безпечити охорону ЕОМ, у якій було виявлено сліди злочину, сервер, пункти вимкнення живлення, якщо техніка знаходиться у ввімкненому стані, тощо; забезпечити неможливість вчинення сторонніми особами будь-яких дій з комп'ютерною технікою, їх користування іншими технічними засобами, що можуть за допомогою бездротових технологій вносити зміни в інформацію (видаляти її).

Особлива увага під час проведення обшуку повинна звертатися на виявлення: записних книжок, мобільних телефонів, документів про надходження та одержання грошових переказів, інших цінностей, анкет для отримання закордонних паспортів; митних декларацій; трудових договорів; копій квитанцій на міжнародні поштові відправлення та переводи; установчих документів, що підтверджують право на заняття туристичною діяльністю, діяльністю з працевлаштування (в тому числі і за кордоном); проїзних квитків та ін.

Список використаних джерел:

1. Весельський В. К., Пясковский В. В. Торгівля людьми в Україні (Проблеми розслідування) : навчальний посібник. К. : КНТ, 2007. 268 с.
2. Діяльність прокурора з протидії злочинам, пов'язаним з торгівлею людьми та незаконною трансплантацією органів і тканин : навч. посіб. / І. М. Козьяков, О. М. Толочко, В. М. Куц, А. М. Орлеан, І. П. Ковтун та ін.; Нац. акад. прокуратури України. Кам'янець-Подільський : Буйницький О. А., 2014. 166 с.

Одержано 01.11.2017

УДК 343.3

Ксенія Володимирівна ЮРТАЄВА,
кандидат юридичних наук, старший викладач кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ НЕЗАКОННОМУ ВИКОРИСТАННЮ КОМП'ЮТЕРНИХ ПАРОЛІВ ТА КОДІВ ДОСТУПУ, ЯКІ НАДАЮТЬ ДОСТУП ДО КОМП'ЮТЕРНИХ СИСТЕМ АБО ЇХ ЧАСТИН

Останнім часом в Україні почастішали випадки незаконного використання комп'ютерних паролів, кодів доступу та подібних даних, які надають доступ до комп'ютерних систем або їх частин. Зазначені діяння вчиняються для отримання доступу до банківський рахунків, конфіденційної інформації, що зберігається в комп'ютері або в комп'ютерній системі, до

приватних акаунтів користувачів комп'ютерних мереж тощо. Іноді комп'ютерні шахраї займаються незаконним збором подібних даних з метою їх продажу й подальшого незаконного використання.

На теперішній час КК України не містить окремих норм щодо кримінальної відповідальності за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин [1]. Ратифікована Україною Конвенція Ради Європи про кіберзлочинність 2001 р. передбачає встановлення відповідальності за виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення злочинів, передбачених статтями 2-5 Конвенції [2]. Проте Україна реалізувала зазначену вимогу лише частково, зробивши відповідне застереження під час ратифікації вказаної угоди.

Провівши аналіз положень чинного КК України, приходимо до висновку, що притягнення до кримінальної відповідальності за продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, на теперішній час є практично неможливим. Так, наприклад, деякі фахівці пропонують кваліфікувати розповсюдження кодів доступу до комп'ютерної системи як пособництво у вчиненні інших комп'ютерних злочинів. У такому випадку слідчим має бути доведено усвідомлення особи хоча б у загальних рисах, що розповсюдження або продаж комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, є частиною конкретного комп'ютерного злочину та сприяє його вчиненню, що на практиці здійснити вкрай складно. Вбачається, що незаконне, без права на це розповсюдження конфіденційної інформації як-от комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, є самостійною, ізольованою діяльністю особи, яка зазвичай спрямована на невизначене та не персоніфіковане коло осіб. Умисел особи зазвичай обмежуються збутом (розповсюдженням) зазначених предметів з отримання матеріальної винагороди або без такої, тому подібну діяльність

вбачається недоцільним розглядати як співучасть у вчиненні інших комп'ютерних злочинів.

Окремо слід розглянути випадки, коли особа будь-яким чином без право на це умисно отримує комп'ютерний пароль, код доступу або подібні дані, які надають доступ до комп'ютерної системи або її частини, для подальшого їх використання для вчинення інших комп'ютерних злочинів самостійно, без залучення інших осіб. Прикладом цього можуть бути фішинг, вішинг, смішинг та інші види комп'ютерного шахрайства. Вбачається, що незаконне отримання комп'ютерних паролів, кодів доступу або подібних даних, за наявності необхідних підстав можливо кваліфікувати як готування до вчинення комп'ютерного злочину. Проте у деяких випадках притягнення до кримінальної відповідальності стає неможливим, наприклад, за готування до злочину, передбаченого ст. 163 КК України (порушення таємниці кореспонденції, що передається через комп'ютер), оскільки останній є злочином невеликої тяжкості, готування до яких не тягне за собою кримінальної відповідальності. Крім того умисел на вчинення подальших комп'ютерних злочинів не завжди можливо довести. Утім, слід зазначити, що фішинг-шахраї часто збирають та накопичують конфіденційну інформацію з метою передачі (збуту) іншим особам, що знову повертає нас до вже аналізованих проблем співучасті у вчиненні подібних злочинів.

Підсумовуючи, можна зробити висновок, що чинний КК України на теперішній час не передбачає ефективних можливостей притягнення до кримінальної відповідальності за дії, пов'язані з незаконним використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин. До Верховної Ради України було подано декілька законопроектів щодо встановлення відповідальність за вказане діяння, однак жодний з них не був прийнятий. Відповідальність за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних передбачена в ст. 285 КК Грузії, ст. 216 КК Естонської Республіки, ст. 260-4 КК Республіки Молдови, ст. 46 Антикорупційного закону Румунії, §1028A(6) Титулу 18 США. Враховуючи негативну динаміку розповсюдження суспільно небезпечних діянь, пов'язаних з протиправними діями з комп'ютерними паролями, кодами доступу або подібними даними, вбачається обґрунтованим передбачення кримінальної відповідальності за вказані діяння у Розділі XVI Особливої частини КК України

«Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Список використаних джерел:

1. Кримінальний кодекс України URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 01.10.2017).
2. Конвенція про кіберзлочинність 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575 (дата звернення: 01.10.2017).

Одержано 01.11.2017