УДК 343.97

Іванченко О. Ю.,
аспірант кафедри адміністративного та кримінального права
юридичного факультету
Дніпропетровського національного університету імені Олеся Гончара

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ, ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ НА НАЦІОНАЛЬНОМУ РІВНІ

CYBERCRIME CRIMINOLOGICAL CHARACTERISTICS, PREVENTION OF CYBERCRIME AT NATIONAL LEVEL

Стаття присвячена комплексній кримінологічній характеристиці кіберзлочинності та проблемам запобігання їй органами внутрішніх справ і Національною поліцією України. У роботі визначено поняття кіберзлочинності та надано класифікацію кіберзлочинів. Охарактеризований сучасний стан кіберзлочинності в Україні: встановлені її рівень, динаміка, величина та фактори латентності, структура, географія. Надана характеристика особистості кіберзлочинця. Виявлені, описані та проаналізовані соціально-демографічні, кримінально-правові та морально-психологічні риси осіб, засуджених за вчинення кіберзлочинів. Встановлені та проаналізовані основні політико-правові, соціально-економічні, організаційно-управлінські та культурно-психологічні фактори кіберзлочинності.

Ключові слова: *кіберзлочинність, стан, особистість злочинця, детермінація, запобігання, органи внутрішніх справ, поліція, взаємодія, психологічні риси осіб, культурно-психологічні фактори кіберзлочинності.*

Статья посвящена комплексной криминологической характеристике киберпреступности и проблемам предупреждения ее органами внутренних дел и Национальной полицией Украины. В работе определено понятие киберпреступности и предоставлена классификация киберпреступлений. Охарактеризован современный уровень киберпреступности в Украине: установлены ее уровень, динамика, величина и факторы латентности, структура, география. Предоставлена характеристика личности киберпреступника. Выяснены, описаны и проанализированы социально-демографические, криминально-правовые и морально-психологические черты лиц, осужденных за совершение киберпреступлений. Установлены и проанализированы основные политико-правовые, социально-экономические, организационно-управленческие и культурно-психологические факторы киберпреступности.

Ключевые слова: *киберпреступность, состояние, личность преступника, детерминация, предупреждение, органы внутренних дел, полиция, взаимодействие, психологические черты лиц, культурно-психологические факторы киберпреступности.*

The article is devoted complex criminological characteristics of cybercrime and the problems preventing it by Interior and National Police of Ukraine. The paper defines the notion of cyber crime and cyber given classification. Described the current state of cybercrime in Ukraine set the level, dynamics, size and latency factors, structure, geography. The characteristic personality cyber criminal. Identified, described and analyzed socio-demographic, criminal and moral-psychological characteristics of persons convicted of committing cybercrimes. Installed and analyzed the main political, legal, social, economic, organizational, managerial, cultural and psychological factors cybercrime.

Key words: *cybercrime, state offender, determination, prevention, law enforcement bodies, police cooperation, psychological traits of people, cultural and psychological factors cybercrime.*

Метою дослідження є формування комплексної кримінологічної характеристики кіберзлочинності та вироблення на цій основі науково обґрунтованих рекомендацій щодо запобігання цим злочинам ОВС та Національною поліцією. Для досягнення поставленої мети необхідно вирішити такі задачі: визначити поняття кіберзлочинності, з'ясувати її феномен та прояви; здійснити кримінологічну класифікацію кіберзлочинів; охарактеризувати сучасний стан кіберзлочинності в Україні через опис і пояснення її кількісних та якісних кримінологічних показників; надати характеристику особистості кіберзлочинця, визначити її специфічні риси; дослідити особливості детермінації кіберзлочинності; охарактеризувати правові засади запобігання кіберзлочинності ОВС і Національною поліцією; визначити та описати систему заходів запобігання кіберзлочинності ОВС і Національною поліцією, виробити пропозиції щодо її удосконалення; дослідити засади та прикладні аспекти взаємодії ОВС і Національної поліції з іншими суб'єктами запобігання кіберзлочинності та запропонувати на цій підставі шляхи її оптимізації. Об'єктом дослідження є суспільні відносини у сфері забезпечення кібернетичної складової кримінологічної безпеки України. Предметом дослідження є кіберзлочинність, а саме її кримінологічна характеристика та запобігання органами внутрішніх справ.

