Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ

С.В. Бабанін

ЗАПОБІГАННЯ КОМП'ЮТЕРНИМ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

Науково-практичний посібник

Дніпро
2022

УДК 343.85
Б 12

Рекомендовано науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 3 від 19.11.2021)

Автор: ***Бабанін С. В.*** – кандидат юридичних наук, доцент, доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ.

РЕЦЕНЗЕНТИ

Школа С. М. – завідувач кафедри публічного права Інституту соціальних і гуманітарних наук Національного технічного університету «Дніпровська політехніка», кандидат юридичних наук, доцент.

Бублейник В. А. – адвокат (Рада адвокатів Дніпропетровської області), кандидат юридичних наук.

Б 12 Запобігання комп'ютерним кримінальним правопорушенням : наук.-практ. посібник / С. В. Бабанін. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 80 с.

ISBN 978-617-8032-57-9

У науково-практичному посібнику розглянуто питання запобігання кримінальним правопорушенням, передбаченим розділом XVI Особливої частини КК України, та деяким іншим, що містять як обов'язкові об'єктивні ознаки складу кримінального правопорушення окремі елементи сфери використання комп'ютерів, систем та комп'ютерних мереж, які, згідно Конвенції Ради Європи» Про кіберзлочинність», визнаються кіберзлочинами.

Науково-практичний посібник розроблено на основі аналізу вітчизняного законодавства, наукової та публіцистичної літератури з урахуванням власних думок і практичних пропозицій автора.

Видання розраховане на науковців, викладачів, аспірантів (ад'юнктів), студентів (курсантів) ЗВО, у яких готують правників, працівників правоохоронних органів, прокуратури та суду, а також на всіх, хто цікавиться питаннями запобігання комп'ютерним кримінальним правопорушенням.

ISBN 978-617-8032-57-9

ЗМІСТ

Вступ

Конституція України у ч. 1 ст. 17 проголошує, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Положення Конституції закріплюються у законах та підзаконних нормативно-правових актах. Так, Закон України «Про основи національної безпеки» у ст. 1 відносить інформаційну безпеку до складових частин національної безпеки, а в ст. 3 інформаційне середовище суспільства – до об'єктів національної безпеки. Україною ратифіковано Конвенцію про кіберзлочинність (Закон України від 07.09.2005 р.), що визначає перелік комп'ютерних кримінальних правопорушень.

Розвиток та впровадження комп'ютерних технологій у всіх сферах діяльності людини потребує вирішення питань забезпечення безпеки використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також і кримінально-правовими засобами. У багатьох країнах, у тому числі в Україні, ці посягання одержали умовну назву «комп'ютерні кримінальні правопорушення (злочини)».

КК України передбачає відповідальність за них у декількох розділах.

Розділ XVI Особливої частини КК «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить шість з цих норм: ст.ст. 361, 361^1, 361^2, 362, 363, 363^1.

Окрім того, у інших розділах КК України є норми, що містять як обов'язкові об'єктивні ознаки складів кримінальних правопорушень окремі елементи сфери використання комп'ютерів, систем та комп'ютерних мереж. До цих норм слід віднести: ст. ст. 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер», 176 «Порушення авторського права та суміжних прав», ч. 3 ст. 190, а саме шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки, ст.ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення», 216 «Незаконне виготовлення, підроблення, використання або збут незаконно виготовлених, одержаних чи підроблених марок акцизного збору чи контрольних марок», ч.ч. 2, 3 ст.

301 «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів».

Також комп'ютерна техніка може виступати знаряддям інших кримінальних правопорушень, наприклад, фальсифікації виборчих документів, документів референдуму чи фальсифікації підсумків голосування, надання неправдивих відомостей до органів Державного реєстру виборців чи фальсифікації відомостей Державного реєстру виборців (ст. 158 КК), незаконного заволодіння транспортним засобом (ст. 289 КК), підроблення документів, печаток, штампів та бланків (ст. 358 КК) тощо. При притягненні до відповідальності за ці кримінальні правопорушення використання комп'ютерної техніки потребує додаткової кваліфікації лише у випадку, якщо такі діяння становлять окремий склад кримінального правопорушення, вказаний вище. У світі спостерігається стрімке зростання суспільної небезпечності кримінальних правопорушень, пов'язаних із застосуванням засобів комп'ютерної техніки.

На думку американських експертів, збитки від одного кіберзлочину у середньому складають від 450 тис. до 1 млрд. дол. США., тоді як одне фізичне пограбування банку у середньому обходиться у 3,2 тис. дол. На сьогоднішній день кіберзлочинність спричиняє більші збитки, ніж торгівля наркотичними засобами. Як було зазначено на конференції Information Week 500, прибуток від злочинної діяльності у сфері використання засобів комп'ютерної техніки складає 105 млрд. дол. США на рік, і цей показник весь час зростає. Зараз світова статистика вказує на те, що кіберзлочин вчиняється у середньому кожні дванадцять секунд[1].

Визначальною характеристикою комп'ютерних кримінальних правопорушень є й високий ступінь їхньої латентності, що за різними даними становить від 80 до 98%. За даними національного відділення ФБР з комп'ютерних злочинів від 85% до 97% комп'ютерних посягань навіть не виявляються. За оцінками інших експертів латентність кіберзлочинів у США сягає 80%, у Великобританії – 85%, у Німеччині – 75%, в Україні – 90%. У країнах Європи та США, де накопичено достатньо велику та достовірну статистику з комп'ютерних злочинів, до суду передаються не більше 1% правопорушень цього виду[2].

Вивчені матеріали судової та слідчої практики дозволяють

[1] Кобилянська Л.М. Кіберзлочинність як глобальна загроза економічній безпеці сучасної держави. *Науковий вісник Херсонського державного університету. Серія «Економічні науки»*. Випуск 8. Частина 5. 2014. С. 14-17.

[2] Ларкін М.О. Особливості розслідування комп'ютерних злочинів: навчально-методичний посібник для студентів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки «Правознавство». Запоріжжя: ЗНУ, 2014. 84 с. С. 57-58.

констатувати, що переважна більшість кіберзлочинів вчиняються з корисливих мотивів (82%), серед інших спонукань можна виділити хуліганські, інтерес, помсту, самоствердження. Ці правопорушення учетверо частіше вчиняються чоловіками. Проте за даними американських соціологів жінки складають третину від загального числа заарештованих хакерів. Вікові характеристики комп'ютерних злочинців виглядають таким чином. До 2002 р. переважна більшість виявлених осіб, що скоїли злочини у сфері комп'ютерних технологій, відносилися до вікової категорії від 25 до 35 років. Починаючи з 2003 р. і до цього часу велика частина зловмисників – це молоді люди у віці від 18 до 25 років.

А. Осипенко зазначає, що серед комп'ютерних злочинців 20% складають особи 14-18 років, 57% – 19-25 років, 15% – 26-35 років, 8% – 36-55 років. Отже, існує тенденція до омолоджування комп'ютерних злочинців, яка синхронізується із загальним омолоджуванням злочинності, і може призвести до того, що незабаром доля та суспільна небезпека хакерів, які не досягли 16-річного віку, посилюватиметься у процесі зростання комп'ютеризації суспільства, хоча основна їх частина становитиме осіб вікової групи 25-30 років[3].

Якщо говорити щодо перспектив розвитку інформаційно-комунікаційних технологій (ІКТ) в Україні і, відповідно, про підвищення ефективності запобігання комп'ютерним кримінальним правопорушенням, то у світовому рейтингу країн із прийняття та розвитку ІКТ Україна посідає 79-е місце, поступаючись Грузії (78-е місце) і Боснії та Герцеговині (77-е місце)[4].

До заходів запобігання комп'ютерним кримінальним правопорушенням відносяться, зокрема, кримінально-правові та пов'язані з ними інші заходи, спрямовані на виявлення та належне документування цього виду правопорушень.

Окремі з вказаних заходів розглянуті у цьому посібнику.

---

[3] Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: Монография. Омск, 2009. 480 с. С. 109-110.

[4] Індекс розвитку інформаційно-комунікаційних технологій. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D0%B4%D0%B5%D0%BA%D1%81_%D1%80%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BA%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D0%B9

Розділ 1
КРИМІНАЛЬНО-ПРАВОВІ ЗАХОДИ ЗАПОБІГАННЯ КОМП'ЮТЕРНИМ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

1.1. Порівняльна характеристика розділу II Конвенції про кіберзлочинність та Кримінального кодексу України

1 липня 2006 р. для України набула чинності Конвенція про кіберзлочинність від 23 листопада 2001 р., ратифікована Верховною Радою 07 вересня 2005 р.

Учасниками Конвенції є 35 європейських держав – членів Ради Європи (Албанія, Австрія, Вірменія, Азербайджан, Бельгія, Боснія і Герцеговина, Болгарія, Хорватія, Кіпр, Чеська Республіка, Данія, Естонія, Фінляндія, Франція, Грузія, Німеччина, Угорщина, Ісландія, Італія, Латвія, Литва, Мальта, Молдова, Чорногорія, Нідерланди, Норвегія, Португалія, Румунія, Сербія, Словаччина, Словенія, Іспанія, Швейцарія, Македонія, Великобританія та Україна) та 5 держав, які не є членами Ради Європи (Австралія, Домініканська Республіка, Японія, Панама, США).

Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами та даними, шляхом установлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [5].

Порівняльна характеристика розділу II Конвенції про кіберзлочинність та КК України надає можливості наочно побачити відповідність національного законодавства України положенням міжнародного нормативно-правового акту.

[5] 1 липня – восьма річниця набуття чинності для України Конвенції про кіберзлочинність. URL: https://minjust.gov.ua/news/ministry/1-lipnya---vosma-richnitsya-nabuttya-chinnosti-dlya-ukraini-konventsii-pro-kiberzlochinnist-20026.

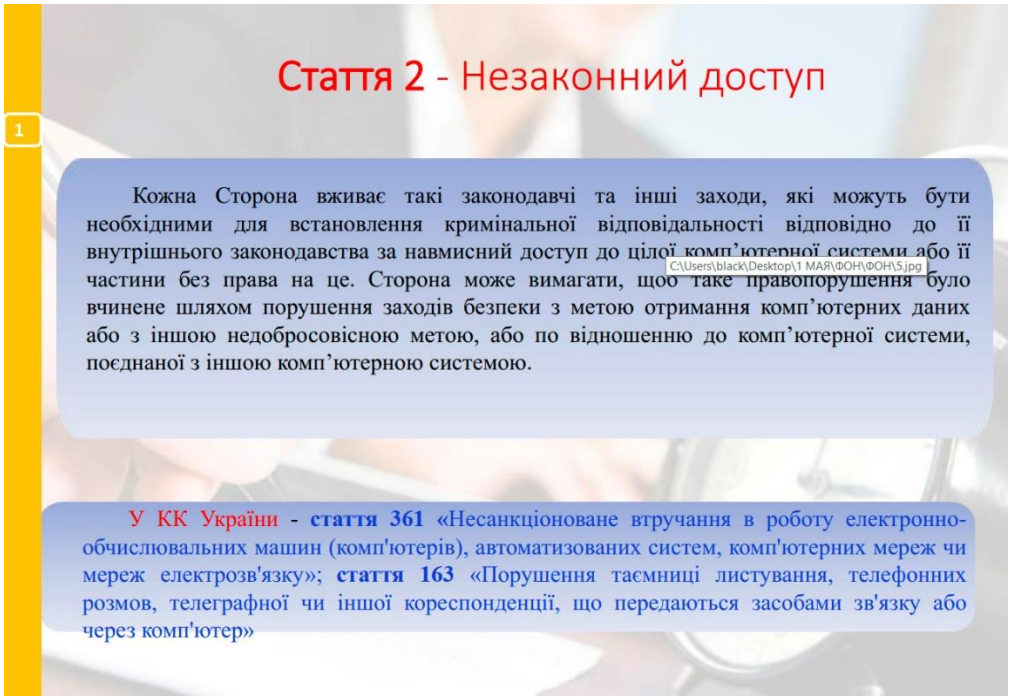


Рис. 1.1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Незаконний доступ (ст. 2)

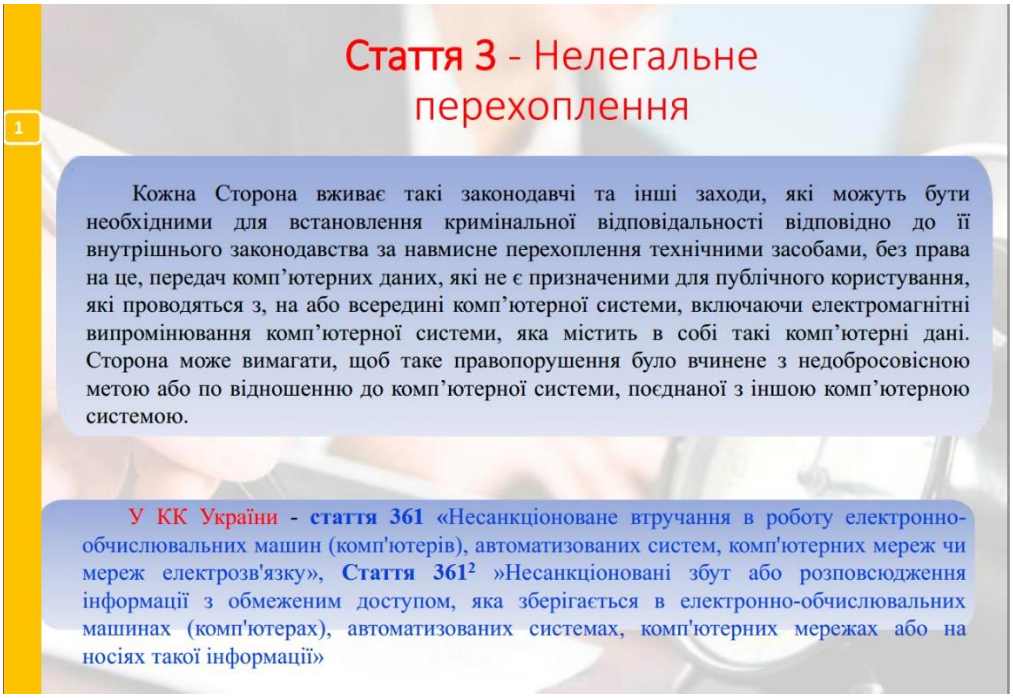


Рис. 1.2. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Нелегальне перехоплення (ст. 3)

