УДК 343.2/.7

МОДЕЛЬ КОМП'ЮТЕРНИХ ЗЛОЧИНЦІВ

MODEL OF COMPUTER CRIMINALS

Ричка Д.О.,
аспірант ІІІ курсу юридичного факультету
Дніпровського національного університету
імені Олеся Гончара

Стаття присвячена розгляду суб'єкта злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку. Проведення аналізу ознак комп'ютерних злочинців надало змогу вивести типову модель комп'ютерних злочинців.
Ключові слова: суб'єкт, суб'єкт комп'ютерного злочину, кібер-злочинець, модель комп'ютерних злочинців, комп'ютерні технології, комп'ютерний злочин.

Статья посвящена рассмотрению субъекта преступлений в сфере использования электронно-вычислительных машин, систем и компьютерных сетей електросвязи. Проведение анализа признаков компьютерных преступников дало возможность создать типичную модель компьютерных преступников.
Ключевые слова: субъект, субъект компьютерного преступления, кибер-преступник, модель компьютерных преступников, компьютерные технологии, компьютерное преступление.

The article is devoted to consideration of the subject of crimes in the field of the use of electronic computers, systems and computer networks and networks of electrocardiographs. Conducting an analysis of the signs of computer criminals has allowed to bring a typical model of computer criminals.
Key words: subject, subject of a computer crime, cyber-criminal, model of computer criminals, computer technologies, computer crime.

Постановка проблеми. Комп'ютерна злочинність не тільки не залишає перші сходинки світових злочинів, а й набирає нових обертів. Якщо, наприклад, у 1980-х роках вміння користуватися електронно-обчислювальними машинами (далі – ЕОМ) або й взагалі їх наявність були рідкістю, то сьогодні скоріш дивує невміння користуватися електронними гаджетами. Практично на будь-якій роботі застосовується електронний документооббіг. Використання сучасних здобутків науки і техніки доступно будь-якій віковій категорії, будь-яким населенним пунктам та соціальним класам, тому і вчинення комп'ютерних злочинів малолітніми особами або людьми похилого віку не є поодинокими. Зарубіжні експерти роблять висновок про обумовленість розширення потенційних можливостей для вчинення злочинів даної категорії [1, с. 256–267; 2, с. 76].

Стан опрацювання проблеми. Дослідженням суб'єкта комп'ютерних злочинів займалися наступні науковці: Антонян Ю.М., Батурин Ю.М., Біленчук П.Д., Борисова Л.В., Бутузов В.М., Вертузаєв М.С., Владиміров В.А., Голубєв В.О., Долгова В.І., Жмихов А.А., Ігошев К.Е., Котляревський О.І., Лазарєв А.М., Левицький Г.А., Остапець С.Л., Плугатир М.В., Сергач О.І., Снігерьов О.П., Шелонцев В.П., Юрченко О.М. та інші.

До останніх здобутків даної тематики можливо віднести працю Борисової Л.В. «Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні і психофізіологічні аспекти», в якій проводиться аналіз професійної приналежності осіб до комп'ютерних злочинів.

Плугатир М.В. у праці «Особа, що має право доступу до комп'ютерної інформації як суб'єкт злочину, передбаченого ст. 362 КК України» наводить класифікацію суб'єктів Розділу XVI Кримінального кодексу (далі – КК) України.

Проведення наукового дослідження необхідне, аби на підставі ознак, притаманних комп'ютерним злодіям, розробити типову модель комп'ютерних злочинців, що допоможе співробітникам правоохоронних органів у розслідуванні даної категорії злочинів. Саме тому метою статті є розроблення моделі комп'ютерних злочинців.

Виклад основного матеріалу. За Ігошевим К.Е., суб'єкт злочину є мінімальною сукупністю ознак, які характеризують особу, яка скоїла злочин, які необхідні, аби притягнути її до кримінальної відповідальності. На думку вченого, особистісні якості людини і зовнішнє середовище у взаємодії визначають мотивацію прийняття рішення щодо злочинної діяльності у сфері використання комп'ютерних технологій [3, с. 105].

Снігерьов О.П. та Сергач О.І. зазначають, що суб'єктом комп'ютерних злочинів можуть бути як особи, що мають доступ до комп'ютерної системи (програмісти, оператори ЕОМ, наладчики обладнання, користувачі), так і сторонні громадяни [4, с. 85].

Згідно зі статтєю 20 КК України суб'єктом злочину, передбаченого ч. 1 ст. 361 КК України, може бути будь-яка фізична особа, яка на момент скоєння злочину досягла шістнадцятирічного віку. Це загальна кримінальна правосуб'єктність. Обов'язковою умовою притягнення особи до кримінальної відповідальності за вчинене суспільно небезпечне протиправне діяння є її осудність – здатність розуміти суспільну значимість своїх дій та керувати

ними. Неосудні особи не підлягають кримінальній відповідальності (ст. 21 КК України). Тобто спеціальним суб'єктом у даному випадку є особа, яка, крім наявності осудності та досягнення віку кримінальної відповідальності, також має певні спеціальні ознаки, які вказані в нормі права (спеціальні ознаки).

