УДК 343.98.06

Олена Самойленко,
канд. юрид. наук, доцент,
доцент кафедри криміналістики
Національного університету «Одеська юридична академія»

ТИПИЗАЦІЯ ОСОБИ, ЩО ВЧИНЯЄ ЗЛОЧИН, ПОВ'ЯЗАНИЙ ІЗ ВИКОРИСТАННЯМ ОБСТАНОВКИ КІБЕРПРОСТОРУ (З ПОЗИЦІЙ КРИМІНАЛІСТИЧНОЇ НАУКИ)

У статті з позицій криміналістичної науки здійснюється типізація осіб, що скоюють злочини з використанням обстановки кіберпростору. Окрема увага приділяється визначенню стосовно вказаної категорії злочинів закономірних зв'язків у системах «злочинець – організована група», «типові сліди – злочинець» та «злочинець – специфіка злочинної діяльності». Сформульовані автором положення сприятимуть практичній роботі слідчих та оперативних підрозділів у контексті встановлення комплексу взаємопов'язаних злочинів, учинених із використанням обстановки кіберпростору.

Ключові слова: кіберпростір, мобільність, обстановка, особа злочинця, технології анонімізації, фахівець.

Постановка проблеми. Ознаки та якості особи злочинця, що прямо впливають на регуляцію злочинної діяльності, завжди зумовлюють природу слідів злочину, однак і сам злочинець перебуває під впливом об'єктивних умов навколишнього середовища, яке може позначатися на злочинцеві вже в момент початку злочинної діяльності. Оскільки сьогодні все частіше навколишнім середовищем злочинця стає кіберпростір, то в криміналістичній науці постає проблема типізації особи такого злочинця.

Аналіз останніх досліджень і публікацій з даної теми. У контексті характеристики особи злочинця, що діє із використанням обстановки кіберпростору, безумовно, варті уваги роботи П. Д. Біленчука, В. Б. Вехова, В. В. Крилова, В. В. Кравчука, С. В. Кригіна, В. М. Кулика та багатьох інших науковців. Майже традиційним став розподіл комп'ютерних злочинців, які здійснювали несанкціоноване втручання в систему, за метою та сферою їхньої діяльності на: «хакерів» (які отримують задоволення від вторгнення в систему та її вивчення), «кракерів» (втручаються з метою завдавання шкоди системі), «фріків» (мають на меті отримання кодів доступу до послуг, паролів тощо), «колекціонерів» (колекціонують та використовують програмні продукти), «кіберкруків» (здійснюють мережеві шахрайства), «комп'ютерних піратів» (злам продуктів та їх розповсюдження за плату) й багато інших видів [1, с. 133–134]. Однак сфера діяльності злочинця не завжди відображає зв'язок особи злочинця, що використовує обстановку кіберпростору для вчинення злочину, з типовими слідами його вчинення. На наше переконання, фактично рівень професіональності конкретної особи як користувача комп'ютера зумовлює можливість змінення нею сфери діяльності.

Мета статті полягає у визначенні типів особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору, на підставі професіонального рівня користувача як злочинця.

Виклад основного матеріалу. Маркетологи з ринку праці визначають такі фахові рівні користувачів комп'ютерів: користувач, упевнений користувач, досвідчений користувач, користувач професійного рівня [2]. Критеріями такої диференціації слугують кількість програм, які опанував користувач; ступінь опанування ним кожної з програм; рівень професійної самооцінки. З урахуванням того кримінологи наводять три типи комп'ютерних злочинців: «початківці», «злочинці, що закріпились» та «професіонали» [3]. Формальне застосування такого роду підходів для типізації особи злочинця, що діє з використанням обстановки кіберпростору, не матиме практичного сенсу з позицій формулювання типових версій про особу злочинця. Адже професійний рівень користувача не відображає всього спектру ознак злочинця, активно задіяних у процесі детермінації механізму злочину.

