорганізованість в об'єднання за попередньою змовою для спільної діяльності з метою а) безпосереднього вчинення учасниками злочинної організації тяжких або особливо тяжких злочинів; б) керівництва чи координації злочинної діяльності інших осіб; в) забезпечення функціонування як самої злочинної організації, так і інших злочинних груп;

— стійкість цих об'єднань та їх ієрархічність (об'єднання навколо певного веб-сайту злочинної спрямованості з різними правами доступу до нього);

— наявність єдиного плану для вчинення кіберзлочинів, відомого всім учасникам групи та розподілу функцій учасників групи, спрямованих на досягнення цього плану.

Як приклад організованої злочинності у кіберпросторі можна навести діяльність міжнародного злочинного угруповання під назвою CarderPlanet [21; 22].

Метою членів зазначеної злочинної організації, об'єднаних мережею Інтернет, було отримання надприбутків від протиправної діяльності, пов'язаної з викраданням інформації про справжні платіжні картки міжнародних платіжних систем VISA, Master Card, American Express, Diners Club International, продажем цієї інформації, використанням цієї інформації при розрахунках у мережі Інтернет, виготовленням підроблених платіжних карток, їх збутом та використанням на території країн як Західної, так і Східної Європи. Серед організаторів та найбільш активних учасників зазначеної злочинної організації були громадяни України, Російської Федерації, Республіки Білорусь, США та країн Західної Європи.

CarderPlanet створив свій web-сайт, організувавши його учасників за ієрархічною структурою, змодельованою у віртуальному світі на традиціях італійської мафії: Сім'я — організатори міжнародного Союзу кардерів. Члени Сім'ї мали необмежений доступ до коштів з рахунків кредитних карток і були ініціаторами найбільш значних шахрайських схем CarderPlanet; адміністратори CarderPlanet — мали особисті робочі відносини з членами Сім'ї (потенційні члени Сім'ї); ватажки організованих груп CarderPlanet — члени CarderPlanet, що створили власні групи в окремих країнах для здійснення інтерактивної шахрайської діяльності за схемами, узгодженими з членами Сім'ї, пропонували послуги та допомогу за іншими шахрайськими схемами; постачальники — обслуговували різні потреби шахрайської діяльності членів CarderPlanet (комп'ютерні зломщики, спеціалісти по підробленню документів, платіжних карток, постачальники заготовок, сировини тощо).

Узагальнюючи вищенаведене, до характерних ознак організованої кіберзлочинності (кібернетичною злочинністю) необхідно віднести:

— сукупність протиправних діянь (кіберзлочинів), учинених шляхом використання кібернетичних комп'ютерних систем управління та обробки інформації (кіберзлочинність);

— вчинення злочинів даного виду в зв'язку зі створенням та діяльністю організованих злочинних кіберугруповань — кримінально орієнтованих співтовариств користувачів кіберпростору;

— середовищем вчинення кіберзлочинів та діяльності організованих кіберугруповань є кіберпростір — штучне електронне середовище існування інформаційних об'єктів у цифровій формі, створене в результаті функціонування кібернетичних комп'ютерних систем.

Таким чином, організовану кіберзлочинність можна визначити як сукупність кіберзлочинів, що вчиняються у зв'язку зі створенням та діяльністю у кіберпросторі організованих злочинних співтовариств його користувачів (кіберугруповань). Для досягнення злочинної мети

члени кіберкгруповань використовують кібернетичні комп'ютерні системи управління та обробки інформації.

Розуміння сутності організованої кіберзлочинності та процесів, що відбуваються у кіберпросторі у зв'язку з діяльністю організованих злочинних кіберугруповань, сприятиме проведенню подальших досліджень у напрямку розробки нових, більш ефективних методів і засобів боротьби з даним видом організованої злочинності.

Список використаних джерел

1. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30 черв. 1993 р. // Відомості Верховної Ради України. — 1993. — № 35. — Ст. 358.

2. Киберполитика : Глоссарий [Электронный ресурс]. — Режим доступа : http://www.cyberpolitics.ru/content/view/77/29/

3. Великий тлумачний словник сучасної української мови / [уклад і голов. ред. В. Т. Бусел]. − К. : Ірпінь : ВТФ "Перун", 2002. − 1440 с.

4. Словарь по кибернетике : [св. 2000 ст.] / [под. ред. В. С. Михалевича]. — [2-е изд.]. — К. : Гл. ред. УСЭ им. М. П. Бажана, 1989. — 751 с.