Кінець XX століття ознаменувався стрімким розвитком інформаційних технологій, що почали впроваджуватися в усі сфери життєдіяльності людей. Використання сучасних персональних комп'ютерів, інформаційно-обчислюваних мереж і комп'ютеризованих комунікаційних мереж забезпечило кожній особі можливості доступу до інформації, що зберігається у відповідних банках даних незалежно від доби і місцезнаходження абонента. Окрім переваг, комп'ютеризація має ряд негативних наслідків, серед яких є поява якісно нового виду злочинності – кіберзлочинності. Наслідки цієї злочинності зачіпають не тільки інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство в цілому. Кіберзлочини найчастіше став-

лять під загрозу життєво важливу інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства.

Під кіберзлочинністю слід розуміти сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Поняття «кіберзлочинність» часто вживається поряд з поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених термінів поняття «кіберзлочинність» є найширшим поняттям та охоплює найбільше коло злочинних посягань у віртуальному середовищі, а також його використання передбачає міжнародне законодавство. Так, Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність. Тому вважаємо обґрунтованим вживання саме цього терміна для кримінологічного дослідження цього різновиду злочинності.

Можемо виділити такі ознаки кіберзлочинності.

Ці злочини 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 по локальних і глобальних комп'ютерних мережах, зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі (В.А.Голубєв).

Кіберзлочини вчиняються 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 виступати як засобом вчинення злочину, так і предметом злочину.

На сьогодні найбільш розповсюдженою є класифікація кіберзлочинів на дві групи: агресивні та неагресивні. До першою групи належать кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм.

Переходячи до кримінологічної характеристики кіберзлочинності, слід зазначити, що більшість виявлених злочинів, що вчиняються з використанням комп'ютерних технологій, розпорошені у звітності різних підрозділів правоохоронних органів серед показників економічної та інших видів злочинності. Через таку недосконаліть статистичної звітності неможливо провести комплексну характеристику кіберзлочинності. У зв'язку з цим проаналізуємо лише передбачені Розділом XIV Особливої частини Кримінального кодексу України (далі – КК України) злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Отже, рівень цієї злочинності за 2010 рік становив 190 зареєстрованих злочинів, за 2011 рік – 131, за 2012 рік – 255, за 2013 рік –595 злочинів. Можна побачити, значний приріст в динаміці досліджуваного виду злочинності в Україні за останні 4 роки. Порівняно з 2010 роком, кількість виявлених злочинів збільшилась майже втричі. Питома вага злочинності у сфері електронно-обчислюваних машин у структурі злочинності в Україні становить приблизно 0,05%. Рівень судимості за 2010 рік складав 68 осіб, за 2011 рік – 56 осіб, за 2012 рік – 93 особи.

Стостовно структури досліджуваної злочинності, то найбільшу питому вагу (40-60% від усіх зареєстрованих злочинів у цій сфері) складають діяння, пов'язані з несанкціонованим втручанням в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ст. 361 КК України), та діяння, передбачені ст. 362 КК України, а саме 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 (25–45%). Певним чином це пояснюється найширшими диспозиціями зазначених вище статей КК України, що охоплюють більшість форм кримінальної діяльності у сфері функціонування електронно-обчислюваних машин.

Однак зазначені вище статистичні показники, на жаль, не відбивають реальний стан кіберзлочинності, оскільки цей різновид злочинів має високий рівень латентності. За експертними оцінками, рівень латентності кіберзлочинів становить 90–95%. Причинами латентності найчастіше виступають складнощі виявлення та розслідування кіберзлочинів, неповідомлення потерпілих осіб про факти вчинення таких злочинів. Так, більшість великих компаній хвилюються про свою ділову репутацію та намагаються усунути наслідки кіберзлочинів власними зусиллями. Кіберзлочинність характеризується високим рівнем природної латентності.

Кримінологічна характеристика особи кіберзлочинцямає важливе значення, оскільки ефек-

тивна, успішна боротьба з кіберзлочинам неможлива без всебічного аналізу образу мислення і особи порушника.

Кіберзлочини в Україні переважно вчиняють чоловіки, але за останні 4 роки питома вага жінок значно зросла (до 30%). Це пояснюється підвищенням інтересу жінок до сучасних інформаційних технологій.