На нашу думку, слідчий на підставі аналізу слідів учинення злочину з використанням

обстановки кіберпростору може висновувати про професіональний рівень користувача як злочинця, що зумовлений певною сукупністю ознак, як-от: 1) здатність злочинця використовувати технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів-анонімайзерів); 2) мобільність злочинця (індивідуальна професійна, соціальна або географічна) [4]; 3) психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети; 4) роль у складі організованої злочинної групи. Щодо першої ознаки, то вільний доступ користувачів до технологій анонімізації під час роботи в мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж (VPN-технологій) та інших засобів-анонімайзерів) не означає, що кожний такий користувач використовує технологію правильно. Щодо другої, то мобільність означає здатність швидко орієнтуватися в ситуації, вибирати найбільш доцільні форми діяльності [5, с. 682]. Щодо третьої, то злочинцям, що діють із використанням обстановки кіберпростору, притаманний вольовий компонент людської психіки. У цьому сенсі можна провести паралелі між вольовою дією особи та її злочинною діяльністю з використанням кіберпростору. По-перше, зловмисник свідомо вчиняє одиничний злочин шляхом елементарної вольової дії або комплекс органічно взаємопов'язаних злочинів шляхом складної вольової дії. По-друге, його діяльність завжди є вмотивованою, причому від складності злочинної діяльності в кіберпросторі залежить конкуренція мотивів учинення. Четверта ознака – роль злочинця у складі організованої групи – перетинається з кримінологічним дослідженням мережевої або корпоративної моделі як видів організованої групи, що протиставляються між собою [6, с. 81; 7].

З огляду на вищенаведені теоретичні позиції, спираючись на узагальнення матеріалів національної судово-слідчої практики й на підставі наведених нами критеріїв визначення професіональності (кваліфікації) злочинця можна певним чином типізувати особу, що вчиняє злочин з використанням обстановки кіберпростору.

Злочинець-користувач початкового рівня з урахуванням своїх професійних навичок роботи з комп'ютером не використовує технології анонімізації доступу до ресурсів Інтернет; характеризується високою соціальною мобільністю з різних причин (нереалізованість комунікаційних потреб (людина з обмеженими фізичними можливостями, наявність психічних хвороб), йому властива наявність географічної мобільності за відсутності професійної та економічної мобільності (сезонний працівник; робота за кордоном вахтовим методом; кур'єр; водій; сортувальник тощо, причому злочинець виконує роботи низької кваліфікації)). Проблеми конкуренції мотивів учинення злочину він не має, його злочинна діяльність зазвичай становить собою елементарну вольову дію, як-от розміщення в мережі Інтернет інформації певного змісту.

Злочинець такого типу вчиняє в кіберпросторі злочини, пов'язані з насильницько-егоїстичними чи насильницько-дискримінаційними діями, окремі види злочинів з антидержавно-політичних мотивів (злочини проти основ національної безпеки України; злочини, пов'язані з тероризмом; пропаганда війни й поширення комуністичної, нацистської символіки та пропаганда комуністичного й націонал-соціалістичного (нацистського) тоталітарних режимів). Наведемо приклад [8]. Мешканець Херсонської області гр. К., зареєстрований як користувач соціальної мережі «ВКонтакте» («Інтернет ресурс» – «http://vk.com») під своїм «ніком», у період з 25 березня 2011 року до 03 жовтня 2014 року на особистій сторінці в розділі «Новини», переглядаючи відеофайли, розміщені невстановленою особою в розділі «Новини» зазначеної соціальної мережі, яку технічними та іншими засобами встановити неможливо, що за висновком експерта містять ознаки порнографії та належать до продукції порнографічного характеру, за допомогою функції «додати в мої відеозаписи» надав загальний доступ для перегляду цих десяти відеозаписів користувачам соціальної мережі. К. було засуджено за вчинення злочинів, передбачених ч. 2 ст. 300, ч. 2 ст. 301 КК України.