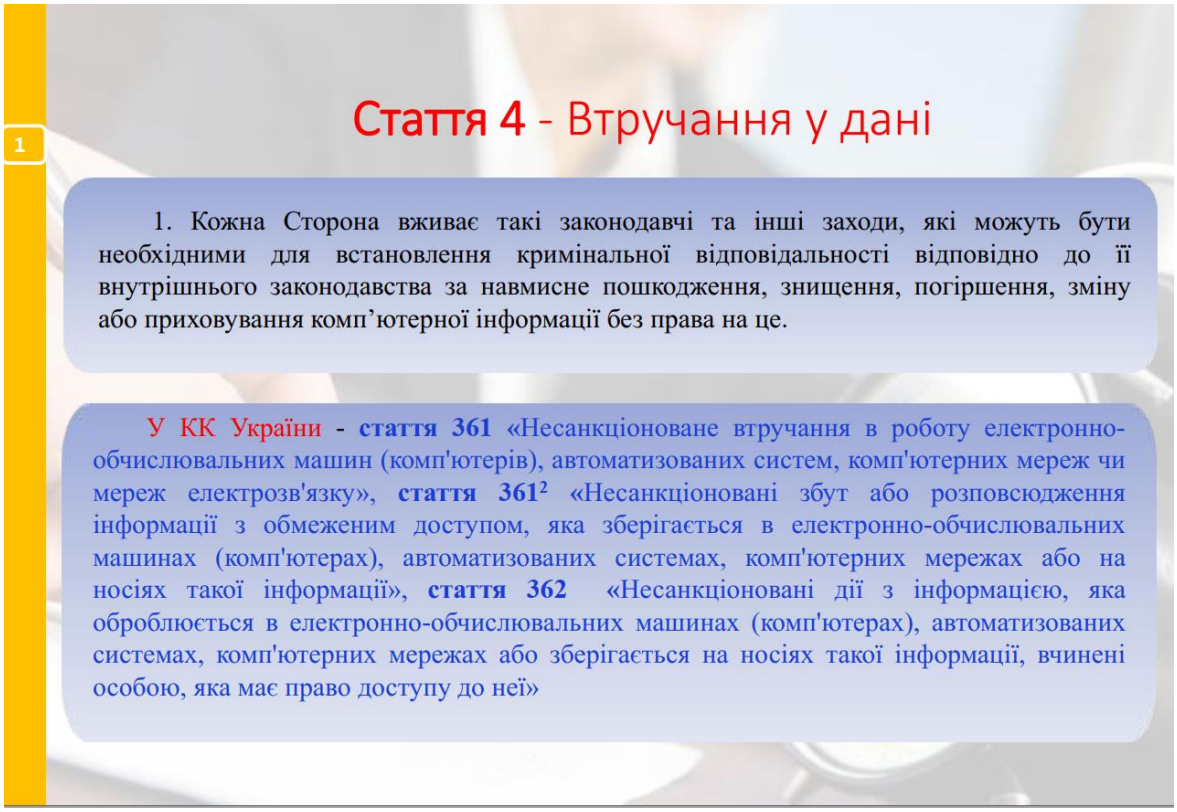


Рис. 1.3. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Втручання у дані (ст. 4)

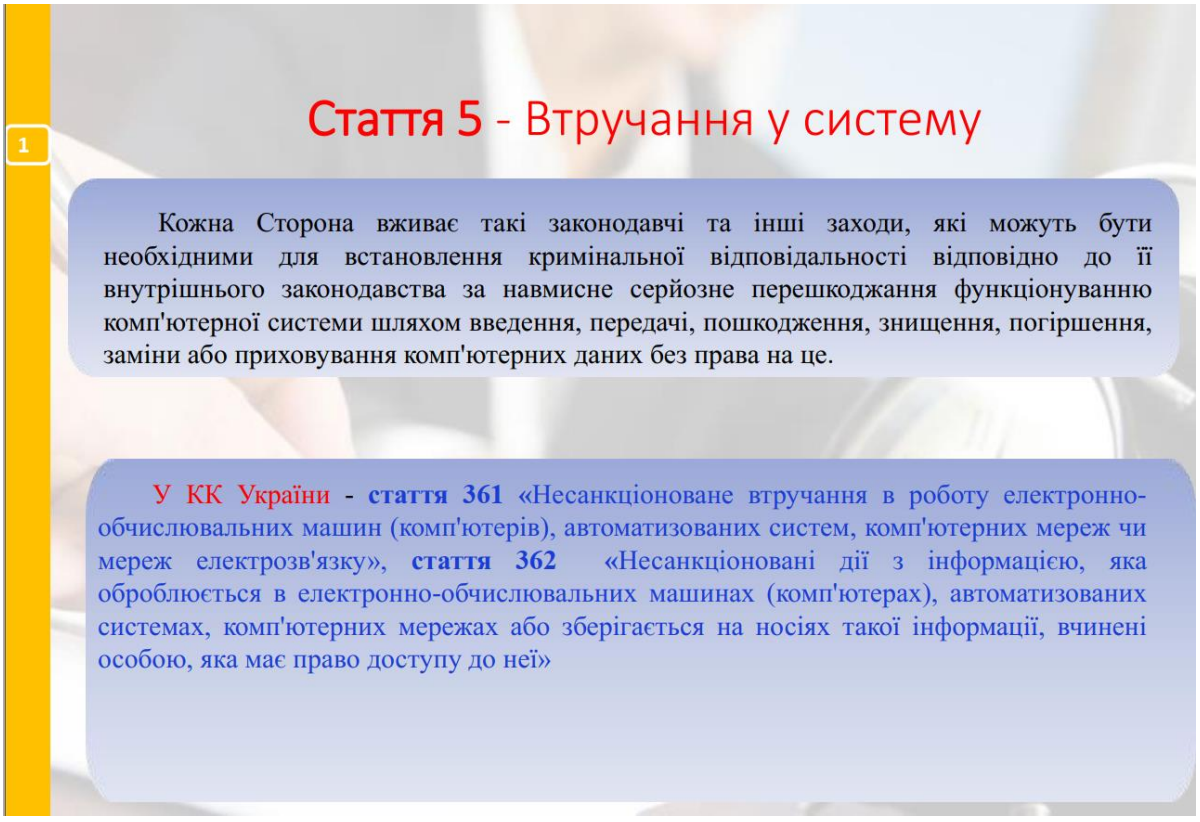


Рис. 1.4. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Втручання у систему (ст. 5)

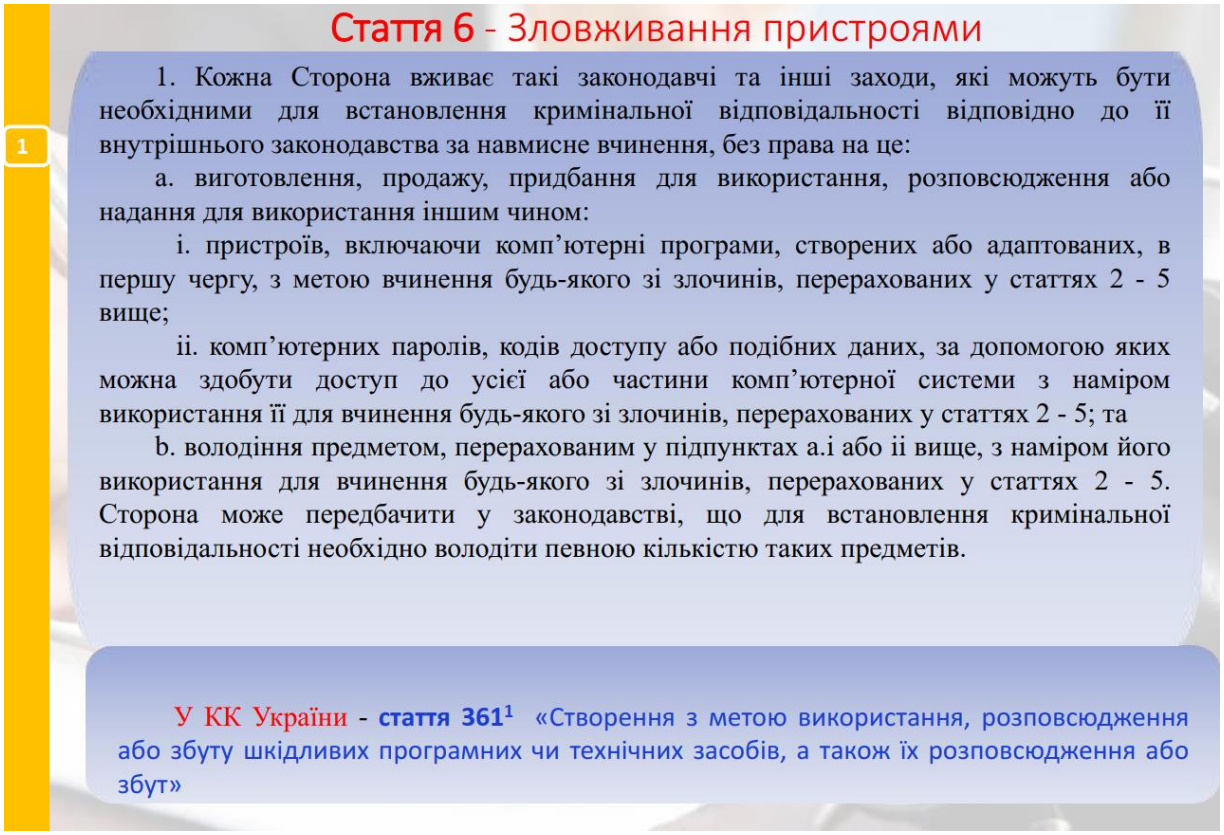


Рис. 1.5. Правопорушення, пов'язані з комп'ютером. Зловживання пристроями (ст. 6)

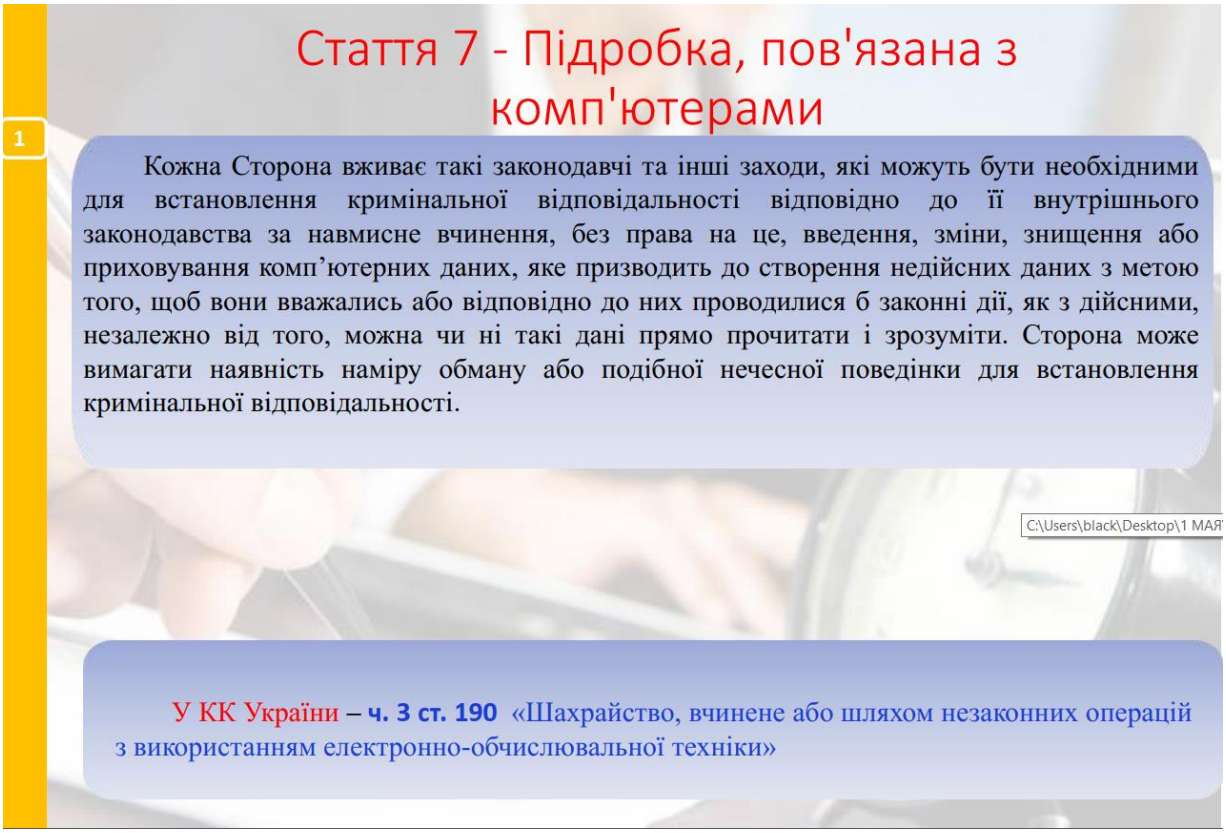


Рис. 1.6. Правопорушення, пов'язані з комп'ютером. Підробка, пов'язана з комп'ютерами (ст. 7)

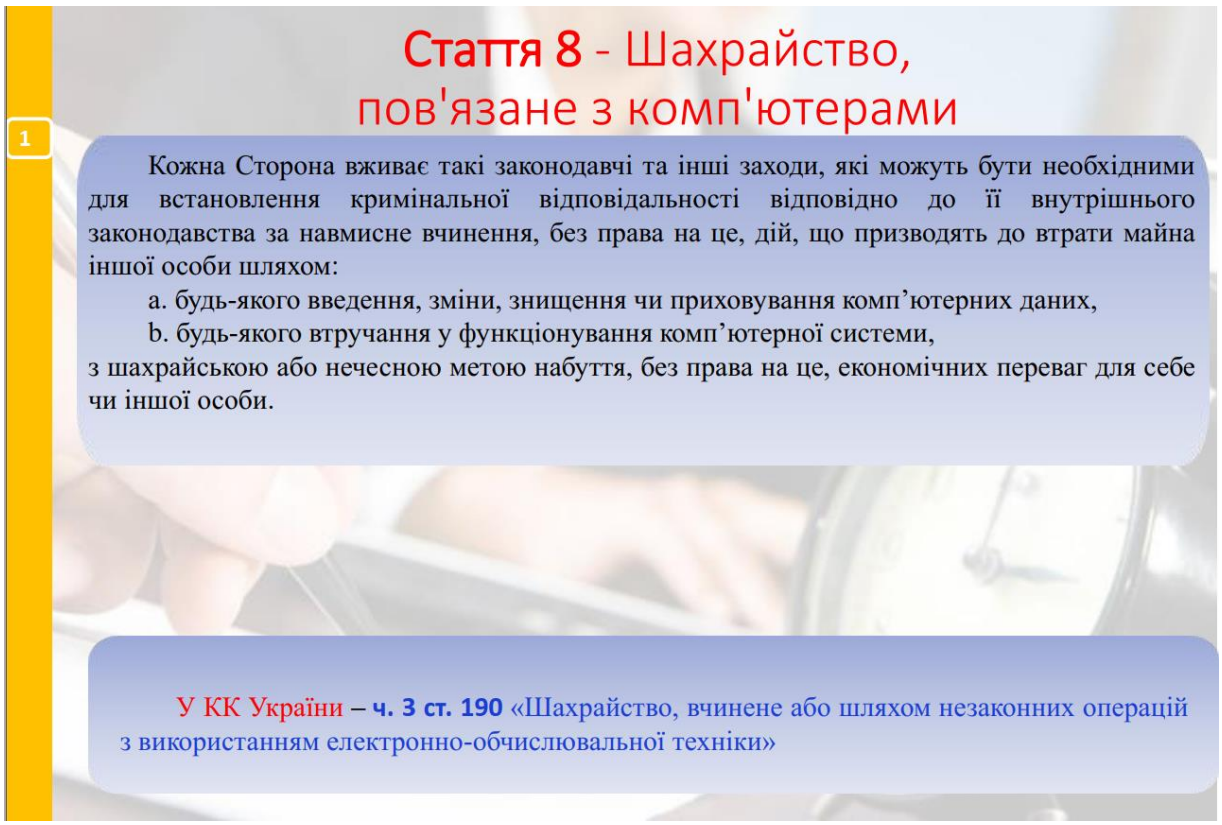


Рис. 1.7. Правопорушення, пов'язані з комп'ютером.
Шахрайство, пов'язане з комп'ютерами (ст. 8)