Залежно від віку виділяють дві групи кіберзлочинців: від 14 до 20 років, від 21 року і старші. До особливостей вчинення кіберзлочинів першою групою осіб належить відсутність цілеспрямованої, продуманої підготовки до злочину; оригінальність способу; неприйняття заходів для приховування злочину; факти невмотивованого бешкетництва. Діяння осіб понад 21 рік, як правило, мають усвідомлений корисливий характер. Дослідження показують, що злочинці цієї групи, як правило, є членами добре організованих, мобільних і технічно оснащених висококласним обладнанням і спеціальною технікою (нерідко оперативно-технічного характеру) злочинних груп і співтовариств. Осіб, які входять в їх склад, загалом можна характеризувати як висококваліфікованих спеціалістів з вищою юридичною, економічною (фінансовою) і технічною освітою. Злочини носять багатоепізодний характер, обов'язково супроводжуються діями, спрямованими на приховання злочинів. Саме ця група злочинців і є основною загрозою для людей, суспільства і держави, є реальним кадровим ядром комп'ютерної злочинності як в якісному, так і в кількісному плані. Правоохоронна практика показує, що на долю цих злочинів припадає найбільша кількість посягань, які мають особливо небезпечний характер (В.Б. Вехов).

Специфіка використання комп'ютерної техніки передбачає доволі високий рівень освітнього рівня. Тому серед осіб, що вчиняють кіберзлочини, найчастіше зустрічаються люди з вищою або середньою спеціальною освітою. Багато часу, затраченого на отримання досвіду роботи з високими технологіями, заважає особистому життю. Таким чином, сімейний стан більшості кіберзлочинців – «неодружений».

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%.

Дослідники виділяють найбільш притаманні для типового кіберзлочинця індивідуально-психологічні риси: 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 міжособистих стосунках; заглибленість у свої думки, мрії, фантазії; філософське сприйняття світу; відсутність буттєвих ціннісних орієнтацій; викривлена (збочена) система життєвих цінностей; тотальна недовірливість та виражений цинізм; прагнення уникнути перешкод у подоланні життєвих труднощів.

Зарубіжні вчені виділяють також п'ять найпоширеніших мотивів скоєння комп'ютерних злочинів: корисливий мотив – 66%, політичні мотиви (шпигунство, злочини, спрямовані на підрив фінансової, кредитної політики уряду, дезорганізацію валютної системи країни) – 17%, дослідницький інтерес – 7%; хуліганські мотиви – 5%, помста – 3%.

Показником рівня розвитку будь-якого суспільства стає право не тільки на вільний доступ до інформації, але й на надійний захист інформації обмеженого доступу. На початку XXI століття, коли сучасні інформаційні технології інтенсивно впроваджуються в усі сфери життя і діяльності суспільства, національна безпека починає прямо залежати від забезпечення інформаційної безпеки, що, в свою чергу, гарантує стабільність суспільства, забезпечення прав і свобод громадян та правопорядок.

Громадськість все більше цікавиться цими питаннями, оскільки кожний власник або користувач комп'ютеру – це потенційний потерпілий, якого можуть очікувати тяжкі наслідки в разі вчинення злочину, особливо у комерційному та промисловому секторі, де можливі великі фінансові втрати. Комп'ютерні злочинці за допомогою міжнародних комп'ютерних мереж – на кшталт Інтернету – широко розповсюджують свій кримінальний досвід, не звертаючи увагу на національні кордони, що вимагає відповідних кроків кооперації від поліцейських установ, протидіючих цим злочинам. Все це вимагає оперативного обміну інформацією про комп'ютерні злочини.

З розвитком глобальної комп'ютерної мережі Інтернет набули поширення так звані кіберзлочини. Саме тому проблема захисту інформації сьогодні є особливо актуальною. Багато проблем виникає у зв'язку з крадіжками послуг, зокрема вторгнення до телефонних мереж та незаконна торгівля послугами зв'язку. Також Інтернет широко використовують торговці піратським програмним забезпеченням, порнографією, зброєю та наркотиками для ведення справ, обміну інформацією, координації злочинних дій. Комп'ютерні мережі, окрім всього, можуть стати об'єктом нападу терористів.

В багатьох країнах для боротьби з цим видом злочину створені спеціалізовані підрозділи, які займаються виявленням, розслідуванням кіберзлочинів та збором іншої інформації з цього питання на національному рівні. Саме спеціалізовані національні поліцейські підрозділи утворюють головне ядро сил протидії міжнародній комп'ютерній злочинності. Такі підрозділи вже створені і діють тривалий час у Сполучених Штатах Америки, Канаді, Великобританії, Німеччині, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі та багатьох інших країнах. Це дало можливість накопичити матеріал про законодавче регулювання та організаційний досвід

боротьби з комп'ютерною злочинністю в різних країнах, підготувати ряд аналітичних оглядів і публікацій з цих питань, ознайомити співробітників МВС з цим новим для України видом злочинів, внести конкретні пропозиції щодо удосконалення кримінального законодавства України.