Учиняючи злочини з антидержавно-політичних мотивів, вони можуть діяти як самостійно, так і в складі корпоративної злочинної групи, виконуючи роль організатора, виконавця чи посібника. Так, наприклад, упродовж травня-липня 2014 року гр. О., діючи за попередньою змовою з іншими невстановленими особами, через соціально спрямовані Інтернет-ресурси «ВКонтакте», «Одноклассники», «Facebook», програми «Skype», «Viber», з використанням мобільного зв'язку організовував акції протесту проти дій органів державної влади України в містах Києві, Львові, Тернополі, Кіровограді, Запоріжжі, Дніпропетровську, Одесі, Миколаєві, Херсоні, Полтаві, Миргороді, залучаючи до цього мешканців різних регіонів України [9]. Також він організовував їх фінансування, детально інструктував щодо порядку проведен-

ня акцій, бажаного результату, обов'язкового використання засобів масової інформації, як місцевих, так і загальнодержавних, вимагав складання й надіслання йому фото- та відеозвітів про виконану роботу, а також ставив завдання щодо залучення учасників акцій.

Таких злочинців працівники правоохоронних органів найчастіше виявляють під час моніторингу комп'ютерних мереж. Унаслідок учинення злочинцем-користувачем початкового рівня злочину зазвичай залишаються такі сліди: 1) нетрадиційні – в комп'ютері злочинця у вигляді змін у файловій системі, спеціального програмного забезпечення, інформації на зйомних носіях; на сервері національного оператора або провайдера у вигляді спеціальних файлів реєстрації, так званих Log-файлах, де відбувається протоколювання технічної інформації, що містить відомості про технічний обмін, бази даних; 2) традиційні (матеріальні) сліди у вигляді документів (офіційних та неофіційних).

Злочинець-користувач. Інтерес працівників правоохоронних органів до такого злочинця найчастіше виникає під час проведення оперативно-розшукової діяльності. Якщо злочинець і використовує технології анонімізації доступу до ресурсів мережі Інтернет (часто Tor), то припускається значних помилок, що зводять нанівець його намагання бути анонімним у мережі. Фахівець із комп'ютерного обладнання та мереж під час побіжного аналізу комп'ютера жертви й мережі досить легко визначить фактичні відомості про особу, котра здійснювала певну операцію. Усі види мобільності (географічна, соціальна, професійна та економічна) мають усереднені схожі показники. Втім, розглядаючи географічну мобільність у контексті ринку праці, слід визнати нетиповість «дистанційної роботи» такої особи. Конкуренція мотивів наявна лише за умови діяльності його в складі мережевої злочинної групи: коли він приймає рішення щодо подальшого виконання ролі в групі або вчинення іншого злочину, виявляючи ознаки організатора однієї зі складових мереж мережевої групи. Злочинець такого типу часто вчиняє в кіберпросторі злочини, віднесені до таких класифікаційних підгруп: злочини, що порушують встановлений порядок обігу певних речей; інтелектуальне піратство, злочини, пов'язані з комунікаційними діями. Показовою можна вважати діяльність гр. А., який у квітні 2015 року створив Інтернет-сайти з метою отримання прибутку від розміщеної на сайті реклами. Оскільки рекламні сайти як такі не користуються попитом серед користувачів Інтернету, для привернення уваги на своїх сайтах А. надавав користувачам можливість перегляду фільмів у режимі «он-лайн». Загальна сума збитків, спричинених власникам авторських прав наданням доступу до аудіовізуальних творів компаній «Twentieth Century Fox Film Corporation» та «Universal City Studios LLLP» (Universal) на сайтах «live-films.in.ua» та «kinozal.biz.ua» («kinozal.tech»), становила 2 363 398 грн [10].

Трапляються випадки вчинення зловмисниками злочинів з антидержавно-політичних мотивів, пов'язаних із державно-політичною сферою відносин суб'єктів у кіберпросторі. До прикладу, гр. К. за місцем проживання через можливості провайдера ТОВ «ПТК» з використанням встановленого на його ноутбуці Інтернет-браузера «Opera» з активованим сервісом «VPN» авторизувався в соціальній Інтернет-мережі «ВКонтакте» та від імені створеного ним аккаунта розповсюдив репости записів із закликами до змінення меж території та державного кордону України, порушуючи порядок, встановлений Конституцією України [11].