До ознак, притаманних комп'ютерним злочинцям, можливо віднести:

1. Нявність необхідник знань, навичок і вмінь у роботі з ЕОМ;

2. Можливість доступу до комп'ютерних мереж.

Коло суб'єктів комп'ютерної злочинності не має жодних обмежень, тому правопорушники можуть мати відношення до досить різних сфер діяльності та мати різний рівень підготовки. У більшості випадках комп'ютерні злочини здійснюються особами, які мають досить високу кваліфікацію, тому чим складніший спосіб вчинення злочину, тим вужче коло вірогідних злочинців.

Суб'єкти комп'ютерних злочинів розподіляються на певні види, в залежності від сфер діяльності:

1. Комп'ютерні злочини, що скоюються операторами ЕОМ, периферійних пристроїв введення інформації в ЕОМ і обслуговуючими лінії телекомунікації.

2. Злочини, пов'язані з використанням програмного забезпечення, зазвичай скоюються: системними програмістами; особами, у віданні яких знаходяться бібліотеки програм; прикладними програмістами або ж добре підготовленими користувачами.

3. З апаратурної частини комп'ютерних систем небезпеку скоєння злочинів становлять: системні адміністратори, інженери, інженери термінальних пристроїв, інженери-електронщики, інженери-зв'язківці.

4. Співробітники, які займаються організаційною роботою: управлінням комп'ютерною мережею, керівництвом операторами; керівництвом роботи з використанням програмного забезпечення; управлінням базами даних.

5. Працівники служби безпеки, працівники, які контролюють функціонування ЕОМ.

6. Спеціалісти у випадку змови з керівниками підрозділів і служб, а також з організованими злочинними групами.

Особи, які мають вагомі знання в області комп'ютерних технологій та в більшості керуються корисливими мотивами, становлять підвищену небезпеку. До цієї ж групи належать також і спеціалісти, які засоби щодо безпеки сприймають як виклик своєму професіоналізму [3, с. 106].

Одним з таких хакерів є Адріан Ламо на прізвисько «Бездомний хакер». Він досліджував системи безпеки найбільших компаній (Microsoft, NY Times, Yahoo, Bank of America), зламуючи їх, та надавав інформацію про прогалини в базах компаній, тим самим допомогаючи їм.

Відповідно до результатів досліджень, які проводилися спеціалістами Dafapro Information Services Group, відмічено значне збільшення кількості спроб несанкціонованого доступу до інформації, яка міститься в комп'ютерній мережі загального використання [5, с. 1–3; 2, с. 77].

Під час проведення комплексного аналізу суб'єктів комп'ютерних злочинів виявилося, що станом на 1 січня 2017 року населення України становило 42 584,5 тис. осіб [6], за даними дослідження Інтернет-Асоціації України на початок 2017 року нараховано 21,6 млн користувачів Інтернет [7], тобто 50 відсотків українців є користувачами мережі Інтернет. За показниками Державної Судової Адміністрації, згідно зі звітом судів першої інстанції про розгляд матеріалів кримінального провадження у 2017 році надійшло 79 проваджень [8] за злочини у сфері використання ЕОМ (комп'ютерів) систем та комп'ютерних мереж (ст. 361–363-1 КК).

Відповідно до звіту Державної судової адміністрації України про склад засуджених за 2017 рік за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж (ст. 361–363-1 КК) було засуджено 42 особи, з яких 32 злочини (76%) вчинено чоловіками та 9 – жінками (24%). У 26% дана категорія злочинів вчинялася у складі груп (11). Найбільш розповсюдженими комп'ютерними злодіями на протязі 2017 року стали особи віком від 30 до 50 років (53%), віком від 25 до 30 років (26%), від 18 до 25 років (14%), віком від 50 до 65 років (5%) та від 65 років і вище (2%). Класифікуючи суб'єктів вчинення комп'ютерних злочинів за сферами діяльності, виявилося, що 55% злочинів вчинялися працездатними, які не працювали та не навчалися – найвищий показник; 2% становлять працівники господарських товариств [9]. Комп'ютерні злочини можуть вчиняться і керівниками організацій, адже вони володіють достатньою комп'ютерною підготовкою і професійними знаннями, мають доступ до інформації обмеженого доступу та наділені можливістю віддавати розпорядження, до того ж безпосередньо не відповідаючи за роботу комп'ютерної системи. У професійно-кваліфікаційному плані коло комп'ютерних злочинців досить широке: комерційні директори, банківські службовці, фінансисти, програмісти, інженери-наладчики і монтажники комп'ютерного устаткування, бухгалтери тощо [10, с. 431–441; 2, с. 78].

