DOI https://doi.org/10.30525/978-9934-26-229-6-63

CYBERFRAUD TODAY

КІБЕРШАХРАЙСТВА СЬОГОДЕННЯ

Lytvyn E. P.
Cadet
Lviv State University of Internal Affairs
Lviv, Ukraine

Литвин Е. П.
курсант
Львівського державного університету
внутрішніх справ
м. Львів, Україна

Priakhin Ye. V.
Candidate of Legal Sciences, Associate Professor, Associate Professor at the Department of Criminal Procedure and Criminalistics
Lviv State University of Internal Affairs
Lviv, Ukraine

Пряхін Є. В.
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та криміналістики
Львівського державного університету
внутрішніх справ
м. Львів, Україна

Сьогодні рідко почуєш фразу: «У мене у метро (маршрутці) вкрали гаманець (або телефон чи сумку)». І це не тому, що злочинців стало менше, а тому, що з технологічним прогресом розвивається і модифікується сам лиходій, який переходить в іншу сферу суспільного життя – кіберпростір. На початку 60-х років минулого століття, коли були зареєстровані перші злочини, вчинені з використанням електронно-обчислювальних машин, в американській пресі з'явилося поняття «комп'ютерна злочинність». Цей термін використовували в засобах масової інформації, вчені, працівники правоохоронних органів, незважаючи на те, що для цього не було ні криміналістичних, ні правових підстав. Визначення поняття «комп'ютерний злочин» вперше було надане у 1983 році в Парижі (Франція) групою експертів Організації економічної співробітництва та розвитку ООН: комп'ютерний злочин – це будь-яке незаконне, неетичне чи не дозволене діяння, що стосується автоматизованої обробки даних чи передачі даних [1].

Чинником, який найбільше впливає на кібершахрайство в Україні, є Інтернет, що зараз виступає основним знаряддям комп'ютерного шахрайства. Інтернет-асоціацією України спільно з холдингом Factum Group Ukraine проведено дослідження репрезентативного населення України віком від 15 р. і старше. За результатами проведених досліджень установлено, що динаміка проникнення Інтернету має показники, за якими 65% населення (21,35 млн) є регулярними користувачами мережі Інтернет, у 67% населення (21,9 млн) підключено домашній Інтернет.

Чинником, який також впливає на злочинність даної категорії, є мобільність доступу до мережі. Так, 57% інтернет-користувачів використовують для доступу мобільний телефон або смартфон; 45% – домашній переносний персональний комп'ютер; 39% – стаціонарний персональний комп'ютер; 15% – планшетний персональний комп'ютер; 10% – робочий комп'ютер. І всі ці показники мають тенденцію до зростання. На думку А. Ф. Зелінського, «порівняно низький коефіцієнт злочинності в Україні – це результат насамперед винятково високої латентності (прихованості) злочинів і погано поставленого обліку». Отож, поглиблене дослідження шахрайств, вчинених із використанням комп'ютерних мереж, неможливе без аналізу такого додаткового показника, як латентність злочинності [2].

Кібершахрайство являє собою незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей. Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної (в т.ч. фейкової) інформації через мережу Інтернет. Кіберзлочинністю прийнято вважати кримінально карані дії, що передбачають несанкціоноване проникнення в роботу комп'ютерних мереж, комп'ютерних систем та програм, з метою видозміни комп'ютерних даних. При цьому комп'ютер виступає в якості предмета злочину, а інформаційна безпека – в якості об'єкта. До подій, пов'язаних зі цим видом кримінальних правопорушень можна віднести ситуації, при яких комп'ютер – знаряддя для вчинення кримінальних правопорушень, з метою порушення авторських прав, громадської безпеки, прав власності, моральності. Класифікувати наразі кібершахрайство можливо так:

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема: незаконний доступ, наприклад, шляхом злому, обману та іншими засобами; нелегальне перехоплення комп'ютерних даних; втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру; зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

У той же час, з урахуванням мотивації злочинців, кібер-правопорушення представляється можливим умовно розділити на наступні категорії: 1) кібершахрайство з метою заволодіння коштами чи інформацією (для власного користування або для подальшого продажу); 2) втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам); інші злочини [3].

Для прикладу, у Дніпропетровській області правоохоронці викрили місцеву жительку, яка незаконно оформляла онлайн-кредити на громадян. За попередніми даними, фігурантка ошукала близько 40 осіб більш ніж на 300 тис. грн. Зокрема, через підбір пароля зловмисниця отримала доступ до електронної скриньки однієї з потерпілих, де зберігалися копії документів та особисті фото. З використанням цих даних правопорушниця отримала доступ до онлайн-банкінгу та увійшла до мобільного застосунку «Дія». Правоохоронці наголосили, що розкриття цієї схеми підтвердило неможливість отримання онлайн-кредиту з використанням цифрових документів у «Дії» [4].