Інтерес працівників правоохоронних органів до такого злочинця виникає найчастіше під час проведення оперативно-розшукової діяльності (оперативної розробки). Після вчинення злочину злочинець-користувач залишає такі типові сліди: 1) нетрадиційні – в комп'ютері на робочому місці злочинця у вигляді змін у файловій системі та наявності певного спеціального програмного забезпечення, інформації на зйомних носіях; у сервері, в комп'ютері-жертві у вигляді змін в оперативному запам'ятовуючому пристрої, у конфігурації, позаштатних режимів роботи; на серверах національного та/або закордонного оператора/провайдера у вигляді спеціальних файлів реєстрації, баз даних; 2) традиційні матеріальні сліди у вигляді слідів-предметів (офіційних та неофіційних документів); речей, що мають особливий порядок обігу (спеціальні технічні пристрої, зброя тощо); слідів-відображень (відбиток пальця, мікрочастка одягу на засобах комп'ютерної техніки та поруч із ними); слідів-речовин (наркотичні засоби; прекурсори, вибухова речовина тощо).

Злочинець-упевнений користувач зазвичай пов'язаний з організацією-жертвою за трудовою угодою або має особисті стосунки з фізичною особою-жертвою (90 % матеріалів), через це має доступ до інформації, необхідної для вчинення злочину (ідеться про паролі, адреси, коди доступу, назву файлу, шлях до нього тощо). Втім цей факт не заважає йому досить вдало використовувати технології анонімізації доступу до ресурсів мережі Інтернет з метою приховування злочинної діяльності, створення ілюзії віддаленого

доступу до предмета посягання. Серед видів мобільності переважають соціальна та професійна, інші мають середні показники. Злочинець зазначеного типу традиційно вчиняє в кіберпросторі злочини, спрямовані на заволодіння чужим майном та пов'язані з ними злочини у сфері функціонування електронних розрахунків; злочини, що порушують механізми захисту від монополізму та недобросовісної конкуренції; інтелектуальне піратство та злочини, пов'язані з комунікаційними діями; злочини, пов'язані з анархістськими діями в кіберпросторі. До речі, 80 % матеріалів кримінальних проваджень стосовно наведеної категорії злочинів кваліфікуються за сукупністю статей, де обов'язковим елементом постають злочини, що передбачені розділом XVI КК України. Такий злочинець приблизно в половині випадків діє в складі корпоративної організованої групи як виконавець злочину.

Розглянемо приклад [12]. Гр. А., перебуваючи на посаді старшого оперуповноваженого з особливо важливих справ інформаційно-моніторингового відділу Управління координації та моніторингу ризиків Головного управління внутрішньої безпеки Міністерства доходів і зборів України, діючи умисно, з корисливих мотивів з вересня 2013 року до лютого 2014 року на початку кожного місяця, перебуваючи в м. Києві, неодноразово здійснював несанкціонований збут інформації з обмеженим доступом щодо експортно-імпортних операцій на митній території України, що зберігається в Єдиній автоматизованій інформаційній системі (ЄАІС) Міндоходів, громадянину України Б. за щомісячну грошову винагороду в розмірі від 1000 до 2000 гривень. Несанкціоноване копіювання інформації здійснювалося з робочого місця іншої особи без відома та за відсутності останньої. Для входу в ЄАІС А. використовував свій особистий логін та пароль. Збут інформації відбувався шляхом завантаження файлів з інформацією за допомогою комп'ютерної техніки, розташованої в різних місцях через ресурси «http://rusfolder.ru», «http://www/sendspace.com» («файлообмінники»). Надалі пароль для їх завантаження покупець отримував через електронну поштову скриньку під час електронного листування. Окремо надавався пароль для розархівування файлів. З метою приховування своєї протиправної діяльності, досягнення максимальної конспірації та уникнення відповідальності за скоєні дії А. за реалізовані ним інформаційні масиви з обмеженим доступом отримував грошові кошти через «електронні гаманці» системи «WebMoney Transfer», зокрема, за реквізитами, зареєстрованими ним на вигаданих осіб. Кінцевим рахунком для отримання грошових коштів у готівковій формі був «електронний гаманець» за реквізитами А.