З цього можна зробити декілька висновків: комп'ютерні злочини можливо вчиняти без особливих знань в області комп'ютерної техніки за наявності вільного часу; діаметрально протилежна думка: чим нижчий рівень знань у сфері ЕОМ, автоматизованих систем, тим більший ризик бути виявленим.

Суб'єктом «несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку» та «створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, їх реалізації або збуту» є фізична осудна особа, якій до вчинення злочину виповнилось шістнадцять років.

Суб'єктом умисного комп'ютерного злочину, такого як, зокрема, злочин, передбачений ст. 361 КК, є особа, яка всі свої знання і волю спрямовує на досягнення злочинного результату: доступу до інформації, її перекручення, розповсюдження комп'ютерного вірусу або інших шкідливих комп'ютерних програм. Якщо припустити можливість вчинення комп'ютерного зло-

чину неосудною особою, стає очевидним, що в її діях не буде форми вини, за відсутністю якої в юридичному складі конкретного злочину не можуть бути визначені не лише суб'єкт, а й суб'єктивна сторона злочину. При цьому не можна виключати випадків вчинення комп'ютерних злочинів неосудними особами.

Як зазначає Міхєєв Р.І., осудність тісно пов'язана з віком кримінальної відповідальності. Вік у кримінальному праві, поряд з осудністю, є одним з обов'язкових загальних умов визнання особи винною і відповідальною за скоєне [11, с. 65]. Однак на практиці хакери-підлітки яскраво конкурують з дорослими. Лазарєв А.М. вказує: «Інтелектуальний розвиток юнаків досягає високого ступеню і якісно не відрізняється від рівня інтелектуального розвитку дорослих. Хоча мислення неповнолітніх протікає по тих же законах вищої нервової діяльності, що і в дорослих, однак у них воно не досягає тієї зрілості, яка притаманна дорослим. Поступаються неповнолітні юнацького віку і по рівню вольового розвитку. Недостатнє вольове «загартування» в значному ступені пояснює підвищену емоційність, збуджуваність, яка легко переходить в запальність, психічну неврівноваженість, що породжує схильність до афектованих спалахів» [12, с. 21]. Однак, незважаючи на це, малолітні кібер-злочинці спроможні завдати значну шкоду охоронюваним суспільним інтересам. В мережі Інтернет постійно публікуються повідомлення, які підтверджують дійсність такого твердження.

На даний час на створення малолітніх «хакерів» впливає комп'ютеризація, в процесі якої вони не можуть завжди сприймати комп'ютерну злочинність як таку, вважаючи це просто цікавим проведенням часу. До того ж вони ще не наділені свідомістю дорослої людини, як здатна усвідомлювати протиправність таких вчинків. Під впливом інформаційного навантаження малолітні діють фактично під психологічним примусом з боку засобів масової інформації, преси, загальних кумирів, моди на комп'ютерні правопорушення [13]. Можливе подальше зниження віку настання кримінальної відповідальності, що обумовлено частими правопорушеннями, пов'язаними з незаконним доступом до комп'ютерної інформації, які здійснюються неповнолітніми особами, котрі не досягли віку кримінальної відповідальності.

Частка злочинів, що полягають у розповсюдженні шкідливих програм для електронно-обчислювальної техніки за 2017 рік, становить 5% від загальної кількості комп'ютерних злочинів. У більшості випадків розповсюдження дисків, які містять шкідливі програми, здійснюється переважно під час реалізації піратського програмного забезпечення. До складу таких дисків зазвичай входять різні набори програм, призначених для «зламування» комп'ютерних систем, а також шкідливі програми – програмні вкладення та віруси [14, с. 42].

Аналізуючи XVI Розділ КК України «Злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку», специфічний суб'єкт міститься у статті 362 КК України «Несанкціоновані дії з інформацією, яка обробляється 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». Це випадок, коли певні якості суб'єкта прописані в диспозиції статті КК.

Нормою статті 362 КК України визначено ознаку спеціального суб'єкта – наявність в особи права доступу до інформації, що обробляється в ЕОМ, АС чи комп'ютерних мережах або зберігається на носіях такої інформації. Ришелюк М.А. вважає, що право доступу до інформації безпосередньо пов'язане з виконанням суб'єктом злочину трудових, службових обов'язків або внаслідок наданого власником інформації дозволу [15, с. 951]. На думку Бутузова В.М., Остапця С.Л. та Шелонцева В.П., така особа має право доступу до інформації, що є предметом злочину, у зв'язку із займаною посадою або виконанням спеціальних повноважень. Доступ до такої інформації здійснюється лише згідно з правилами розмежування доступу, встановленими власником такої інформації чи уповноваженою ним особою, а користувачі інформації визначаються власником інформації або уповноваженою ним особою, ними ж встановлюються їхні повноваження [16, с. 31].