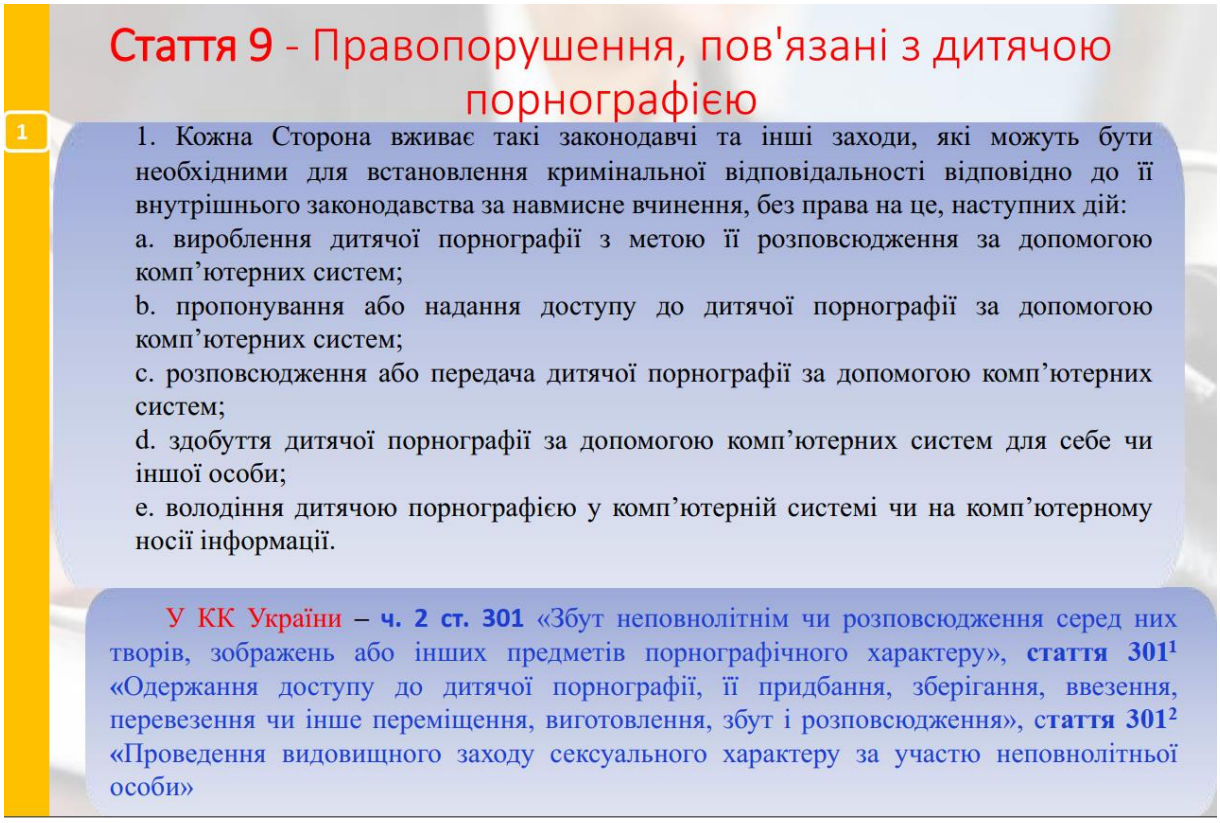


Рис. 1.8. Правопорушення, пов'язані зі змістом.
Правопорушення, пов'язані з дитячою порнографією (ст. 9)

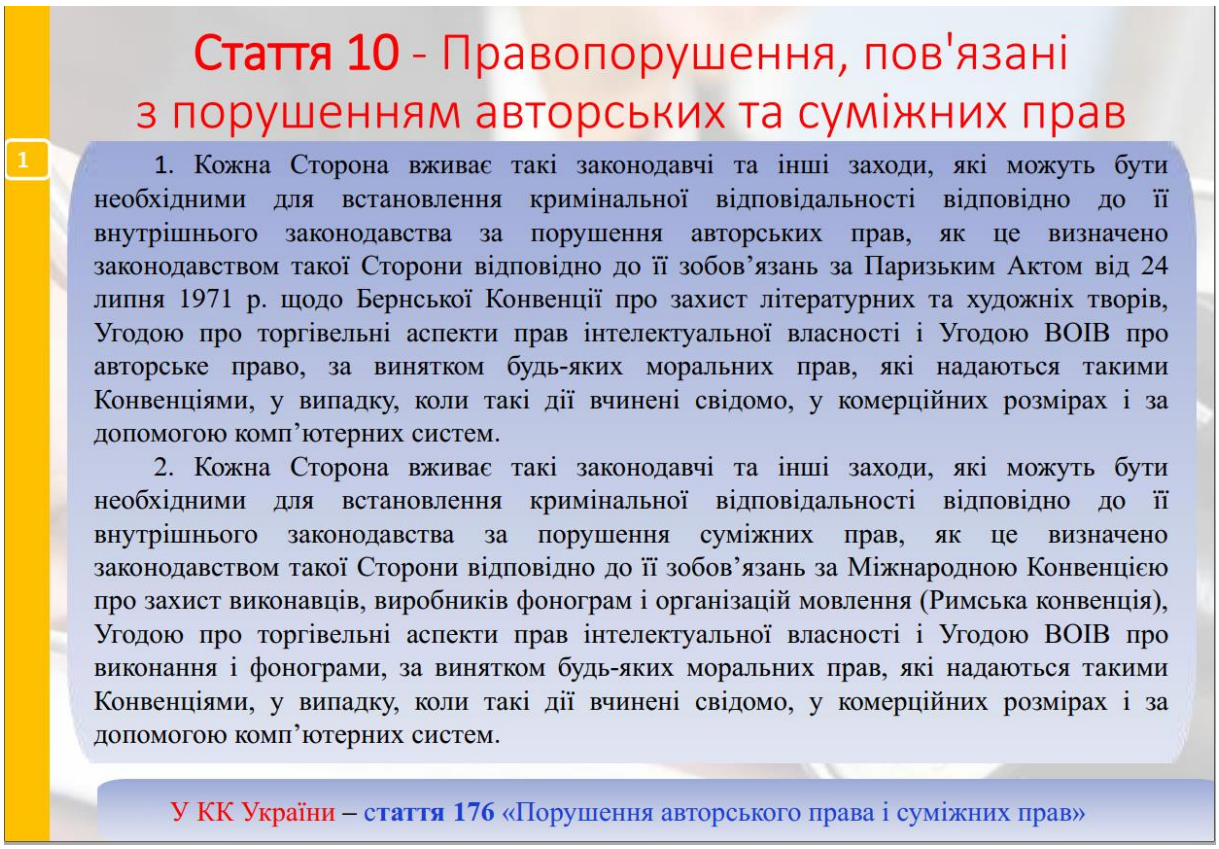


Рис. 1.9. Правопорушення, пов’язані з порушенням авторських та суміжних прав (ст. 10)

1.2. Склади комп’ютерних кримінальних правопорушень (схематичне зображення та зразки обвинувальних вироків судів)

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч.1 ст. 361, ч.1 ст. 361-1, ч.1 ст. 361-2 КК України (Шевченківський районний суд м. Львова, справа № 466/9246/20)

Рис. 1.10. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку (ст. 361)

ОСОБА_1, у період часу з 2019 по 2020 рік, у невстановлений досудовим слідством час, перебуваючи за місцем свого проживання за АДРЕСОЮ_2, з використанням електронно-обчислювальної машини (ЕОМ) – комп`ютер із хард-диском S/N S20BJ9DZ119213, IP-адреса: НОМЕР_1, діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, попередньо отримав на закритому

форумі «Даркнет», а саме: «BHF.IO» програмне забезпечення під назвою: «SQLi Dumper v.9.7 [Cracked By PC-RET].exe», що, згідно з базами даних «VIRUSTOTAL» – є шкідливим програмним забезпеченням, та призначене для несанкціонованого втручання в роботу комп`ютерних мереж та електронно-обчислювальних машин, та у разі його запуску, надає можливість через вразливість сайтів мережі Інтернет формувати базу даних про користувачів мережі Інтернет, а також отримувати доступ до їх логінів та паролів.

Далі обвинувачений вніс відповідні дані із адресами інтернет-сайтів до вказаної шкідливої програми, таким чином створивши з метою використання шкідливий програмний засіб, призначений для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп`ютерів) та автоматизованих систем.

Окрім цього, обвинувачений ОСОБА_1, в період часу з 2019 по 2020 рік, у невстановлений досудовим слідством час, перебуваючи за місцем свого проживання за АДРЕСОЮ_2, використовуючи електронно-обчислювальну машину (ЕОМ) – комп’ютер із хард-диском S/N S20BJ9DZ119213, IP-адреса: НОМЕР_1, діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, шляхом підбору авторизаційних даних, а саме логіну та паролю, за допомогою програмного забезпечення під назвою: «ІНФОРМАЦІЯ_2», яке згідно баз даних «VIRUSTOTAL», є шкідливим програмним забезпеченням, отримав доступ до облікових записів: «ІНФОРМАЦІЯ_3», «ІНФОРМАЦІЯ_4», «ІНФОРМАЦІЯ_5», «ІНФОРМАЦІЯ_6», «ІНФОРМАЦІЯ_7», «ІНФОРМАЦІЯ_8», «ІНФОРМАЦІЯ_9», «ІНФОРМАЦІЯ_10», «ІНФОРМАЦІЯ_11», «ІНФОРМАЦІЯ_12», «ІНФОРМАЦІЯ_13», «ІНФОРМАЦІЯ_14», «ІНФОРМАЦІЯ_15», «ІНФОРМАЦІЯ_16», «ІНФОРМАЦІЯ_17», «ІНФОРМАЦІЯ_18», «ІНФОРМАЦІЯ_22», «ІНФОРМАЦІЯ_23», «ІНФОРМАЦІЯ_19», «ІНФОРМАЦІЯ_20», що є інформацією з обмеженим доступом, що створені та захищені відповідно до вимог Цивільного кодексу України, Законів України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», здійснив несанкціоноване втручання в роботу облікових записів комп`ютерної мережі сервісу»Gmail.com», що призвело до витоку інформації.

Окрім цього, обвинувачений ОСОБА_1, в період часу з 2019 по 2020 рік, у невстановлений досудовим слідством час, перебуваючи за місцем свого проживання за АДРЕСОЮ_2, використовуючи електронно-обчислювальну машину (ЕОМ) – комп’ютер із хард-диском S/N

S20BJ9DZ119213, якій було надано IP-адресу: НОМЕР_1, діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, збув базу даних під назвою «ІНФОРМАЦІЯ_21» шляхом відправлення в середовище закритого форуму «Даркнет», а саме: «BHF.IO», на обліковий запис покупця, логінів та паролів користувачів мережі Інтернет, що надають доступ до акаунтів електронної пошти сервісу «Gmail.com», що є інформацією з обмеженим доступом, яку попередньо незаконно отримав за допомогою шкідливого програмного засобу.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч.ч.1,2 ст.361-1 КК України (Бориславський міський суд Львівської області, справа № 438/1630/20)

Рис. 1.11. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1)

ОСОБА_1 обвинувачується в тому, що 27 червня 2020 року о 10 годині 23 хвилини, перебуваючи за місцем праці за адресою: АДРЕСА_2, діючи умисно, усвідомлюючи протиправність своїх дій, використовуючи

свій персональний комп`ютер (системний блок торгової марки «Dell OptiPlex 990» із влаштованим SSD накопичувачем «Intel 240Gb S/N: PHWA630605P4240AGN») здійснив розповсюдження програмного забезпечення «crack win 7.rar», яке, відповідно до висновку комп`ютерно-технічної експертизи є шкідливим програмним забезпеченням (засобом), надіславши його за допомогою месенджера Viber користувачу з номером мобільного телефону НОМЕР_1, яким користується ОСОБА_2 .

Таким чином, ОСОБА_1 обвинувачується у розповсюдженні шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп`ютерів) автоматизованих систем, комп`ютерних мереж чи мереж електрозв`язку, тобто кримінальному правопорушенні, передбаченому ч.І ст.361 – 1 КК України.

Окрім цього, ОСОБА_1 обвинувачується в тому, що 11 липня 2020 року о 14 годині 34 хвилин, перебуваючи за місцем праці за адресою: АДРЕСА_2, діючи умисно, усвідомлюючи протиправність своїх дій, використовуючи свій персональний комп`ютер (системний блок торгової марки «Dell OptiPlex 990» із влаштованим SSD накопичувачем «Intel 240Gb S/N: PHWA630605P4240AGN») здійснив розповсюдження програмного забезпечення «KMS Auto-Net-1.5.4.zip», яке, відповідно до висновку комп`ютерно-технічної експертизи є шкідливим програмним забезпеченням (засобом), надіславши його за допомогою месенджера Viber користувачу з номером мобільного телефону НОМЕР_1, що ним користується ОСОБА_2.

Таким чином, ОСОБА_1, обвинувачується у розповсюдженні шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп`ютерів) автоматизованих систем, комп`ютерних мереж чи мереж електрозв`язку, вчиненому повторно, тобто кримінальному правопорушенні, передбаченому ч.2 ст.361 -1 КК України.

Окрім цього, ОСОБА_1 обвинувачується в тому, що 24 липня 2020 року о 15 годині 14 хвилин, перебуваючи за місцем свого проживання за адресою: АДРЕСА_1, діючи умисно, усвідомлюючи протиправність своїх дій, використовуючи свій персональний мобільний телефон (торгової марки «Redmi Note 5» IMEH НОМЕР_2 IMEI2 НОМЕР_3) здійснив розповсюдження програмного забезпечення «KMSAuto-Net-1.5.4.zip», яке, відповідно до висновку комп`ютерно-технічної експертизи є шкідливим програмним забезпеченням (засобом), надіславши його за допомогою месенджера Viber користувачу з номером мобільного телефону НОМЕР_1, яким користується ОСОБА_2.