Типовим первинним джерелом інформації про такого злочинця стає заява або повідомлення про вчинення кримінального правопорушення. Унаслідок скоєння злочину «злочинцем-упевненим користувачем» зазвичай залишаються такі сліди: 1) нетрадиційні – в комп'ютері, який застосовував злочинець, у вигляді змін у файловій системі, спеціального «хакерського» програмного забезпечення; в комп'ютері-жертві у вигляді змін в оперативному запам'ятовуючому пристрої, у конфігурації, позаштатних режимів роботи; на серверах частіше національного оператора/провайдера у вигляді спеціальних файлів реєстрації, баз даних; 2) традиційні – матеріальні сліди у вигляді слідів-предметів (офіційних та неофіційних документів); додаткових технічних пристроїв; спеціалізованої конфігурації обладнання, нестандартного периферійного обладнання); слідів-відображень та слідів-речовин (фарба для принтера, порошки та змазки для техніки; клеї, чистий пластик і фарби для виготовлення підроблених банківських пластикових карток тощо).

Злочинець-досвідчений користувач. Між досвідченим та впевненим злочинцем-користувачем відмінності є незначними. Це пов'язано з тим, що впевнений злочинець має високий рівень професійної мобільності й у разі невикриття правоохоронними органами першого скоєного ним злочину він підвищує свій професійний рівень, часто відмовляється від участі в організованій злочинній групі та розпочинає індивідуальну злочинну діяльність. Як фахівець високої кваліфікації, він використовує технології анонімізації доступу до ресурсів мережі Інтернет, через що має високий ступінь географічної мобільності. Злочинну діяльність учиняє шляхом складної вольової дії, тому завжди наявна конкуренція мотивів. Встановлення під час досудового розслідування факту наявності конкуренції мотивів злочинця та шляхів розв'язання цієї проблеми дозволить надалі зазначити необхідність залучення слідчим психолога з метою визначення психотипу, складання психологічного портрету злочинця. Для злочинця цього типу характерним є скоєння злочинів, спрямованих на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків; злочинів, що порушують механізми захисту від монополізму та недобросовісної конкуренції: інтелектуального піратства та злочинів, пов'язаних із комунікаційними

діями. Аналогічно до попереднього типу понад половина таких злочинів підлягають кваліфікації за сукупністю зі статтями розділу XVI КК України (класифікаційна підгрупа злочинів, пов'язаних з анархістськими діями в кіберпросторі). Комплекс слідів злочину, які залишає досвідчений користувач, майже аналогічний слідам, залишеним упевненим користувачем, на відміну до того, що нетрадиційні сліди часто залишаються на серверах закордонного оператора/провайдера.

Так, у м. Біла Церква Київської області гр. Н. з метою здійснення DDoS-атак на будь-які сервери за винагороду завантажив та скопіював на жорсткий диск свого комп'ютера з Інтернету програмне забезпечення, необхідне для організації та проведення DDoS-атак за назвою «Bleck Energy», що надавало йому можливість здійснювати DDoS-атаки на вибрані ним сервери, IP-адреси та ресурси [13]. Виконавши тестування зазначеного програмного продукту, Н., спілкуючись на сторінках форуму «xakerok.org», від не встановленої слідством особи отримав додатковий спеціальний «файл динамічної бібліотеки» «*.dll», після чого програмний продукт «Bleck Energy» став повністю придатним для здійснення DDos-атак. Також від не встановленої слідством особи на імя «Botnetman» зловмисник отримав так званий «Botnet» (файл управління комп'ютерами, зараженими вірусами), що надавав можливість одночасно з 1000 комп'ютерів здійснити звернення на той чи інший сервер, IP-адресу чи ресурс у мережі Інтернет, таким чином паралізувавши його роботу. 21.02.2008 р. Н. за допомогою ICQ (програма для відправлення повідомлень у мережі Інтернет) з № 475917365 (псевдонім «Botanik») та № 400349 (без псевідоніму) на форумах сайту «www.xakery.ru» розмістив оголошення в розділі «DDoS service» з приводу проведення DDoS-атак на буд-які сервери за винагороду. 04.07.2008 на ці оголошення на ICQ № 475917365 до Н. від не встановленої слідством особи, представленої під псевдонімом «Wolf», надійшло замовлення на проведення DDoS-атаки на сервери за різними IP-адресами, належними ТОВ «ОСМП», ТОВ «Кіберплат Україна». Виконуючи заказ, Н. увійшов у глобальну мережу Інтернет на ресурс «www.cxim.inattack.ru/www2/www» та за допомогою програми «Bleck Energy» протягом доби здійснював DDoS-атаки на сервери зазначених компаній, за що від «Wolf» на зареєстрований у мережі Інтернет гаманець в електронній платіжній системі отримав винагороду в розмірі 100000 рублів, які згодом перевів у гривні на власну платіжну картку.