Необхідно терміново розробити та прийняти на державному рівні національну Програму протидії комп'ютерним злочинам, що забезпечить належний рівень організації питань з аналізу, прогнозування, попередження, викриття та розслідування такого небезпечного явища в суспільстві, яким є комп'ютерний злочин.

Відомо, що особа злочинця досліджується різними науками. Кримінологічні дослідження обмежуються головним чином тими особливостями людини, які необхідні для використання з метою кримінальної профілактики, попередження злочинів.

Характеризуючи особу комп'ютерного злочинця, необхідно відзначити основну ознаку, а саме: в електронну злочинність втягнуто широке коло осіб, (від висококваліфікованих фахівців до дилетантів). Правопорушники приходять з усіх сфер життя і мають різний рівень підготовки.

Для протидії цьому новому виду злочинів необхідно вивчення цієї проблеми і дослідження криміналістичних та психологічних рис кіберзлочинців. Вітчизняні та зарубіжні дослідження дають змогу намалювати портрет типового комп'ютерного злодія, тобто відповідний профіль цього соціального типу [1].

Формування банку типових моделей різних категорій злочинців, вивчення загальних рис цих людей дає змогу оптимізувати процес виявлення кола осіб, серед яких вірогідно вести пошук злочинця.

Проведені соціологічні і кримінолого-криміналістичні дослідження, зокрема в Австралії, Канаді, США, Німеччині, допомогли розподілити комп'ютерних злочинців за віком на три великі категорії [2]:

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, які мають доступ до ЕОМ. Ця особа, як правило:

– працює в 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 поступки інших працівників;

– добре знайома з роботою систем захисту інформації і має ключі від основних замків службових приміщень.

Діапазон рівня спеціальної 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.

Особистими характеристиками портрета комп'ютерного злочинця є активна життєва позиція, нестандартність мислення і поведінки, обережність, уважність.

З точки зору психофізіологічних характеристик комп'ютерний злочинець – це, як правило, яскрава, мисляча й творча особа, великий професіонал своєї справи, здатний іти на технічний виклик, бажаний працівник. Водночас це людина, яка боїться втратити свій авторитет або соціальний статус в рамках своєї соціальної групи. Зовні їх поведінка рідко відрізняється від встановлених у суспільстві соціальних стандартів і норм поведінки. Крім того, практика свідчить про те, що комп'ютерні злочинці у своїй більшості не мають кримінального минулого.

Значна частина комп'ютерних злочинів здійснюється індивідуально. Але сьогодні має місце тенденція співучасті в групових посяганнях. Кримінальна практика свідчить про те, що 38% злочинців діяли без співучасників, тоді як 62% скоювали злочини в складі організованих злочинних угрупувань [3].

Деякі з правопорушників цієї категорії технічно оснащені досить слабко, а інші мають дорогі, престижні, науково місткі й могутні комп'ютерні системи. Прогрес у технології супроводжується впровадженням нових методів вчинення злочинів. Комп'ютери і засоби телекомунікації дають зручну можливість для здійснення злочинних намірів з віддалених пунктів.

Велику кількість комп'ютерних злочинців складають посадові керівники всіх рангів (більше 25%). Це обумовлено тим, що керівником є, як правило, спеціаліст більш високого класу, який володіє достатніми професійними знаннями, має доступ до широкого кола інформації, може давати відповідні вказівки та розпорядження і безпосередньо не відповідає за роботу комп'ютерної техніки.

Термін «хакер» вперше почав використовуватись на початку сімдесятих років у Масачусетскому технологічному інституті по відношенню до молодих програмістів, які проектували апаратні засоби ЕОМ та намагались сконструювати перші персональні комп'ютери. Коли у Сполучених Штатах Америки з'явились великі ЕОМ, компанії дозволяли студентам користуватися ними. Як правило, для цього відводили нічні години і студенти, яких стали звати

хакерами, саме у цей час працювали на ЕОМ. Далі такі неформальні групи розподілялись на зміни. Одна зміна мала для праці квант часу, наприклад, з 3 до 4 години ночі. Закінчивши програмування, хакери залишали розроблені програми у шухлядах біля комп'ютеру. Кожен міг заглянути при цьому в записи своїх друзів. Досить часто вони брали чужі нотатки та вносили до них виправлення, намагаючись удосконалити результати програмування.