Таким чином, ОСОБА_1, обвинувачується у розповсюдженні

шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп`ютерів) автоматизованих систем, комп`ютерних мереж чи мереж електрозв`язку, вчиненому повторно, тобто кримінальному правопорушенні, передбаченому ч.2 ст.361 – 1 КК України.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 1 ст. 361-2, ч. 2 ст. 361-2 КК України (Рівненський міський суд Рівненської області, справа № 569/8020/17)

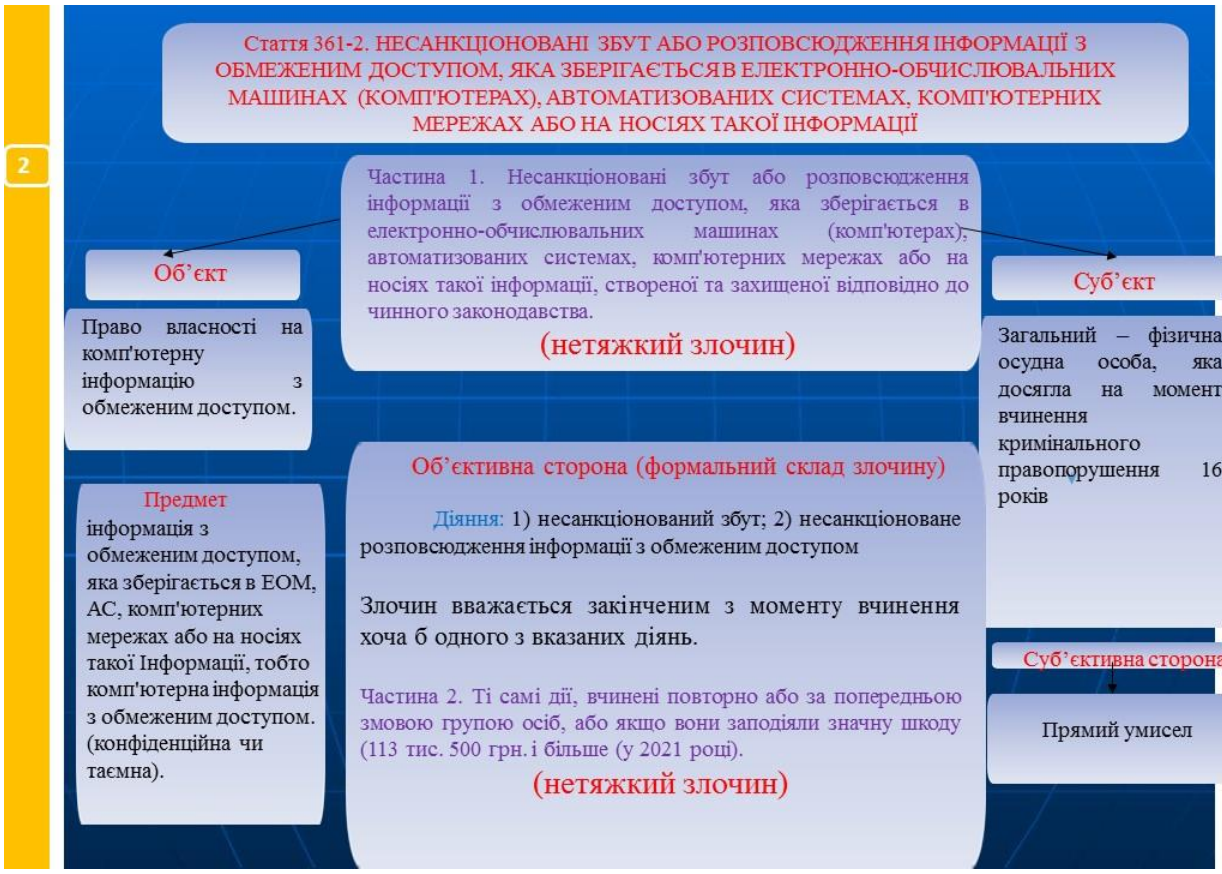


Рис. 1.12. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 362-1)

ОСОБА_2, 28 травня 2016 року, перебуваючи за адресою свого проживання, а саме, АДРЕСА_1, діючи умисно, із корисливих мотивів, реалізуючи свій злочинний умисел, направлений на несанкціонований збут інформації з обмеженим доступом, розмістив оголошення на

Інтернет майданчику «OLX» про продаж бази даних Державного реєстру фізичних осіб – платників податків з інформацією про прізвище, ім'я та по батькові, стать, дату народження, місце народження, місце проживання, ідентифікаційний код та дату його отримання, відомості з якого, відповідно до «Положення про реєстрацію фізичних осіб у Державному реєстрі фізичних осіб-платників податків», затвердженого наказом Міністерства доходів і зборів України № 779 від 10 грудня 2013 року, використовуються контролюючими органами виключно для здійснення контролю за дотриманням податкового законодавства України та є інформацією з обмеженим доступом.

У подальшому, 30 грудня 2016 року, близько 16:00 год., ОСОБА_2, діючи умисно, всупереч ч. 2 ст. 11, ч. 1 ст. 21 Закону України «Про інформацію», ст. 3, ч. 1 ст. 5 Закону України «Про захист персональних даних», перебуваючи за адресою свого проживання, а саме, АДРЕСА_1, здійснив несанкціонований збут ОСОБА_3 інформації з обмеженим доступом, у вигляді бази даних Державного реєстру фізичних осіб-платників податків, що зберігається в автоматизованих системах, за що останній перерахував ОСОБА_2 на його картковий рахунок ПАТ КБКБ «Приват Банк» грошові кошти в сумі 800 гривень.

Своїми умисними діями, що виразилися у несанкціонованому збуті інформації з обмеженим доступом, яка зберігається в автоматизованих системах, ОСОБА_2 вчинив злочин, передбачений ч. 1 ст. 361-2 КК України.

Окрім того, ОСОБА_2, 16 лютого 2017 року, близько 13:00 год., діючи умисно, повторно, всупереч ч. 2 ст. 11, ч. 1 ст. 21 Закону України «Про інформацію», ст. 3, ч. 1 ст. 5 Закону України «Про захист персональних даних», перебуваючи за адресою свого проживання: АДРЕСА_1, використовуючи оголошення, розміщене на Інтернет майданчику «OLX» щодо продажу бази даних Державного реєстру фізичних осіб-платників податків, під час проведення оперативної закупівлі, здійснив несанкціонований збут інформації з обмеженим доступом, у вигляді бази даних Державного реєстру фізичних осіб-платників податків, що зберігається в автоматизованих системах, за що ОСОБА_2 було перераховано на його картковий рахунок ПАТ КБКБ «Приват Банк» грошові кошти в сумі 995 гривень.

Своїми умисними діями, що виразилися у несанкціонованому збуті інформації з обмеженим доступом, яка зберігається в автоматизованих системах, вчиненими повторно, ОСОБА_2 вчинив злочин, передбачений ч. 2 ст. 361-2 КК України.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч.1 ст. 362 та ч. 3 ст. 362 КК

України (Кіцманський районний суд Чернівецької області, справа № 718/605/19)

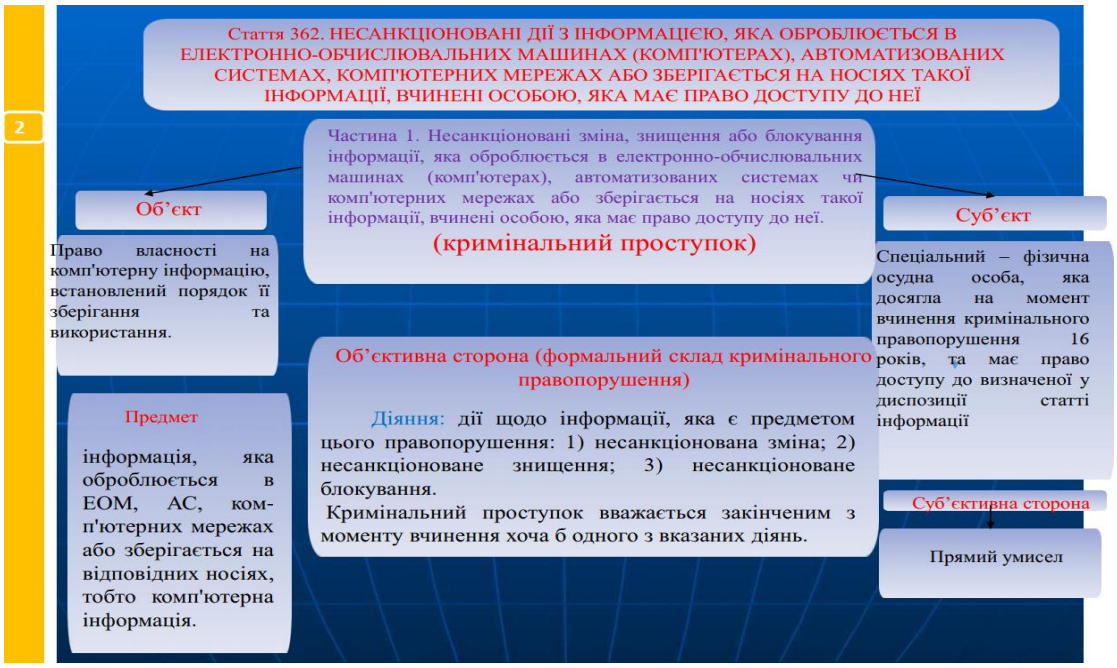


Рис. 1.13. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 – кримінальний проступок)

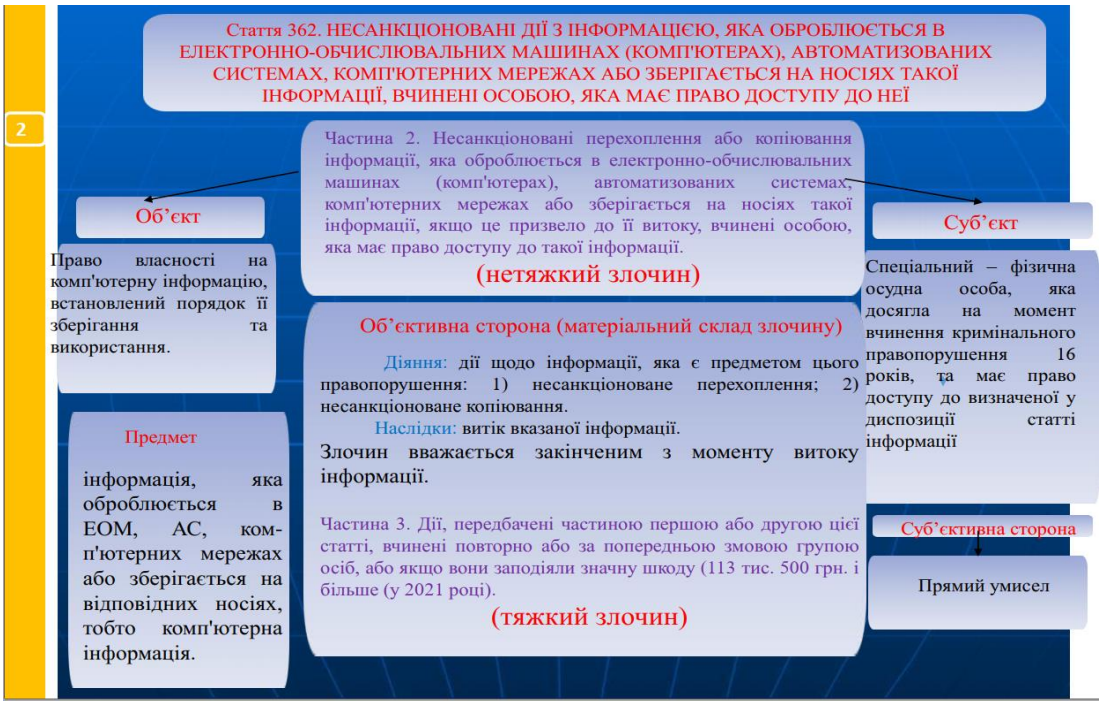


Рис. 1.14. Несанкціоновані дії з інформацією, яка обчислюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 – злочин)

09 червня 2018 року ОСОБА_2, виконуючи на підставі наказу

Чернівецького обласного управління АТ «Ощадбанк» № 636-к від 05.12.2017 року обов'язки контролера-касира сектора касових операцій ТВБВ №10025/082 філії Чернівецького обласного управління АТ «Ощадбанк», розташовано по вул. Незалежності, 32, в м. Кіцмань Чернівецької області, та, згідно до посадової інструкції, затвердженої 07.12.2017 року начальником філії Чернівецького обласного управління АТ «Ощадбанк», маючи, у силу своїх повноважень доступ до системи банківського обслуговування СБОН+, діючи умисно, в порушення вимог п. п. 6.5. та 6.8. розділу VI (Процедура відміни/сторнування Касових операцій з приймання Платежів) Положення про здійснення операцій із приймання платежів у національній валюті від фізичних осіб та суб'єктів господарювання в установах АТ «Ощадбанк, затвердженого Постановою Правління АТ «Ощадбанк» № 196 від 11.03.2016 року, у системі банківського обслуговування СБОН+, здійснила відміну/сторнування платежу платіж за «Державне мито» платника ОСОБА_5 в сумі 366 грн. та 10 грн. комісія, без відома останнього.

Також, 11.07.2018 року ОСОБА_2, виконуючи на підставі наказу Чернівецького обласного управління АТ «Ощадбанк» № 636-к від 05.12.2017 року обов'язки контролера-касира сектора касових операцій ТВБВ 10025/082 філії Чернівецького обласного управління АТ «Ощадбанк», розташованого по вул. Незалежності, 32, в м. Кіцмань Чернівецької області, та згідно посадової інструкції, затвердженої 07.12.2017 року начальником філії Чернівецького обласного управління АТ «Ощадбанк», маючи в силу своїх повноважень доступ до системи банківського обслуговування СБОН+, знаходячись на своєму робочому місці, діючи умисно, повторно, в порушення вимог п. п. 6.5. та 6.8. розділу VI (Процедура відміни/сторнування Касових операцій з приймання Платежів) Положення про здійснення операцій з приймання платежів у національній валюті від фізичних осіб та суб'єктів господарювання в установах АТ «Ощадбанк, затвердженого Постановою Правління АТ «Ощадбанк» № 196 від 11.03.2016 року, в системі банківського обслуговування СБОН+, здійснила відміну/сторнування платежу платіж за «Електроенергію» платника ОСОБА_6 в сумі 250 грн. та 5 грн. комісія, без відома останнього.

Окрім цього, за аналогічних обставин, 11 липня 2018 року ОСОБА_2, здійснила відміну/сторнування платежу платіж за «Електроенергію» платника ОСОБА_7 в сумі 200 грн. 88 коп. та 5 грн. комісія, без відома останньої та здійснила відміну/сторнування платежу платіж за «Електроенергію» платника ОСОБА_8, в сумі 30 грн. 60 коп. та 5 грн. комісія, без відома останньої.