Злочинець-користувач професіонал. Здатність такого злочинця до використання технологій анонімізації доступу до ресурсів Інтернет, індивідуальна професійна, соціальна та географічна мобільність злочинця, складність його злочинної діяльності (що визначає психотип злочинця) характеризуються найбільш високим рівнем кваліфікації. Це вимагає максимальної концентрації зусиль працівників поліції, залучення до розслідування значної кількості спеціалістів різного фаху, здійснення діяльності в межах міжнародного співробітництва. Для слідчого або кіберполіцейського в процесі розслідування відповідної злочинної діяльності ключовою обставиною слугуватиме участь злочинця такого типу в складі організованої групи або злочинної організації з транснаціональними зв'язками. Як приклад можна навести групу так званих «балаківських хакерів», діяльність яких було докладно описано в російських джерелах інформації [14]. Організована група осіб у 2003 році здійснювала кібератаки на інтернет-сайти дев'яти букмекерських британських компаній. Їхні web-сторінки було заблоковано й робота припинилася. Для розблокування роботи сторінки злочинці вимагали передати гроші.

Можна назвати три закономірності злочинної діяльності осіб відповідного типу: 1) «професіонал» зазвичай є одним з організаторів у структурі мережевої організованої групи, створеної для вчинення злочинів з корисливих мотивів, пов'язаних із фінансово-економічною сферою відносин у кіберпросторі, та із соціально-економічних мотивів, пов'язаних із соціальною сферою відносин суб'єктів; 2) «професіонал» зазвичай вчиняє на замовлення третьої особи будь-який зі злочинів з антидержавно-політичних мотивів або ідейних мотивів, пов'язаних зі світоглядною сферою; 3) злочини, пов'язані з анархістськими діями в кіберпросторі, «професіонал» може вчиняти одноособово (за відсутності сукупності зі злочином іншої класифікаційної підгрупи досліджуваної категорії злочинів). Втім, через брак матеріалів практики щодо фактичного притягнення до кримінальної відповідальності на території України «професіоналів» визначені статистичні показники у наведених закономірностях чітко визначити на цей час неможливо.

Як приклад маємо такий випадок [15]. У Херсонській області за вчинення кримінального правопорушення, передбаченого ч. 2 ст. 361-1 КК України, до відповідальності було притягнуто двох осіб. Гр. А., маючи спеціальні технічні знання у сфері

програмування, за допомогою не встановленого досудовим розслідуванням комп'ютера з метою використання та розповсюдження на базі операційної системи «Android» створив програмне забезпечення за назвою «grafon.apk» та файл «restricted» для мобільних комп'ютерів, після чого передав гр. Б. логін і пароль доступу до панелі управління зазначеного програмного забезпечення. У не встановлений слідством день і час у травні 2016 року через панелі управління бот-мережею «SexDrugWokrug.apk», використовуючи не встановлений досудовим розслідуванням комп'ютер, А. використав і розповсюдив через низку власних сайтів зазначене програмне забезпечення з метою отримання віддаленого доступу та проведення несанкціонованих операцій з платіжними засобами українських і зарубіжних користувачів та подальшого виведення грошових коштів із вказаних платіжних засобів через систему миттєвих інтернет-розрахунків «WebMoney Transfer» на власні банківські рахунки.

Інформацію про вчинення кримінального правопорушення злочинцем такого типу вдається отримати в результаті проведення оперативно-розшукової діяльності працівниками правоохоронних органів, а також під час діяльності в порядку надання міжнародної правової допомоги. При цьому нетрадиційні й традиційні сліди злочину зазвичай містяться на місці підготовки до злочину (розробки вірусу, програм зламу, добору паролів) та місці (комп'ютері, сервері або стримері) обробки інформаційного продукту як предмета посягання.