У науковій літературі виокремлюють основні складники, які можуть впливати на зниження рівня кіберзлочинності, а саме:

– правові та законодавчі складники. На боці протидії кіберзлочинності перебуває державна система у вигляді законодавчої і виконавчої гілок влади, зі своїми нормами права (спрямованими на протидію злочинам і сприяння боротьбі з кіберзлочинами). Чинником стримування злочинності є зміни в правових нормах або в процесах реформування державних органів (зокрема, утворення 2015 р. підрозділу кіберполіції Національної поліції України, створення спеціальних відділів протидії кіберзлочинності в структурі Служби безпеки України);

– приватний сектор і банківська система, які також надають підтримку в боротьбі з кібершахрайством у межах своїх прав. Контролювання фінансових потоків відіграє не останню роль, особливо щодо шахрайств, скоєних із використанням систем віддаленого банківського обслуговування;

– профілактика і досвід. Основним чинником, який виключає можливість комп'ютерних шахраїв довгий час використовувати ті самі

способи вчинення кримінальних правопорушень, є профілактика, набутий підрозділами Національної поліції (іншими органами правоохоронної спрямованості) досвід, проведення бесід, оприлюднення проблеми в засобах масової інформації тощо. Так само важливу роль відіграють процесуальні та правові прецеденти, які використовуються під час розслідування і документування кримінальних правопорушень органами досудового розслідування Національної поліції України, прокуратури й оперативними підрозділами з боротьби з кіберзлочинністю.

На жаль, шахрайство існувало і існує в умовах війни, бо схеми злодіїв отримали нові втілення. Тяжкі часи завжди провокують не лише спалах патріотизму, самовідданості та братерського єднання. Серед нас також живуть і ті, хто намагається заробити на горі інших. Як зазначається на веб-сайті Укрінформ, «з початку військового вторгнення рф в Україну кіберполіцейські викрили 106 осіб на вчиненні шахрайства в Інтернеті». Серед найрозповсюдженіших схем шахрайства в умовах воєнного стану є псевдоблагодійність, пропозиції оренди неіснуючого житла, фейкові пасажирські перевезення та продаж неіснуючих товарів, зокрема й військової амуніції. Правоохоронці також фіксують випадки шахрайства під виглядом організації переправлення через державний кордон чоловіків призовного віку або надання інформації щодо безвісти зниклих громадян. Кіберполіція закликає громадян перераховувати гроші тільки на рахунки офіційних благодійних фондів, рахунки, вказані на сайті НБУ, або через додаток «Дія». Варто надавати перевагу післяплаті за товари та послуги. Також правоохоронці застерігають від замовлення документів, що нібито дозволять перетнути кордон чоловікам у віці 18–60 років, оскільки окрім ризику потрапити на гачок шахраїв, замовникам підробних документів загрожує кримінальна відповідальність [4].

Як бачимо, кіберзлочинність і її особливості досить сильно відрізняються від злочинності загальнокримінальної спрямованості. Зростання кількості шахрайств із використання комп'ютерних мереж залежить від збільшення ступеня проникнення високих інформаційно-програмних технологій у повсякденне життя населення України. Соціальні мережі та Інтернет є потенційною загрозою для багатьох користувачів, які наражають свої персональні дані на небезпеку. Незнання, як захистити себе та свої персональні дані – є дуже важливим викликом сучасності для людини XXI століття.

Література:

1. Неділько Я. Поняття кіберзлочинів та їх види. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf

2. Лефтеров Л. В. Кримінологічний аналіз шахрайств, учинених із використанням комп'ютерних мереж. URL: http://pap-journal.in.ua/wp-content/uploads/2020/08/5_2018.pdf#page=318

3. Пфо О. М. Основні поняття і класифікація кіберзлочинності. URL: https://core.ac.uk/download/pdf/84825482.pdf

4. Мультимедійна прлатформа іномовлення України «Укрінформ». URL: https://www.ukrinform.ua

DOI https://doi.org/10.30525/978-9934-26-229-6-64

DETENTION OF A MINOR SUSPECT UNDER MARTIAL LAW

ЗАТРИМАННЯ НЕПОВНОЛІТНЬОГО ПІДОЗРЮВАНОГО В УМОВАХ ВОЄННОГО СТАНУ

Lytvynenko O. G.
Doctor of Philosophy in specialty 081 «Law», Senior Lecturer at the Department of Organization of Pretrial Investigation, Faculty No. 1 of the Kryvyi Rih Educational and Scientific Institute of the Donetsk State University of Internal Affairs

Литвиненко О. Г.
доктор філософії за спеціальністю 081 «Право», старший викладач кафедри організації досудового розслідування факультету № 1 Криворізького навчально-наукового інституту Донецького державного університету внутрішніх справ

Aksonov K. V.
Lecturer at the Department of Organization of Pretrial Investigation, Faculty No. 1 of the Kryvyi Rih Educational and Scientific Institute of the Donetsk State University of Internal Affairs Kryvyi Rih, Ukraine

Аксьонов К. В.
викладач кафедри організації досудового розслідування факультету № 1 Криворізького навчально-наукового інституту Донецького державного університету внутрішніх справ м. Кривий Ріг, Україна

Початок війни Росії з Україною змінив не лише звичайний уклад громадян нашої держави, а й законодавчу сферу, в тому числі й кримінальний процес, задля адаптації до його правозастосування в умовах війни. Зокрема такі зміни торкнулись кримінальне процесуальне законодавство в частині затримання.