Також, за аналогічних обставин, 31 липня 2018 року ОСОБА_2,

здійснила відміну/сторнування платежу платіж за «Електроенергію» платника ОСОБА_9, в сумі 217 грн. 68 коп. та 5 грн. комісія, без відома останньої; 08 серпня 2018 року ОСОБА_2, здійснила відміну/сторнування платежу платіж за «Газ» платника ОСОБА_10 у сумі 121 грн. 80 коп. та 5 грн. комісія, без відома останнього; 10 серпня 2018 року ОСОБА_2, здійснила відміну/сторнування платежу платіж за «Земельний податок» платника ОСОБА_11, у сумі 115 грн. 17 коп. та 10 грн. комісія, без відома останньої; 13 серпня 2018 року ОСОБА_2, здійснила відміну/сторнування платежу платіж «за електроенергію» платника ОСОБА_12, у сумі 321 грн. 12 коп. та 5 грн. комісія, без відома останнього; 10 серпня 2018 року ОСОБА_2, здійснила відміну/сторнування платежу «за електроенергію» платника ОСОБА_13, у сумі 147 грн. 12 коп. та 5 грн. комісія, без відома останнього; 31 серпня 2018 року ОСОБА_2 А.О., здійснила відміну/сторнування платежу платіж «за електроенергію» платника ОСОБА_14, у сумі 36 грн. та 5 грн. комісія, без відома останньої.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч.1 ст.363 КК України (Шевченківський районний суд м.Києва, справа № 761/11540/16-к)

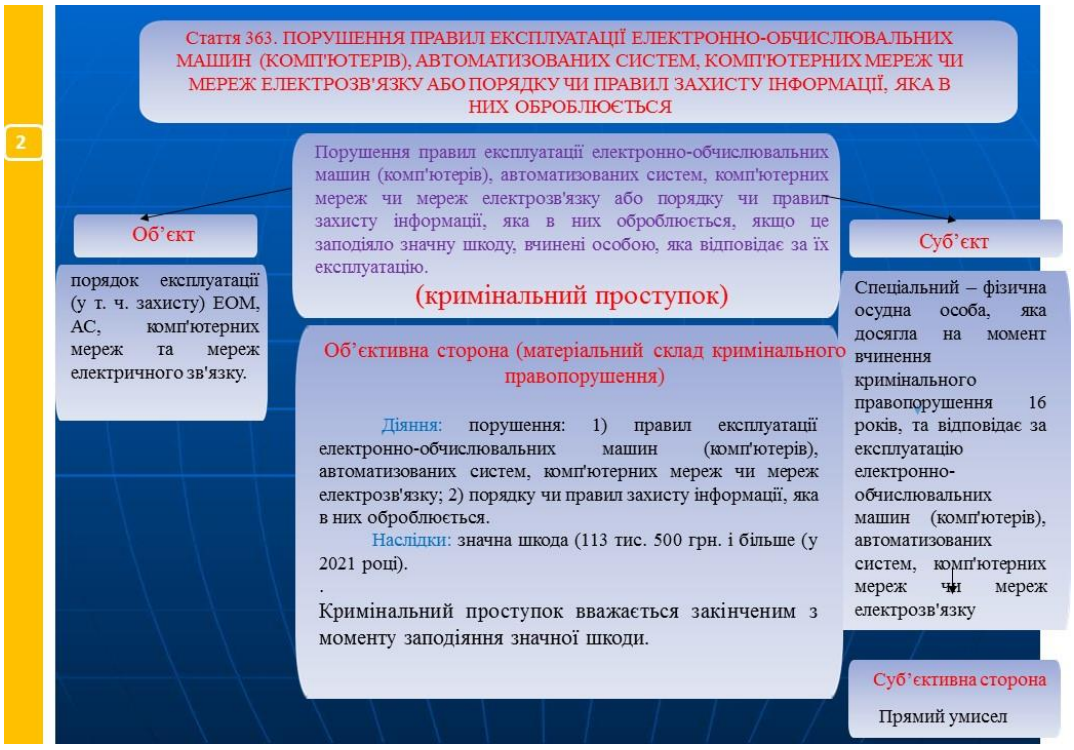


Рис. 1. 15. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363)

ОСОБА_2 у лютому 2014 року, обіймаючи посаду адміністратора

безпеки, для доступу до свого автоматизованого робочого місця (далі АРМ), яке є елементом КСЗІ ЗВІД ДП «УСС» та використовувалось ним для управління та моніторингу, створив пароль адміністратора безпеки «Ncsathokm283», чим порушив вимоги п. 9 «Експертного висновку щодо оцінки КСЗІ ЗВІД ДП «УСС», а саме «паролі адміністратора безпеки та системного адміністратора на доступ до елементів КСЗІ мають довжину не менш, аніж дванадцять символів, не містять поширених слів, використовують спеціальні символи».

Надалі, у 2015 році ОСОБА_2, встановив на своєму АРМ адміністратора безпеки, операційну систему Windows 7 Professional, чим порушив вимоги п. 6.5.1.1. «Плану захисту інформації КСЗІ ЗВІД», а саме «Заборонене використання на АРМ, що використовуються для управління та моніторингу (АРМ адміністраторів та чергової зміни), серверах та активному мережевому обладнанні програмного забезпечення, що не відповідає наведеному в проектній документації». Відповідно до таблиці 3.1. «Опису програмного забезпечення КСЗІ ЗВІД» – для забезпечення функціонування. АРМ обслуговуючого персоналу КСЗІ ЗВІД має використовуватись операційна система Windows XP Professional SP2.

Упродовж 2014-2015 років ОСОБА_2, для особистих потреб, встановив на своєму АРМ адміністратора безпеки наступні програмні засоби: «Skype», «NeroBurn», «ImageBurn» та ін., чим порушив вимоги п.6.5.1.1. «Плану захисту інформації КСЗІ ЗВІД», а саме «Заборонене використання на АРМ, що використовуються для управління та моніторингу (АРМ адміністраторів та чергової зміни), серверах та активному мережевому обладнанні програмного забезпечення, що не відповідає наведеному в проектній документації». У таблиці 3.1. «Опису програмного забезпечення КСЗІ ЗВІД» вищевказані програмні засоби відсутні.

03.03.2014 між ДП «УСС» та Державною міграційною службою України (далі ДМСУ) укладено договір на закупівлю послуг щодо обробки даних, розміщення інформації на веб-вузлах, щодо програмного застосування та інші послуги щодо забезпечення інформаційно-технологічною інфраструктурою (послуги з розміщення поштового серверу та веб-сайту (хостингу) із забезпеченням захищеного Інтернет-доступу до ресурсів веб-сайту та електронної пошти) № 15/11.18/14/КЛ.

12.03.2015 між ДП «УСС» та ДМСУ укладено договір на закупівлю послуг щодо обробку даних, розміщення інформації на веб-вузлах, щодо програмного застосування та інші послуги щодо забезпечення інформаційно-технологічною інфраструктурою (послуги з розміщення поштового серверу та веб-сайту (хостингу) із забезпеченням захищеного

Інтернет-доступу до ресурсів веб-сайту та електронної пошти) № 11.43/15/ін/11, у зв'язку із закінченням терміну дії попереднього.

Відповідно до вказаного договору № 11.43/15/ін/11, ДП «УСС» надавало ДМСУ 200 Гб дискового простору на своєму сервері для функціонування поштового серверу та веб-сайту ДМСУ, а також забезпечувало захищений доступ до поштового серверу та веб-сайту ДМСУ, відповідно до вимог законодавства в галузі захисту інформації, через захищений вузол Інтернет-доступу ДП «УСС». Відповідальною особою за технічні питання з боку ДП «УСС», було призначено адміністратора безпеки КСЗІ ЗВІД ОСОБУ_2

16.10.2014 на веб-сервері сайту ДМСУ, невстановленими особами було створено нелегітимний обліковий запис користувача»ІНФОРМАЦІЯ_2».

Надалі, у період 2015 року невстановленими особами, із використанням шкідливого програмного забезпечення, що функціонувало на АРМ адміністратора безпеки ОСОБИ_2, було скомпрометовано та отримано пароль адміністратора безпеки останнього. За допомогою отриманого паролю адміністратора безпеки, невстановлені особи надали нелегітимному обліковому запису користувача «ІНФОРМАЦІЯ_2» Root-права для можливості входу до серверу ДМСУ і здійснення несанкціонованих дій з інформацією.

В ході аналізу несанкціонованих дій вчинених під обліковим записом «ІНФОРМАЦІЯ_2» було виявлено:

– розміщений на веб-сервері ДМСУ скрипт «pass.php», який по своїй суті є веб-шелом та призначений для здійснення несанкціонованих дій;

– створений файл /tmp/.86893242 з перехопленими автентифікаційними даними АРМ співробітників ДП «УСС» та його клієнтів;

– запущені сторонні Root-процеси «ksysdefd» та «rsyncd», які мали активні з'єднання з IP-адресами 93.115.38.125 та 69.12.73.174 відповідно.

За допомогою вищевказаних несанкціонованих дій, невстановлені досудовим розслідуванням особи, перехоплювали інформацію, яка циркулювала у КСЗІ ЗВІД та на веб-сервері ДМСУ, копіювали її у файли та пересилали на невстановлені сервери закордон, що серед іншого завдало підриву авторитету ДП «УСС» як державного органу у сфері захисту інформації.

Протягом того ж періоду часу, адміністратор безпеки ДП»УСС» ОСОБА_2, обізнаний щодо обов'язків адміністратора безпеки з дотримання політики безпеки та правил експлуатації КСЗІ ЗВІД, перебуваючи за місцем роботи як службова особа державної установи, не

виконав свої обов’язки через несумлінне ставлення до них, бездіяв, тобто будучи зобов’язаним і маючи можливість вчинити дії, що входять до кола його службових обов’язків, не вжив заходів щодо виконання вимог:

– п.6.7 відомості покупних виробів технічного проекту, шифр «ЗВІД-2» щодо використання операційної системи Windows XP для забезпечення функціонування АРМ обслуговуючого персоналу підсистем ЗВІД;

– п.п.4.3.5 інструкції адміністратора безпеки КСЗІ ЗВІД, щодо контролю забезпечення прав доступу системним адміністратором;

– п.п.4.4.3 інструкції адміністратора безпеки КСЗІ ЗВІД, щодо контролю за виконанням вимоги щодо заборони використання програмно-апаратного забезпечення, що не має дозволу на експлуатацію;

– п.3.5 календарного плану захисту інформації КСЗІ ЗВІД, щодо контролю дотримання встановлених правил розмежування доступу до інформації, що циркулює в ЗВІД;

– п.3.6 календарного плану захисту інформації КСЗІ ЗВІД, щодо перевірки ПЗ та інформації на АРМах та серверах ЗВІД на наявність шкідливих програм (комп’ютерних вірусів);

– п.3.9 календарного плану захисту інформації КСЗІ ЗВІД, щодо перевірки відсутності (наявності) вірусної активності, спроб НСД.

Службовою перевіркою ДП «УСС» від 10.12.2015, було виявлено порушення ОСОБОЮ_2 правил експлуатації КСЗІ ЗВІД та положень інструкції адміністратора безпеки, що призвело до несанкціонованого доступу до інформації, яка містилась на веб-сервері ДМСУ та її витоку.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 1 ст.363-1 КК України (Деснянський районний суд м. Чернігова, справа № 750/2149/16-к)

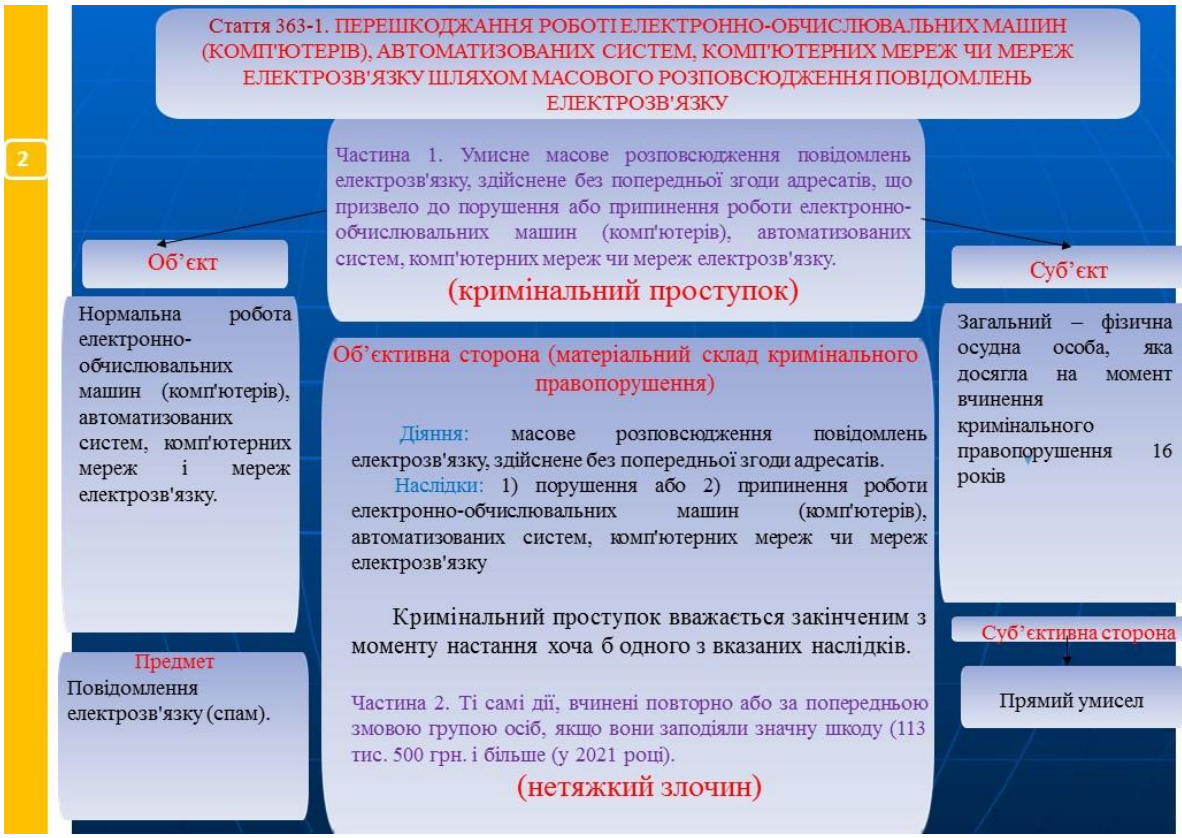


Рис. 1.16. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1)

Протягом періоду з вересня 2013 року по січень 2014 року обвинувачений, ОСОБА_1 умисно масово розповсюджував повідомлення електрозв'язку, без попередньої згоди адресатів, що призвело до порушення роботи мереж електрозв'язку, а саме: призупинення надання послуг операторами зв'язку ТОВ «Астеліт» та ПрАТ «Київстар», за наступних обставин.

Так, у вересні 2013 року, у невстановлений слідством час, ОСОБА_1, створивши сайт з назвою «ІНФОРМАЦІЯ_7» винайшов спосіб порушення роботи мереж електрозв'язку у вигляді дзвінків та SMS-повідомлень, без фактичного звукового та текстового змісту, на абонентські номери будь-якого рухомого (мобільного) зв'язку, із використанням ноутбуку «Dell» Precision M6600, s\n 6SBQ1, що належав йому та зазначеного сайту, адміністратором якого він є. Здійснював атаки з великою кількістю запитів, що призводить до відмови в обслуговуванні,

усвідомлюючи що відправлення великої кількості повідомлень електрозв'язку, спрямованих на визначений конкретний абонентський номер рухомого (мобільного) зв'язку будь-якого оператора, протягом нетривалого періоду часу спричинить порушення або призупинення роботи мереж електрозв'язку у вигляді погіршення роботи та тимчасового створення перешкод для використання за призначенням зазначеного абонентського номера рухомого (мобільного) зв'язку, та отримував від користувачів даної пропозиції грошову винагороду.