Висновки

Таким чином, спираючись на узагальнення матеріалів національної судово-слідчої практики й на підставі визначених нами критеріїв, ми запропонували такі типи особи злочинця, що вчиняє злочин із використанням обстановки кіберпростору: 1) злочинець-користувач початкового рівня; 2) злочинець-користувач; 3) злочинець-упевнений користувач; 4) злочинець-досвідчений користувач; 5) злочинець-користувач професіонал. Вважаємо, що така типізація особи злочинця дозволить визначити закономірні зв'язки в системах «злочинець – організована група», «типові сліди – злочинець» та «злочинець – специфіка злочинної діяльності», що значно сприятиме практичній роботі слідчих та працівників кіберполіції в контексті встановлення комплексу взаємопов'язаних злочинів, учинених із використанням обстановки кіберпростору.

Список використаних джерел:

1. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: навчальний посібник. К., 2002. 240 с.

2. Грак А. Владения ПК и список программ для резюме. URL: https://www.im-konsalting.ru/blog/uroven-vladeniya-kompyuterom-dlya-rezyume/

3. Ковалев Д.И. Криминологическая характеристика личности преступника, совершившего преступление в сфере компьютерной информации. Вестник Академии. 2011. № 3. С. 90-94. URL: https://elibrary.ru/item.asp?id=16556890.

4. Стрюк М.І., Семеріков С.О., Стрюк А.М. Мобільність: системний підхід. Інформаційні технології і засоби навчання. 2015. Том 49. С. 37-70.

5. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. К., 2005. 1728 с.

6. Транснациональная организованная преступность: дефиниции и реальность: монография / отв. ред. В. А. Номоконов. Владивосток, 2001. 375 с.

7. Корж В.П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности: монография. Харьков, 2002. 412 с.

8. Вирок по справі № 683/444/17 від 21 березня 2017 року Старокостянтинівського районного суду Хмельницької області / Єдиний державний реєстр судових рішень (ЄДРСР). URL: http://reyestr.court.gov.ua/Review/65809534.

9. Вирок по справі № 607/16616/14-к від 19 лютого 2016 року Тернопільського міськрайонного суду Тернопільської області / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/55977478.

10. Вирок по справі № 592/4835/17 від 01 червня 2017 року Ковпаківського районного суду м. Суми / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/66841350.

11. Вирок по справі № 520/316/18 від 24.01.2018 року Київського районного суду м. Одеси / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/71757839.

12. Вирок по справі № 761/10994/14-к від 23 квітня 2014 року Шевченківського районного суду м. Києва / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/38502750.

13. Вирок по справі № 1-7|2010 від 05 жовтня 2010 року Білоцерківського міськрайонного суду Київської області / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/63156830

14. Черкасов В. Н. Дело «балаковских» хакеров. Факты и размышления. Информационная безопасность регионов. 2009. № 2(5); 2010. № 1(6); 2010. № 2; 2011. № 1(8). С. 158-163.

15. Вирок по справі № 161/1345/18 від року 1 березня 2018 року Луцького міськрайонного суду Волинської області / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72886703

В статье с позиций криминалистической науки осуществляется типизация лиц, которые совершают преступления с использованием обстановки киберпространства. Отдельное внимание уделено определению закономерных связей в системах «преступник – организованная группа», «типичные следы – преступник» и «преступник – специфика преступной деятельности». Сформулированные автором положения будут способствовать практической работе следователей и оперативних подразделений в контексте установления комплекса взаимоувязанных преступлений, совершенных с использованием обстановки киберпространства.

Ключевые слова: киберпространство, мобильность, обстановка, лицо преступника, типизация, специалист.

In the article, from the standpoint of criminalistic science, typing of a person who commits a crime using the environment of cyberspace is carried out. Special attention is paid to the identification of regular links in the systems «criminal-organized group», «criminal-typical traces of a criminal» and «criminal-specific criminal activity». The provisions formulated by the author will facilitate the practical work of investigators and operational units in the context of establishing a set of interrelated crimes committed using the cyberspace environment.

Key words: cyberspace, mobility, situation, face of criminal, typification, specialist.