Хакери не псували чужу роботу і не намагались захистити свої програми від інших хакерів. Усі програми, які вони розробляли, були призначені для спільного користування. Хакери вірили, що комп'ютери – це ключ до повного визволення людини, оскільки роблять знання загальнодоступними. Уявлення хакерів про проблеми суспільства та роль у ньому інформаційних технологій знайшли своє визначення у вигляді специфічних маніфестів та звернень. Не можна заперечувати, що деякі з цих положень мали, окрім технічних та філософських аспектів, і суто соціальне забарвлення. Деякі з маніфестів хакерів й досі можна знайти на дошках електронних об'яв (BBS) у великих комп'ютерних мережах.

Практика свідчить про те, що дійсно особливу групу комп'ютерних злочинців становлять хакери, тому розглянемо їх детальніше.

Сам факт появи комп'ютерної злочинності у суспільстві більшість дослідників пов'язує з діяльністю так званих хакерів (англ. hacker) – користувачів обчислювальних систем і мереж ЕОМ, які займаються пошуком незаконних методів отримання несанкціонованого (самовільного) доступу до засобів комп'ютерної техніки і базам даних, а також їх несанкціонованого використання з корисливою метою.

За метою та сферою злочинної діяльності комп'ютерних злочинців можна поділити на окремі підгрупи.

1) Хакери (Hacker). Вони отримують задоволення від вторгнення та вивчення великих ЕОМ за допомогою телефонних ліній та комп'ютерних мереж. Це комп'ютерні хулігани, електронні корсари, які без дозволу проникають в чужі інформаційні мережі для забави. У значній мірі їх тягне до себе подолання труднощів. Чим складніша система, тим привабливіша вона для хакера. Вони є прекрасними знавцями інформаційної техніки. За допомогою телефону і домашніх комп'ютерів вони підключаються до мереж, які пов'язані з державними та банківськими установами, науково-дослідними та університетськими центрами, військовими об'єктами. Хакери, як правило, не роблять шкоди системі та даним, отримуючи насолоду тільки від почуття своєї влади над комп'ютерною системою.

Так, наприклад, американський хакер Річард Чешир, якого запросили в Мюнхен на нараду експертів з охорони відомостей в комп'ютерах, на очах фахівців забезпечив собі доступ спочатку в німецьку, потім в американську інформаційні мережі, а звідти проник в один із найважливіших стратегічних комп'ютерів США.

2) Крекери (Cracker). Це більш серйозні порушники, ніж хакери, здатні спричинити будь-яку шкоду системі. Вони викрадають інформацію, викачуючи за допомогою комп'ютера цілі інформаційні банки, змінюють та псують файли. З технічного боку це набагато складніше того, що роблять хакери.

За декілька годин, не докладаючи особливих зусиль, будь-який технік середньої руки може пограбувати банк даних французького комісаріату з атомної енергії і отримати найконфіденційніші відомості, наприклад, таємний проект створення лазера чи програму будівництва ядерного реактора [4].

3) Фрікери (phone+break=phreak). Вони спеціалізуються на використанні телефонних систем з метою уникнення від оплати телекомунікаційних послуг. Також отримують насолоду від подолання труднощів технічного плану. У своїй діяльності фрікери використовують спеціальне обладнання («чорні» та «блакитні» скрині), яке генерує спеціальні тони виклику для телефонних мереж.

На сьогодні фрікери здебільшого орієнтуються на отримання кодів доступу, крадіжки телефонних карток та номерів доступу з метою віднести платню за телефонні розмови на рахунок іншого абонента. Досить часто займаються прослуховуванням телефонних розмов.

4) Колекціонери (codeskids). Вони колекціонують та використовують програми, які перехоплюють різні паролі, а також коди телефонного виклику та номери приватних телефонних компаній, які мають вихід до загальної мережі. Як правило, вони молодші за хакерів та фрікерів. Обмінюються програмним забезпеченням, паролями, номерами, але не торгують ними.

5) Кіберплути (cybercrooks). Це злочинці, які спеціалізуються на розрахунках. Використовують комп'ютери для крадіжки грошей, отримання номерів кредитних карток та іншої цінної інформації. Отриману інформацію потім продають іншим особам, досить часто контактують з організованою злочинністю. Коди PBX можуть продаватись за 200–500 доларів США неодноразово, як і інші види інформації. Популярними товарами є кредитна інформація, інформаційні бази правоохоронних органів та інших державних установ.