5. Словарь иностранных слов / [под ред. члена-кореспондента АН СССР А. Г. Спиркина, д-ра философ. наук И. А. Акчурина, д-ра философ. наук Р. С. Карпинской]. — [11-е изд. стереотип.]. — М. : Рус. яз., 1984. — 608 с.

6. Большая Советская Энциклопедия : [в 30 т.] / [гл. ред. А. М. Прохоров]. — [3-е изд.]. — М. : "Сов. энциклопедия". — Т. 12. — Кварнер — Колгур, 1973. — 624 с.

7. Про кіберзлочинність : Конвенція Ради Європи // Офіц. вісник України. — 2007. — № 65.— Ст. 2535. — С. 107. — 10 верес. — Код акту 40846 /2007.

8. Черняк Л. Internet и кибернетика [Электронный ресурс] / Леонид Черняк. — Режим доступу : http://www.icfcst.kiev.ua/museum/EP/cybernetic_r.html

9. Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации : по материалам Республики Дагестан : автореф. дис. на соискание ученой степени канд. юрид. наук : спец. 12.00.08 "Уголовное право и криминология; Уголовно-исполнительное право" / М. С. Гаджиев. — Махачкала, 2004. — 19 с.

10. Дремлюга Р. И. Интернет-преступность : автореф. дис. на соискание ученой степени канд. юрид. наук : спец. 12.00.08 "Уголовное право и криминология; Уголовно-исполнительное право" / Р. И. Дремлюга. — Владивосток, 2007. — 26 с.

11. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи // Офіц. вісник України. — 2006. — № 31. — Ст. 2202. — С. 29. — 16 серп.

12. Демянчук Е. В. Интернет как объект оперативно-розыскной деятельности / Е. В. Демянчук // Информатизация и информационная безопасность правоохранительных органов. — М. : Академия управления МВД России, 2004. — С. 214—216.

13. Угрозы информационной безопасности. Новые реалии и адекватность классификации [Електронний ресурс] / Н. Пархоменко, С. Яковлев, П. Пархоменко, Н. Мисник // Конфидент. — 2003 — № 6. — Режим доступу :
http://www.bre.ru/security/20888.html

14. Важенин А. Г. Интернет и преступность : криминологические и правовые аспекты взаимосвязи [Електронний ресурс] / А. Г. Важенин. — Владивосток, 2005. — Режим доступу :
http://www.crime.vl.ru/index.php?p=1007&print=1&more=1

15. Грибанов Д. В. Преступность в кибернетическом пространстве (законодательство и Конвенция о киберпреступности) / Д. В. Грибанов // Рос. юрид. журнал. — 2002. — № 4. — С. 60—64.

16. Сердюк О. О. Соціальна робота з особами з наркотичною та алкогольною залежністю [Електронний ресурс] / О. О Сердюк., Ю. Л. Бєлоусов // Соціальна робота в органах внутрішніх справ України : [навч. посіб.]. — Харків : НУВС, 2006. — С. 303—324. — Режим доступу :
http://www.psychiatry.ua/articles/paper148.htm

17. Алексенко Н. Н. Психоаналитические аспекты поведения человека в киберпространстве [Електронний ресурс] / Н. Н. Алексеенко // Журнал практической психологии и психоанализа. — 2000. — № 3. — сентябрь — Режим доступу :
http://psyjournal.ru/j3p/pap.php?id=20000307

18. Кузнецов А. Борьба с преступлениями, совершаемыми с использованием сети Интернет [Електронний ресурс] / Антон Кузнецов. — Режим доступу :
http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=593

19. Долженков О. Ф. Інфраструктура організованої економічної злочинності / О. Ф. Долженков. — Одеса : НДРВВ ОЮІ НУВС, 2002. — 254 с.

20. Кримінальний кодекс України // Відомості Верховної Ради України. — 2001. — № 25—26. — Ст. 131.

21. Хвостик Е. Украинских карточных мошенников вытянули из сети / Е. Хвостик, Е. Ковалева, М. Никитин // Коммерсантъ. — 2005. — № 132 (3216). — 20 июля.

22. Золотое время Carderplanet [Електронний ресурс]. — Режим доступу :
http : //www.interface.ru /home.asp? artId=2217

Статья посвящена определению понятия организованной киберпреступности. Рассматриваются характерные черты организованной преступной деятельности в киберпространстве.

The article is devoted to the determination of the concept of organized cybercrime. The characteristic features of the organized criminal activity in cyberspace are examined.

Стаття надійшла до редакції журналу 03 листопада 2009 року.