Після чого, на початку 2014 року, ОСОБА_1, достовірно знаючи номер рухомого (мобільного) зв'язку оператора ТОВ «Астеліт» НОМЕР_1 свого товариша ОСОБИ_2, знаходячись за місцем свого проживання у АДРЕСА_2, діючи умисно, реалізовуючи свій злочинний намір, спрямований на масове розповсюдження повідомлень електрозв'язку, без попередньої згоди адресатів, усвідомлюючи, що його дії призведуть до порушення роботи мереж електрозв'язку у вигляд створення перешкод для передавання та приймання повідомлень будь-якого роду по радіосистемах абонентським номерам рухомого (мобільного) зв'язку, не отримуючи згоду користувача абонентського номеру рухомого (мобільного) зв'язку оператора ТОВ «Астеліт» НОМЕР_1, з використанням власного ноутбука «Dell» Precision M6600, s\n 6SBQ1 та створеного ним сайту «ІНФОРМАЦІЯ_7», що, згідно з результатами судової комп'ютерно-технічної експертизи №1129 від 06.11.2015, призначений для відправлення певного запиту до соціальної мережі https://vk.com, після чого відбувається телефонний дзвінок або відправлення SMS-повідомлення на певний мобільний номер телефону, здійснив без фактичного звукового та текстового змісту атаки з великою кількістю запитів на даний номер телефону, що призвело до призупинення роботи мережі електрозв'язку, а саме: призупинення надання послуг оператора зв'язку ТОВ «Астеліт».

Окрім того, на початку 2014 року, ОСОБА_1, достовірно знаючи номер рухомого (мобільного) зв'язку оператора ТОВ «Астеліт» НОМЕР_2 свого товариша ОСОБИ_3, знаходячись за місцем свого проживання у АДРЕСА_2, діючи умисно, реалізуючи свій злочинний намір, спрямований на масове розповсюдження повідомлень електрозв'язку, без попередньої згоди адресатів, усвідомлюючи, що його дії призведуть до порушення роботи мереж електрозв'язку у вигляді створення перешкод для передавання та приймання повідомлень будь-якого роду по радіосистемах абонентським номерам рухомого (мобільного) зв'язку, не отримуючи згоду користувача абонентського номеру рухомого (мобільного) зв'язку оператора ТОВ «Астеліт» НОМЕР_2, з використанням власного ноутбука «Dell» Precision M6600,

s\n 6SBQ1 та створеного ним сайту «ІНФОРМАЦІЯ_7», що, згідно з результатами судової комп'ютерно-технічної експертизи №1129 від 06.11.2015, призначений для відправлення певного запиту до соціальної мережі https://vk.com, після чого відбувається телефонний дзвінок або відправлення SMS-повідомлення на певний мобільний номер телефону, здійснив без фактичного звукового та текстового змісту атаки з великою кількістю запитів на даний номер телефону, що призвело до призупинення роботи мережі електрозв'язку, а саме: призупинення надання послуг оператора зв'язку ТОВ «Астеліт».

Також, у січні 2014 року, ОСОБА_1, достовірно знаючи номер рухомого (мобільного) зв'язку оператора ПрАТ «Київстар» НОМЕР_3 свого товариша ОСОБИ_4, знаходячись за місцем свого проживання у АДРЕСА_2, діючи умисно, реалізуючи свій злочинний намір, спрямований на масове розповсюдження повідомлень електрозв'язку, без попередньої згоди адресатів, усвідомлюючи, що його дії призведуть до порушення роботи мереж електрозв'язку у вигляді створення перешкод для передавання і приймання повідомлень будь-якого роду по радіосистемах абонентським номерам рухомого (мобільного) зв'язку, не отримуючи згоду користувача абонентського номеру рухомого (мобільного) зв'язку оператора ПрАТ «Київстар» НОМЕР_3, із використанням власного ноутбука «Dell» Precision M6600, s\n 6SBQ1 та створеного ним сайту»ІНФОРМАЦІЯ_7», що, згідно з результатами судової комп'ютерно-технічної експертизи №1129 від 06.11.2015, призначений для відправлення певного запиту до соціальної мережі https://vk.com, після чого відбувається телефонний дзвінок або відправлення SMS-повідомлення на певний мобільний номер телефону, здійснив без фактичного звукового та текстового змісту атаки з великою кількістю запитів на даний номер телефону, що призвело до призупинення роботи мережі електрозв'язку, а саме: призупинення надання послуг оператора зв'язку ПрАТ «Київстар».

Також, у січні 2014 року, ОСОБА_1, достовірно знаючи номер рухомого (мобільного) зв'язку оператора ПАТ «Астеліт» НОМЕР_4 свого товариша ОСОБИ_5, знаходячись за місцем свого проживання у АДРЕСА_2, діючи умисно, реалізуючи свій злочинний намір, спрямований на масове розповсюдження повідомлень електрозв'язку, без попередньої згоди адресатів, усвідомлюючи, що його дії призведуть до порушення роботи мереж електрозв'язку у вигляді створення перешкод для передавання та приймання повідомлень будь-якого роду по радіосистемам абонентським номерам рухомого (мобільного) зв'язку, не отримуючи згоду користувача абонентського номеру рухомого (мобільного) зв'язку оператора ПАТ «Астеліт» НОМЕР_4, із

використанням власного ноутбука «Dell» Precision M6600, s\n 6SBQ1 та створеного ним сайту»ІНФОРМАЦІЯ_7», що, згідно з результатами судової комп'ютерно-технічної експертизи №1129 від 06.11.2015, призначений для відправлення певного запиту до соціальної мережі https://vk.com, після чого відбувається телефонний дзвінок або відправлення SMS-повідомлення на певний мобільний номер телефону, здійснив без фактичного звукового та текстового змісту атаки з великою кількістю запитів на даний номер телефону, що призвело до призупинення роботи мережі електрозв'язку, а саме: призупинення надання послуг оператора зв'язку ТОВ «Астеліт».

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 1 ст. 163, ч. 1 ст. 361 КК України (Франківський районний суд м. Львова, справа № 750/2149/16-к)

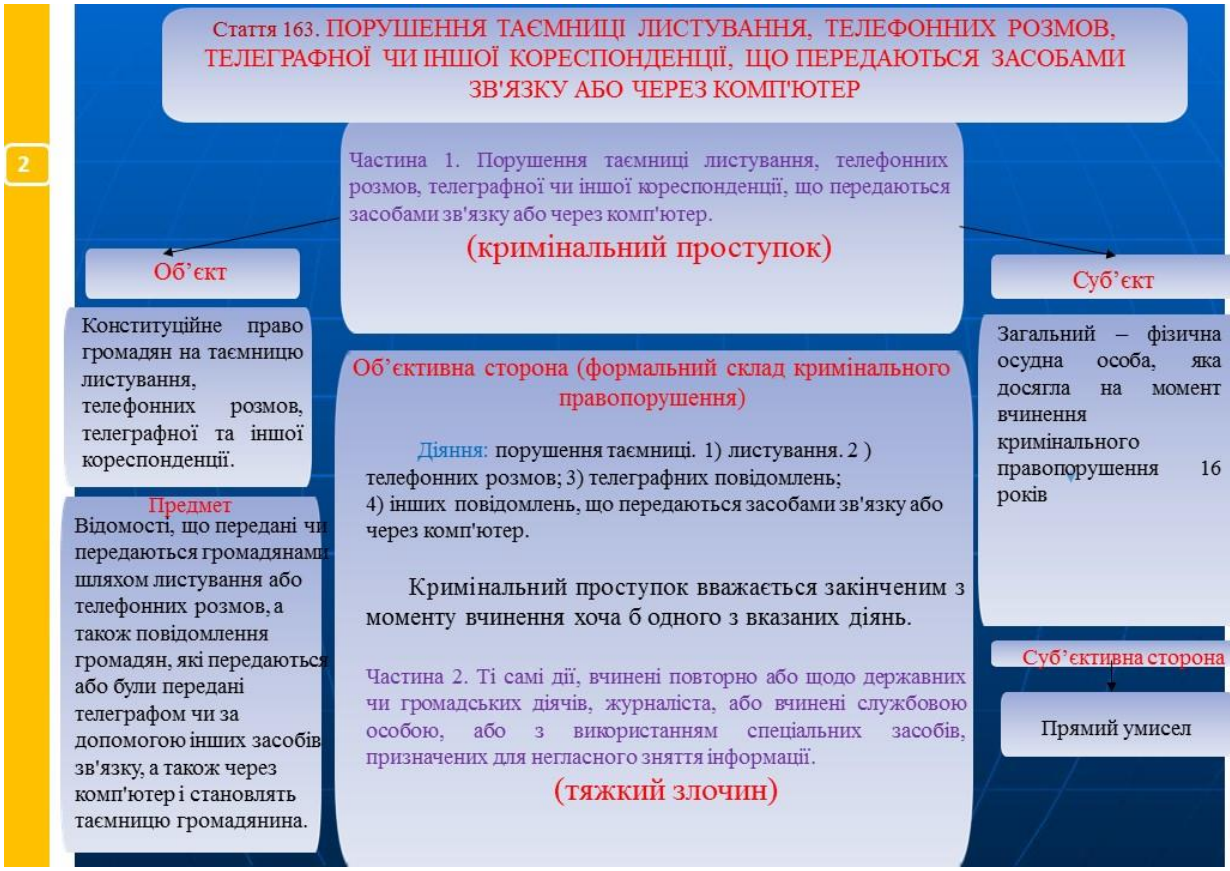


Рис. 1.17. Порушення таємниці листування, телефонних розмов, телеграфічної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163)

ОСОБА_1, у період часу із 17.11.2017 р. по 02.04.2018 р.,

перебуваючи за адресою: АДРЕСА_1, з метою помсти, використовуючи електронно-обчислювальну машину, а саме системний комп`ютерний блок с/н RC342KKRK1130400046, якій в період часу з 01.11.2017 по 02.04.2018 було надано IP-адрес: НОМЕР_1, діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, маючи авторизаційні дані, а саме логін та пароль доступу до облікового запису» ІНФОРМАЦІЯ_2», що належить ОСОБІ_2 та знаходиться у комп`ютерній мережі «i.ua», увійшовши до нього, незаконно ознайомлювався з кореспонденцією, що міститься в обліковому записі останньої та становить її особисту таємницю, чим порушив таємницю кореспонденції, що передавалась ОСОБІ_2 через комп`ютер.

Таким чином, ОСОБА_1 здійснив порушення таємниці кореспонденції, що передається через комп`ютер, тобто вчинив кримінальне правопорушення, передбачене ч. 1 ст. 163 КК України.

Окрім цього, ОСОБА_1, 02.04.2018 р. приблизно о 01:15 год., перебуваючи за адресою: АДРЕСА_1, використовуючи електронно-обчислювальну машину, а саме системний комп`ютерний блок с/н RC342KKRK1130400046, який в період часу з 01.11.2017 р. по 02.04.2018 р. мав доступ до мережі Інтернет з наданою IP-адресою: НОМЕР_1, що обслуговується провайдером ПрАТ «Київстар», діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, маючи авторизаційні дані, а саме логін та пароль доступу до облікового запису «ІНФОРМАЦІЯ_2», що належить ОСОБА_2, та є інформацією з обмеженим доступом, яка створена та захищена відповідно до вимог Цивільного кодексу України, Законів України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», здійснив несанкціоноване втручання в роботу облікового запису «ІНФОРМАЦІЯ_2» комп`ютерної мережі сервісу «i.ua», що належить та використовуються ОСОБОЮ_2, та в подальшому заблокував доступ до даного облікового запису шляхом зміни паролю, а також встановив власний номер мобільного телефону «НОМЕР_2» та власний обліковий запис альтернативної електронної пошти «ІНФОРМАЦІЯ_3», які використовуються для відновлення доступу до облікових записів сервісу «i.ua», що унеможливило б відновлення доступу до власного облікового запису «ІНФОРМАЦІЯ_2» потерпілою ОСОБА_2 .

Таким чином, ОСОБА_1 вчинив несанкціоноване втручання до роботи комп`ютерних мереж, що призвело до блокування інформації, тобто кримінальне правопорушення, передбачене ч. 1 ст. 361 КК

України.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 1 ст. 176 КК України (Подільський районний суд міста Києва, справа № 758/12401/18)

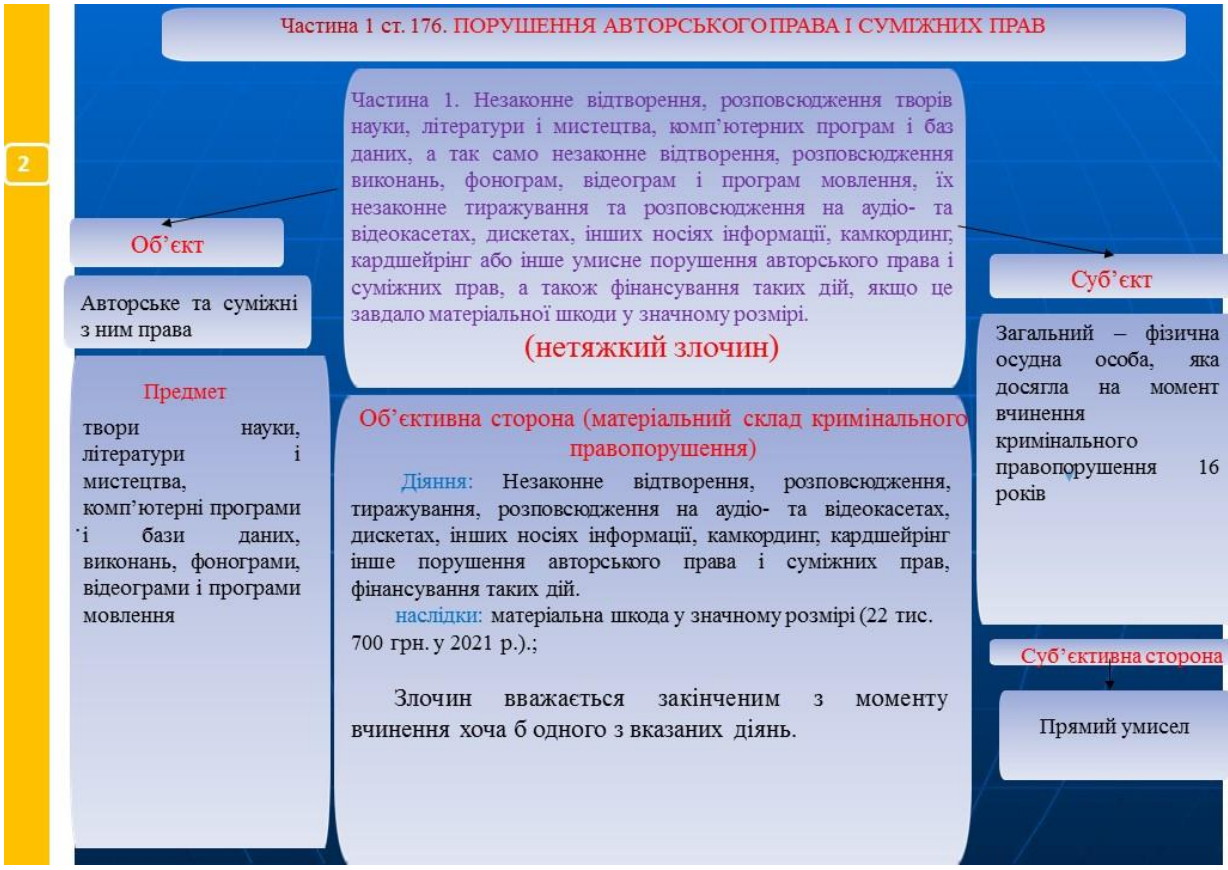


Рис. 1.18. Порушення авторського права і суміжних прав (ч.1 ст. 176)

Відповідно до обвинувального Акту від 26.04.2018 р., невстановлена слідством особа самостійно або за участю третіх осіб, у невстановленому слідством місці та в невстановлений час, здійснювала виробництво дисків для лазерних систем зчитування формату «DVD», що надавала ОСОБІ_2, для їх подальшого незаконного зберігання та розповсюдження на території ринку «Виноградар», що за адресою: АДРЕСА_3.