Таким чином, суб'єктами комп'ютерних злочинів згідно з КК України можуть бути:

1. Загальний суб'єкт – фізична осудна особа, яка досягла шістнадцятирічного віку (ст. 361, 361-1, 361-2, 363-1 КК України);

2. Особа, що має право доступу до інформації, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362 КК України);

3. Особа, яка відповідає за експлуатацію ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку (ст. 363 КК України) [17, с. 114].

Висновки. У ході проведення наукового дослідження вдалося виявити, що найбільшу частку комп'ютерних злочинів вчиняли чоловіки віком від 30 до 50 років. На нашу думку, розумного, досвідченого хакера або не помічають, або не можуть знайти (якщо вже проявилися суспільно-небезпечні наслідки), або ж розшукують у разі вчинення глобальних злочинів. Як показує практика, найвідоміші хакери світу після відбування покарань продовжують займатися своєю справою: відкривають власні школи, курси, допомагають правоохоронним, у тому числі секретним, службам, адже гарні фахівці в даній сфері дуже цінні, і злочинна діяльність сьогодні може стати неоцінимою допомогою державі завтра. Не можна забувати і про прояви латентності, халатності по відношенню до суспільної небезпечності комп'ютерних злочинів; випадки незнання законодавства та розуміння протиправності вчинюваних злочинів. Тож, можна стверджувати, що в більшості випадків злочини вчиняються розумними, досвідченими фахівцями. Цікавий і той факт, що на відміну від інших злочинів, не було виявлено вчинення комп'ютерних злочинів під впливом алкогольних чи наркотичних засобів, отже, ці злочини вимагать високої концентрації та наполегливості. Тому комп'ютерні злочини можливо назвати високоінтелектуальними злочинами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Kriminalistik. 1987. № 5. S. 265–267.
2. Борисова Л.В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. Актуальні проблеми держави і права. 2008. Вип. 44. 356 с. URL: http://nbuv.gov.ua/UJRN/apdp_2008_44_15
3. Голубєв В.О. Суб'єкт злочинної діяльності у сфері використання електронно-обчислювальних машин. URL: http://vlz.in.ua/uploads/File/pdf/St/2003-s/2003-12s/Golubev03-12.pdf
4. Снігірьов О.П., Сергач О.І. Деякі правові проблеми злочинності в сфері комп'ютерної інформації. Інформаційні технології та захист інформації. Збірник наукових праць. Міністерство внутрішніх справ України. Запорізький юридичний інститут. Випуск № 1. 1998. С. 85.
5. Dalapro Reports on Information Security. 1990-1993. Vol. 1–3.
6. Населення України / Мінфін. URL: https://index.minfin.com.ua/ua/reference/people/2017
7. В Україні на початок 2017 року нараховано 21,6 млн користувачів інтернету / Semantrum. URL: https://promo.semantrum.net/uk/2017/04/21/v-ukrayini-na-pochatok-2017-roku-narahovano-21-6-mln-koristuvachiv-internetu
8. Звіт судів першої інстанції про розгляд матеріалів кримінального провадження за 2017 рік. Форма 1-1 / Офіційний сайт. Судова влада України. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017
9. Звіт про склад засуджених за 2017 рік. Форма 7 / Офіційний сайт – Судова влада України. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017
10. Straub D.W., Widom C.S. Deviancy by bits and bytes: computer abusers and control measures. Computer Security: A Global Challenge. Netherlands, 1984. P. 431–441.
11. Михеев Р.И. Основы учения о вменяемости и невменяемости. Владивосток: ДВГУ, 1980. С. 65.
12. Лазарев А.М. Субъект преступления. М.: Министерство высшего и среднего образования СССР. Всесоюзный юридический заочный институт, 1981. С. 21.
13. Розенфнльд Н. Суб'єкт злочину «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), їх систем та комп'ютерних мереж». Центр исследования проблем компьютерной преступности. URL: http://www.crime-research.org/library/Rozenf.htm
14. Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. 268 с.
15. Науково-практичний коментар Кримінального Кодексу. 4-те вид., перероб. та допов. / за ред. М.І. Мельника., М.І. Хавронюка. К.: Юридична думка, 2007. С. 951.
16. Бутузов В.М., Остапець С.Л., Шеломцев В.П. Злочини у сфері використання електронно-обчислюваньних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. ком. К.: Друкарня МВС України, 2005. 86 с.
17. Плугатир М. Особа, що має право доступу до комп'ютерної інформації як суб'єкт злочину, передбаченого ст. 362 КК України. Юридична Україна. Кримінально-правові науки. 2010. № 1. С. 113–116.