6) Торгаші або пірати (waresdudes). Вони спеціалізуються на збиранні та торгівлі піратським програмним забезпеченням. На сьогоднішній день це дуже численна група злочинців. Кількість піратських BBS має співвідношення до хакерських як 20 до 1.

Більшість хакерів мають клички – прізвиська, за якими вони відомі серед інших хакерів. Підбір кличок, як правило, пов'язаний з віком та інтересами хакерів. Ось деякі найбільш розповсюджені з них: Скорпіон (Scorpion), Бандит (Bandito), Капітан (Captain), Розбещенець (Corrupt), Король Таран (Taran King), Зїхавший з глузду Едік (Crazy Eddic), Рейнджер Рік (Ranger Rick), Мисливець за головами (Head Hunter), Червоний Ніж (Red Knight), Шпигун (Spy). Більшість з них свідчить про моральні якості

їх власників, зокрема підкреслення влади, грубої сили. При спілкуванні хакери також широко використовують свій власний мовний жаргон.

Досить часто хакери утворюють за спільними інтересами або поглядами невеличкі групи, зокрема Військо Люцифера, Фахівці катастроф, Військо Дума, Комп'ютерний Клуб Хаосу. Іноді ці групи збираються щорічно, а у великих містах такі зустрічі можуть проводитися щомісячно. Але головною формою обміну інформацією залишаються дошки електронних об'яв (BBS), особливо підпільні. Серед найбільш відомих підпільних BBS можна назвати такі: Безодня (Abyss), Опік (Acid Phreak), Альтернативний Світ (Alternative Universe), Притон Наркоманів (Drug House), Ейфорія (Euphoria), Зона Хакерів (Hackers Zone), Залізна Завіса (Iron Curtain).

Кількість підпільних BBS важко оцінити та підрахувати. За оцінками зарубіжних спеціалістів тільки на території США функціонують десятки тисяч таких BBS, з яких від 100 до 200 є спеціалізованими для хакерів, а приблизно у 1 000 з них є важлива інформація для хакерів (зокрема про засоби злому різних систем, програмне забезпечення для перехвату паролів). Деякі країни, зокрема, Великобританія, Італія та країни Східної Європи, мають ще більшу концентрацію підпільних BBS.

Як загальний висновок треба зазначити, що комп'ютерна злочинність – це міжнародне явище, рівень якої тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах та регіонах. При цьому Україна, на наш погляд, має можливість використати досвід більш розвинутих країн для запобігання та викриття комп'ютерних злочинів. Загальні тенденції, злочинні засоби та заходи запобігання в різні відрізки часу є однаковими для різних країн, що базуються на єдності технічної бази цих злочинів. А з метою попередження таких злочинів необхідне подальше проведення досліджень соціального та криміналістичного профілю (портрет) типового комп'ютерного злодія.

ЛІТЕРАТУРА:

1. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые методы борьбы : автореф. дисс. … канд. юрид. наук / Т.Л. Тропина ; Юрид. ин-т ДГУ [Електронний ресурс]. – Режим доступу : http://www.crime.vl.ru/docs/stats/stat_178.html.

2. Сабадаш В.В. Компьютерная преступность – проблемы латентности / В.В. Сабадаш [Електронний ресурс]. – Режим доступу : http://www.crime-research.ru/articles/sabodash06.

3. Целесообразность разработки международных документов, включая конвенции о борьбе против организованной транснациональной преступности : Всемирная конф. на уровне министров по орг. транснациональной преступности (Неаполь, 21–23 ноября 1994 года). – E/CONF. 88/6, 1994.

4. Лунеев В.В. Преступность XX века. Мировые, региональные и российские тенденции / В.В. Лунеев. – М. : Изд-во НОРМА, 1999. – 516 с.

5. Про моніторинг телекомунікацій : Проект Закону України від 7 серпня 2003 року № 4042 // ЛІГА: ЗАКОН.

6. Про перехоплення та моніторинг телекомунікацій : Проект Закону України від 26 березня 2004 року № 4042-1 // ЛІГА: ЗАКОН.

7. Про перехоплення телекомунікацій : Проект Закону України від 21 березня 2005 року № 4042-2 // ЛІГА: ЗАКОН.

8. Ахтирська Н.М. Статистика комп'ютерної злочинності в Україні / Н.М. Ахтирська [Електронний ресурс]. – Режим доступу : http://www.lib.org.ua/ua/media/tech/59576.html.