Так, 05.07.2014 року ОСОБА_2, перебуваючи в орендованому кіоску НОМЕР_2, за адресою: АДРЕСА_3, на території ринку «Виноградар», приблизно о 14.00 год., переслідуючи мету умисного незаконного розповсюдження DVD-дисків із записами примірників фільмів без дозволу осіб, які мають відповідне авторське право, в порушення вимог Закону України «Про розповсюдження примірників аудіовізуальних творів та фонограм, відеограм, комп'ютерних програм, без даних», з метою незаконної реалізації, зберігала при собі 4863 DVD-дисків, які відносяться до примірників

аудіовізуальних творів та відеограм, комп'ютерних програм для ігор з використанням персональних комп'ютерів та аудіо-твори і фонограми, та є об'єктами авторського права та суміжних прав.

Того ж дня, 05.07.2014 року приблизно о 14.00 год., перебуваючи у кіоску НОМЕР_2, за адресою: АДРЕСА_3, на території ринку «Виноградар» громадянин ОСОБА_4 та ОСОБА_5 було здійснено придбання у ОСОБА_2 двох DVD-дисків, які ОСОБА_2, незаконно зберігала та розповсюджувала, порушуючи авторські права.

Так, за результатами проведеної комп'ютерно-технічної експертизи, висновок експерта № 195/ікт від 14.07.2014 року, по вилученій контрафактній продукції у ОСОБА_2, встановлено, що з наданих 4863 шт. на дослідження дисків для лазерних систем зчитування формату «DVD», 4379 примірників містять ознаки контрафактності, а саме: відсутня повна інформація про авторів творів, про право власників, відсутні контрольні марки України встановленого зразку, наявність на одному диску більше одного твору, диски мають як одну так і дві робочі поверхні, 327 примірників містить ознаки контрафактності, а саме : відсутня повна інформація про авторів творів, про право власників, відсутні контрольні марки України встановленого зразку, наявність на одному диску більше одного твору. Вищевказані примірники являються аудіовізуальними творами та відеограмами, комп'ютерні програми для ігор із використанням персональних комп'ютерів та аудіо-твори та фонограми, що належать до об'єктів авторського права та суміжних прав.

Таким чином, ОСОБА_2 своїми умисними діями вчинила незаконне розповсюдження аудіовізуальних творів та відеограм, комп'ютерних програм для ігор із використанням персональних комп'ютерів та аудіо-твори і фонограми, умисне порушення авторського права, що завдало матеріальної шкоди у значному розмірі.

Такі дії ОСОБИ_2 органом досудового розслідування кваліфіковані за ч. 1 ст. 176 КК України, що виразились в умисному порушенні авторських та суміжних прав, тобто своїми діями вчинила незаконне розповсюдження на носіях інформації аудіовізуальних творів та відеограм, що завдало матеріальної шкоди у значному розмірі.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 3 ст. 190 КК України (Стрийський міськрайонний суд Львівської області, справа № 456/2818/15-к)

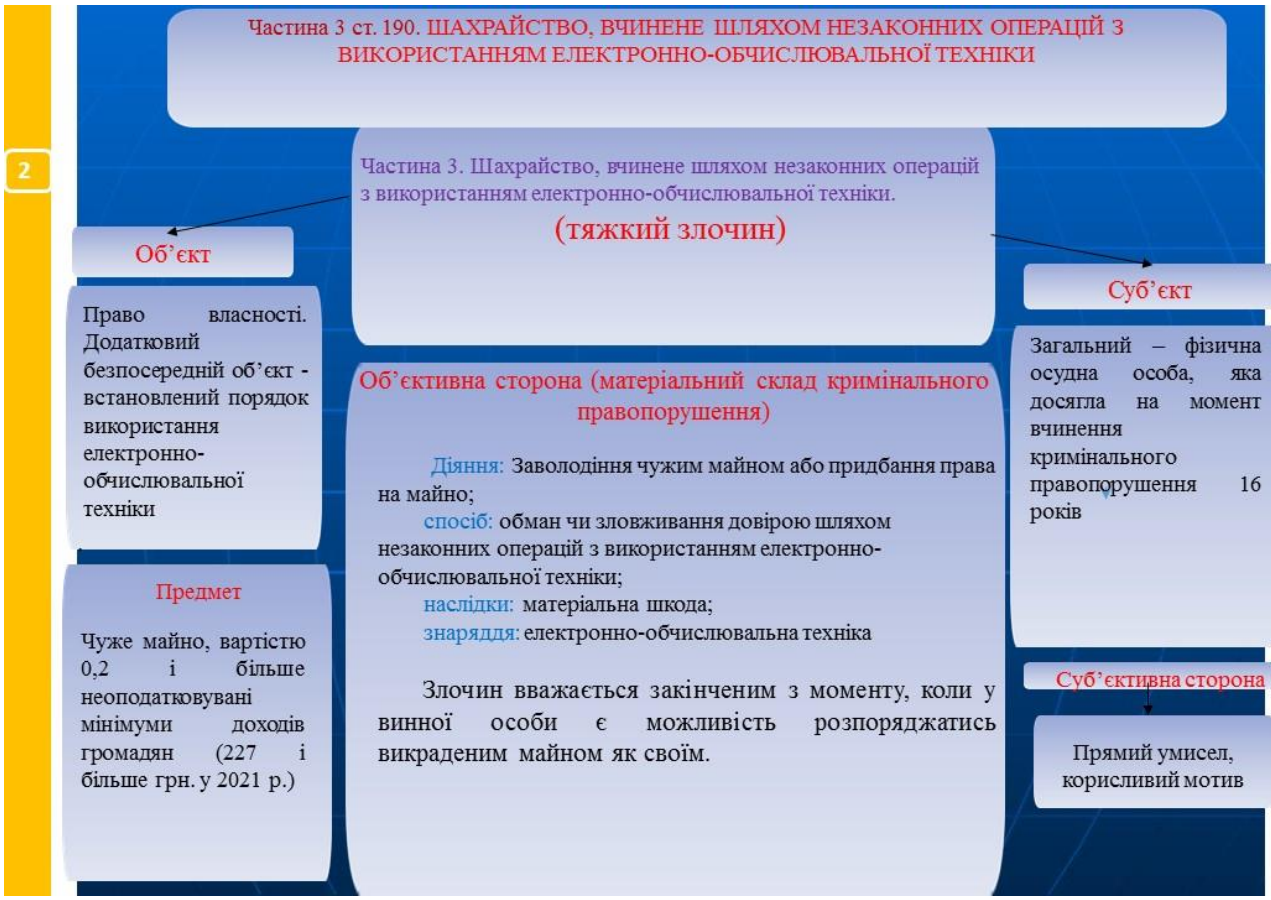


Рис. 1.19. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч.3 ст. 190)

11.10.2013 року обвинувачений ОСОБА_2 зареєструвався на сайті aukro.ua, що належить ТзОВ «Аукро Україна» і являє собою електронний аукціон, створив обліковий запис під логіком «ІНФОРМАЦІЯ_2», з НОМЕР_3 вказавши при цьому свої власні реєстраційні дані: ім'я користувача ОСОБА_2, з логіном на aukro.ua «ІНФОРМАЦІЯ_2» за адресою місця свого проживання АДРЕСА_2.

24.12.2014 року ОСОБА_2, маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіком «ІНФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua.

Під час електронного спілкування по електронній пошті ОСОБА_3 замовила у ОСОБА_2 виставлене на продаж взуття. ОСОБА_2 надав

необхідні дані для здійснення грошового переказу – реквізити пластикової картки ПАТ КБ «ПриватБанк» НОМЕР_2, запевнивши при цьому, що після перерахування коштів перешле взуття протягом доби з часу їхньої домовленості, хоча достовірно знав, що цих умов він виконувати не буде, тобто зловживаючи довірою ввів в оману потерпілу ОСОБА_3

24.12.2014 року, о 17:27:14 год., виконуючи зазначені умови усної домовленості, ОСОБА_3 перерахувала на пластикову картку ПАТ КБ «Приват Банк» НОМЕР_2, зареєстровану на ОСОБА_2, грошові кошти у сумі 190 грн. Однак, ОСОБА_2, шляхом обману та зловживання довірою заволодів 24.12.2014 року перерахованими ОСОБА_3 грошовими коштами, знявши 190 гривень в банкоматі у м. Стрий, які витратив на власні потреби, а всього завдав ОСОБА_3 матеріальної шкоди на суму 190 гривень.

Крім того, 26.12.2014 року ОСОБА_2, маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіком «ІНФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua.

Під час електронного спілкування по електронній пошті ОСОБА_4 замовив у ОСОБА_2 виставлене на продаж взуття. ОСОБА_2 надав необхідні дані для здійснення грошового переказу – реквізити пластикової картки ПАТ КБ «ПриватБанк» НОМЕР_2, запевнивши при цьому, що після перерахування коштів перешле взуття протягом доби з часу їхньої домовленості, хоча достовірно знав, що цих умов він виконувати не буде, тобто зловживання довірою ввів в оману потерпілого ОСОБА_4

29.12.2014 року о 11:54:28 год., виконуючи зазначені умови усної домовленості, ОСОБА_4 перерахував на пластикову картку ПАТ КБ «Приват Банк» НОМЕР_2, зареєстровану на ОСОБА_2, грошові кошти у сумі 190 грн. Однак, ОСОБА_2, повторно шляхом обману та зловживання довірою заволодів 29.12.2014 року перерахованими ОСОБА_4 грошовими коштами, знявши 190 гривень в банкоматі у м. Стрий, які витратив на власні потреби, а всього завдав ОСОБА_4 матеріальної шкоди на суму 190 гривень.

Крім того, 03.01.2015 року ОСОБА_2, маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіком «ІНФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua.

Під час електронного спілкування по електронній пошті ОСОБА_5

замовила у ОСОБА_2 виставлене на продаж взуття. ОСОБА_2 надав необхідні дані для здійснення грошового переказу – реквізити пластикової картки ПАТ КБ «ПриватБанк» НОМЕР_2, запевнивши при цьому, що після перерахування коштів перешле взуття протягом доби з часу їхньої домовленості, хоча достовірно знав, що цих умов він виконувати не буде, тобто зловживаючи довірою ввів в оману потерпілу ОСОБА_5

03.01.2015 року, о 15:25:46 год., виконуючи зазначені умови усної домовленості, ОСОБА_5 перерахувала на пластикову картку ПАТ КБ «Приват Банк» НОМЕР_2, зареєстровану на ОСОБУ_2, грошові кошти у сумі 190 грн. Однак, ОСОБА_2, повторно шляхом обману та зловживання довірою заволодів 03.01.2015 року перерахованими ОСОБОЮ_5 грошовими коштами, знявши 190 гривень в банкоматі м. Стрий, які витратив на власні потреби, а всього завдав ОСОБА_5 матеріальної шкоди на суму 190 гривень.

03.01.2015 року ОСОБА_2, маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіком «НФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua.

Під час електронного спілкування по електронній пошті ОСОБА_6 замовила у ОСОБИ_2 виставлене на продаж взуття. ОСОБА_2 надав необхідні дані для здійснення грошового переказу – реквізити пластикової картки ПАТ КБ «ПриватБанк» НОМЕР_2, запевнивши при цьому, що після перерахування коштів перешле взуття протягом доби з часу їхньої домовленості, хоча достовірно знав, що цих умов він виконувати не буде, тобто зловживаючи довірою, ввів в оману потерпілу ОСОБУ_6

05.01.2015 року, о 17:46:23 год., виконуючи зазначені умови усної домовленості, ОСОБА_6 перерахувала на пластикову картку ПАТ КБ «Приват Банк» НОМЕР_2, зареєстровану на ОСОБУ_2, грошові кошти у сумі 190 грн. Однак, ОСОБА_2, повторно, шляхом обману та зловживання довірою, заволодів 05.01.2015 року перерахованими ОСОБОЮ_6 грошовими коштами, знявши 190 гривень у банкоматі м. Стрий, які витратив на власні потреби, а всього завдав ОСОБІ_6 матеріальної шкоди на суму 190 гривень.

Крім того, 04.01.2015 року ОСОБА_2., маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіном «ІНФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua.

Під час електронного спілкування по електронній пошті ОСОБА_7 замовила у ОСОБИ_2 виставлене на продаж взуття. ОСОБА_2 надав необхідні дані для здійснення грошового переказу – реквізити пластикової картки ПАТ КБ «ПриватБанк» НОМЕР_2, запевнивши при цьому, що після перерахування коштів перешле взуття протягом доби з часу їхньої домовленості, хоча достовірно знав, що цих умов він виконувати не буде, тобто ввів в оману потерпілу ОСОБУ_7.

04.01.2015 року, 0 18:14:16 год., виконуючи зазначені умови усної домовленості, ОСОБА_7 перерахувала на пластикову картку ПАТ КБ «Приват Банк» НОМЕР_2, зареєстровану на ОСОБУ_2, грошові кошти у сумі 190 грн. Однак, ОСОБА_2, повторно, шляхом обману та зловживання довірою, заволодів 04.01.2015 року перерахованими ОСОБОЮ_7 грошовими коштами, знявши 190 гривень в банкоматі м. Стрий, що витратив на власні потреби, а всього завдав ОСОБІ_7 матеріальної шкоди на суму 190 гривень.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 3 ст. 301 КК України (Вільногірський міський суд Дніпропетровської області, справа № 174/234/20)

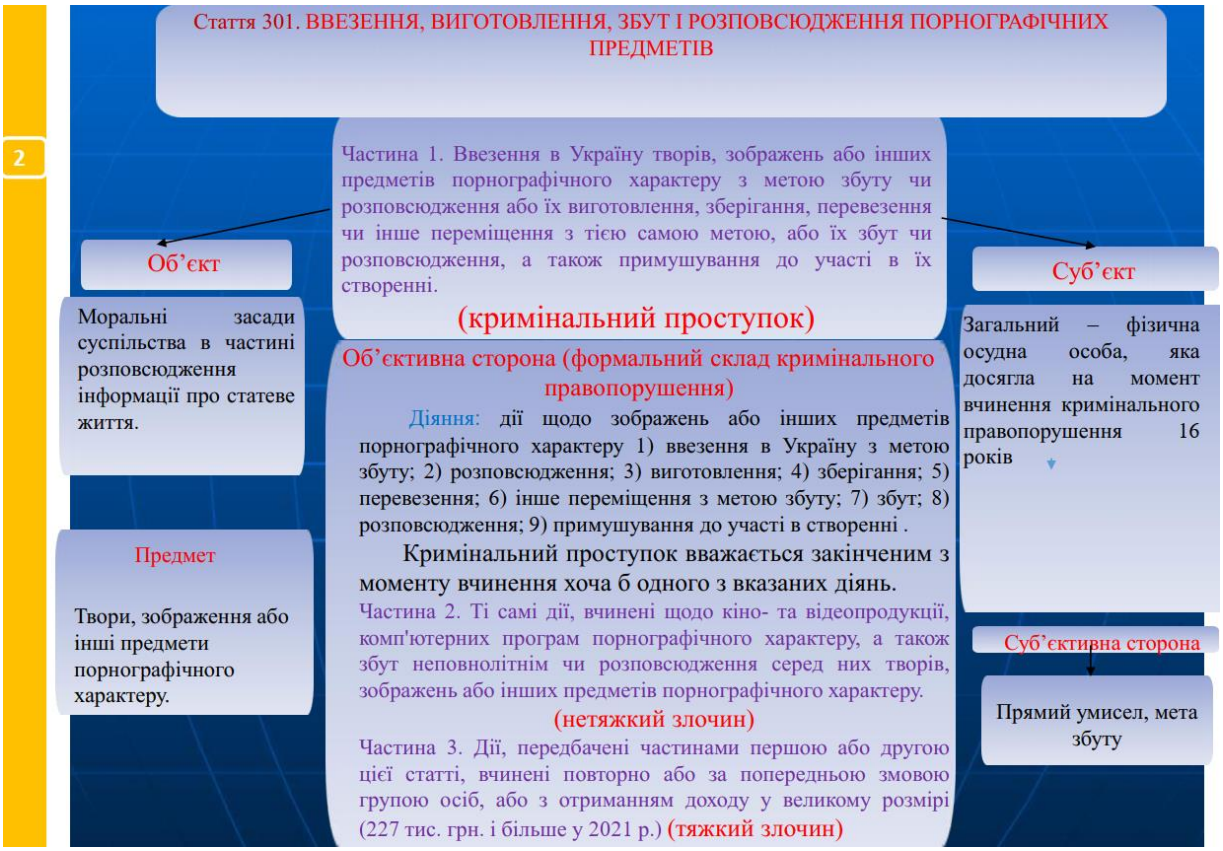


Рис. 1.20. Ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301)

Відповідно до обвинувального акту затвердженого прокурором 31 березня 2020 року ОСОБА_1 обвинувачується в тому, що повторно у не встановлені під час досудового слідства дату та час, знаходячись за місцем свого мешкання за адресою: АДРЕСА_1, маючи злочинний умисел, направлений на виготовлення, зберігання, розповсюдження зображень порнографічного характеру за допомогою фотокамери свого мобільного телефону марки «Xiomi» та власних зусиль здійснив фотографування та таким чином виготовив 2 зображення порнографічного характеру, після чого за допомогою свого персонального комп`ютера, діючи умисно, зберіг 2 вищевказані фотознімки порнографічного характеру, виготовлені ним раніше за своєю участю, тобто порушуючи суспільну мораль у сфері статевих стосунків, діючи всупереч суспільним відносинам, що складаються з приводу протидії розповсюдження порнографії і які є серйозною формою порушення принципів статевої моралі та спричиняє шкоду моральному вихованню людей, шляхом створення викривленого уявлення про інтимні стосунки між статями, а також порушуючи Закон України «Про захист суспільної моралі» від 20.11.2003 (ст. 2 «Виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні забороняються»), завідомо знаючи про те, що виготовлення, розповсюдження предметів і творів порнографічного характеру в Україні заборонено, став незаконно зберігати вказані зображення порнографічного характеру, для подальшого їх розповсюдження в мережі Інтернет.

Продовжуючи свою злочинну діяльність ОСОБА_1, 06.03.2015 о 10:04 годин, перебуваючи за місцем свого мешкання, за вищевказаною адресою, реалізуючи свій злочинний умисел, будучи зареєстрованим з використанням своєї електронної скриньки «ІНФОРМАЦІЯ_2» на веб-сайті» ІНФОРМАЦІЯ_3» з ім`ям: «ІНФОРМАЦІЯ_4» та користуючись послугами інтернет провайдера «Укртелеком», маючи злочинний умисел, направлений на розповсюдження зображень порнографічного характеру, діючи умисно, повторно розмістив 2 фотознімки порнографічного характеру в мережі Інтернет, та залишив зображення порнографічного характеру по теперішній час на своїй сторінці за адресою в мережі Інтернет «ІНФОРМАЦІЯ_4» у вільному доступі для кожного користувача мережі Інтернет, тим самим розповсюдив їх.

Окрім того, повторно, ОСОБА_1, у не встановлені під час досудового слідства дату та час, знаходячись за місцем свого мешкання за адресою: АДРЕСА_1, маючи злочинний умисел, направлений на виготовлення, зберігання та розповсюдження зображень порнографічного характеру, за допомогою фотокамери свого мобільного телефону марки «Xiomi» та власних зусиль здійснив фотографування та таким чином виготовив 3 зображення порнографічного характеру, після

чого за допомогою свого персонального комп`ютера, діючи умисно, зберіг 3 вищевказані фотознімки порнографічного характеру, виготовлені ним раніше за своєю участю, тобто порушуючи суспільну мораль у сфері статевих стосунків, діючи всупереч суспільним відносинам, що складаються з приводу протидії розповсюдження порнографії і які є серйозною формою порушення принципів статевої моралі та спричиняє шкоду моральному вихованню людей, шляхом створення викривленого уявлення про інтимні стосунки між статями, а також порушуючи Закон України «Про захист суспільної моралі» від 20.11.2003 (ст. 2 «Виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні забороняються»), завідомо знаючи про те, що виготовлення, розповсюдження предметів і творів порнографічного характеру в Україні заборонено, став незаконно зберігати вказані зображення порнографічного характеру, для подальшого їх розповсюдження в мережі Інтернет.

Зразок установчої частини обвинувального вироку за вчинення кримінальних правопорушень, передбачених ч. 1 ст. 301-1 КК України (Центральний районний суд м. Миколаєва, справа № 490/7762/21)

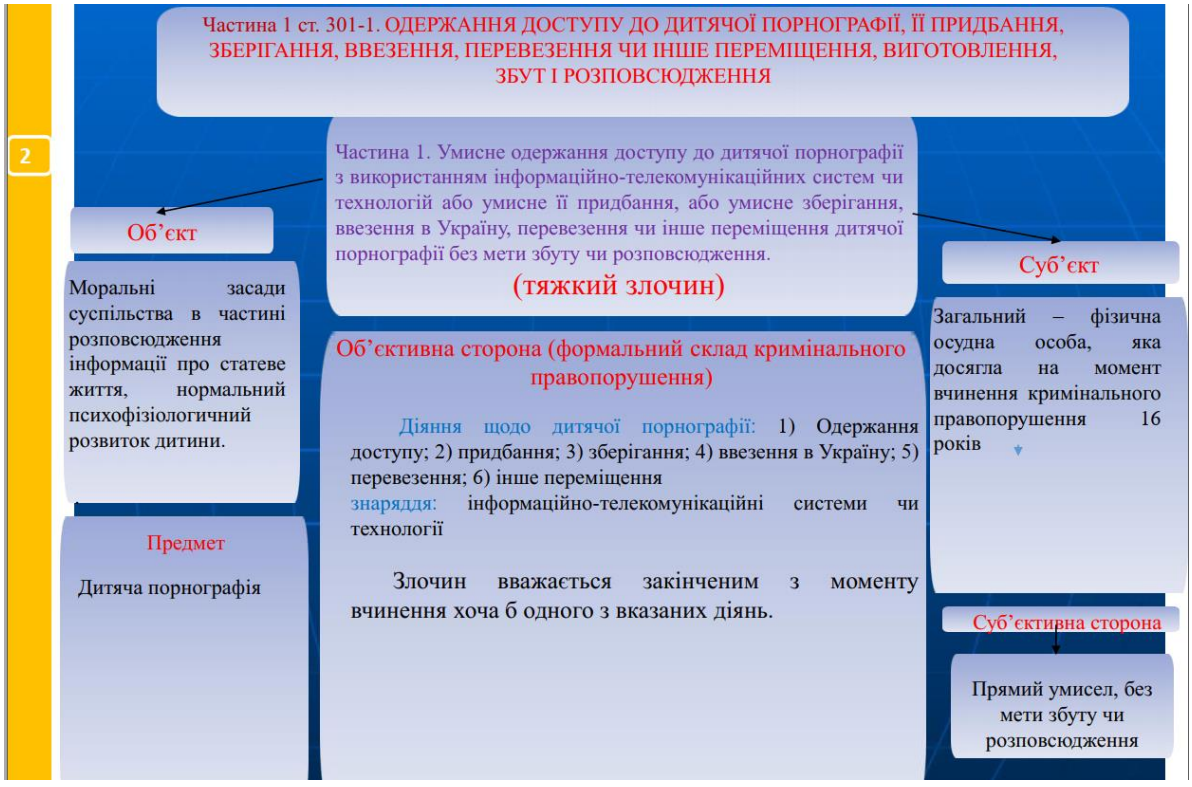


Рис. 1.21. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ч. 1 ст. 301-1)

В період часу з 2019 року по 11 червня 2021 року ОСОБА_1, перебуваючи за місцем свого постійного проживання, а у квартирі

АДРЕСА_3, використовуючи доступ до всесвітньої мережі Інтернет, який згідно договору наданий провайдером ПП «Дикий Сад» та IP-адресу НОМЕР_1, зареєстрованого на ім`я ОСОБА_1, маючи умисел на одержання доступу до дитячої порнографії з метою подальшого її зберігання, без мети збуту чи розповсюдження, порушуючи суспільну мораль, тобто систему етичних норм, правил поведінки, що склалися у суспільстві на основі традиційних духовних і культурних цінностей в частині заборони поширення серед населення вульгарно-натуралістичної, цинічної, непристойної фіксації статевих актів із зображенням у будь-який спосіб дитини, всупереч Закону України «Про захист суспільної моралі» від 20.11.2003 в редакції від 17.03.2021 року, «Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства» ратифікованої 20.06.2012 та Закону України «Про охорону дитинства» від 26.04.2001 в редакції від 17.03.2021, усвідомлюючи суспільно-небезпечний характер свого діяння, завантажив на свій персональний комп`ютер з системним блоком марки «Acer» моделі» M6 series Veritone» (серійний номер відсутній), на якому встановлено два жорстких диски, один з яких фірми виробника «Seagate» моделі «ST1000DM003-1SB1» серійний номер «Z9A1YJND» за допомогою програмного продукту «BitTorrent» 322 графічних файли та 584 відео файли на яких відображаються сцени статевих відносин відвертого порнографічного змісту, які відносяться до продукції порнографічного характеру з ознаками дитячої порнографії, які з моменту завантаження умисно зберігав на своєму комп`ютері та накопичувачі для особистого перегляду без мети збуту чи розповсюдження до тих пір, поки системний блок його персонального комп`ютеру не був вилучений працівниками поліції 11.06.2021 вході проведення санкціонованого обшуку за місцем його проживання.

Таким чином, ОСОБА_1 вчинив кримінальне правопорушення, передбачене ч. 1 ст. 301-1 КК України, що полягає в умисному одержанні доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій та умисному зберіганні без мети збуту чи розповсюдженні.

18 лютого 2021 р. Законом України «Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції)» КК України доповнений статтями 301-1 та 301-2. На сьогодні напрацьованою є лише судова практика за вчинення кримінального правопорушення, передбаченого ч. 1 ст. 301-1 КК України.

Рис. 1.22. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ч. 2 ст. 301-1)

Рис. 1.23. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ч. 3 ст. 301-1)

Рис. 1.24. Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ч. 1 ст. 301-2)

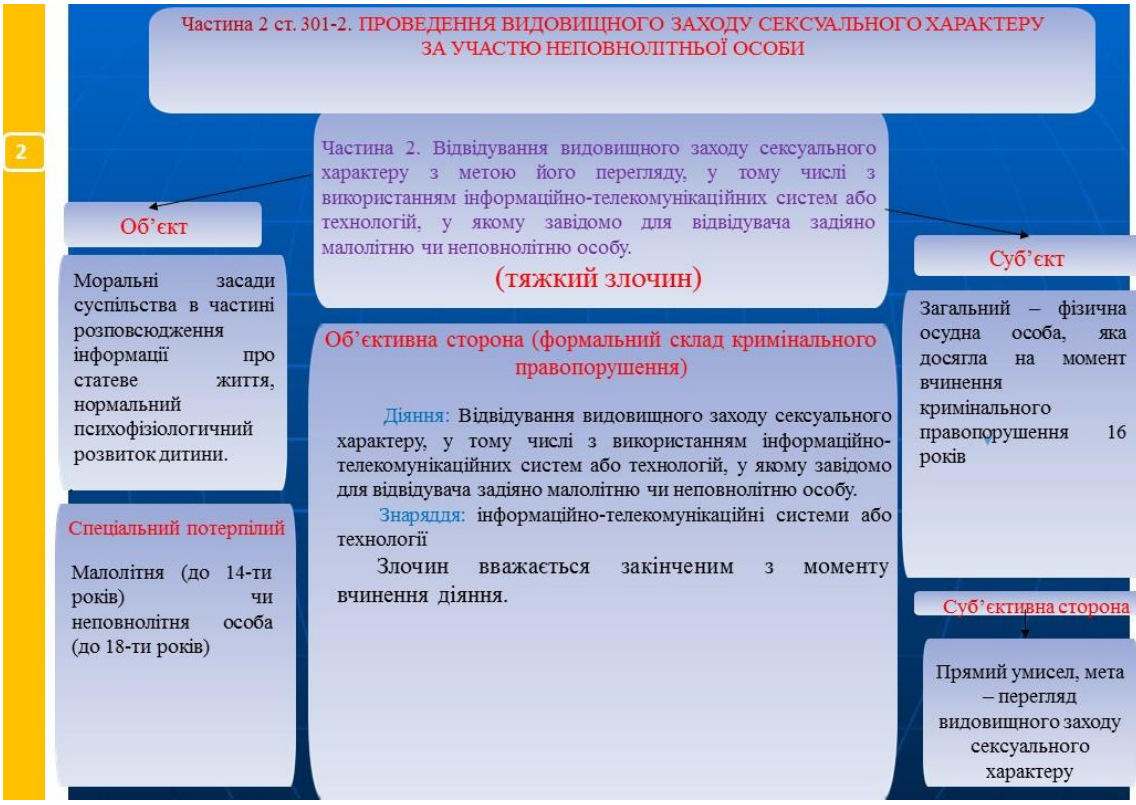


Рис. 1.24. Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ч. 2 ст. 301-2)

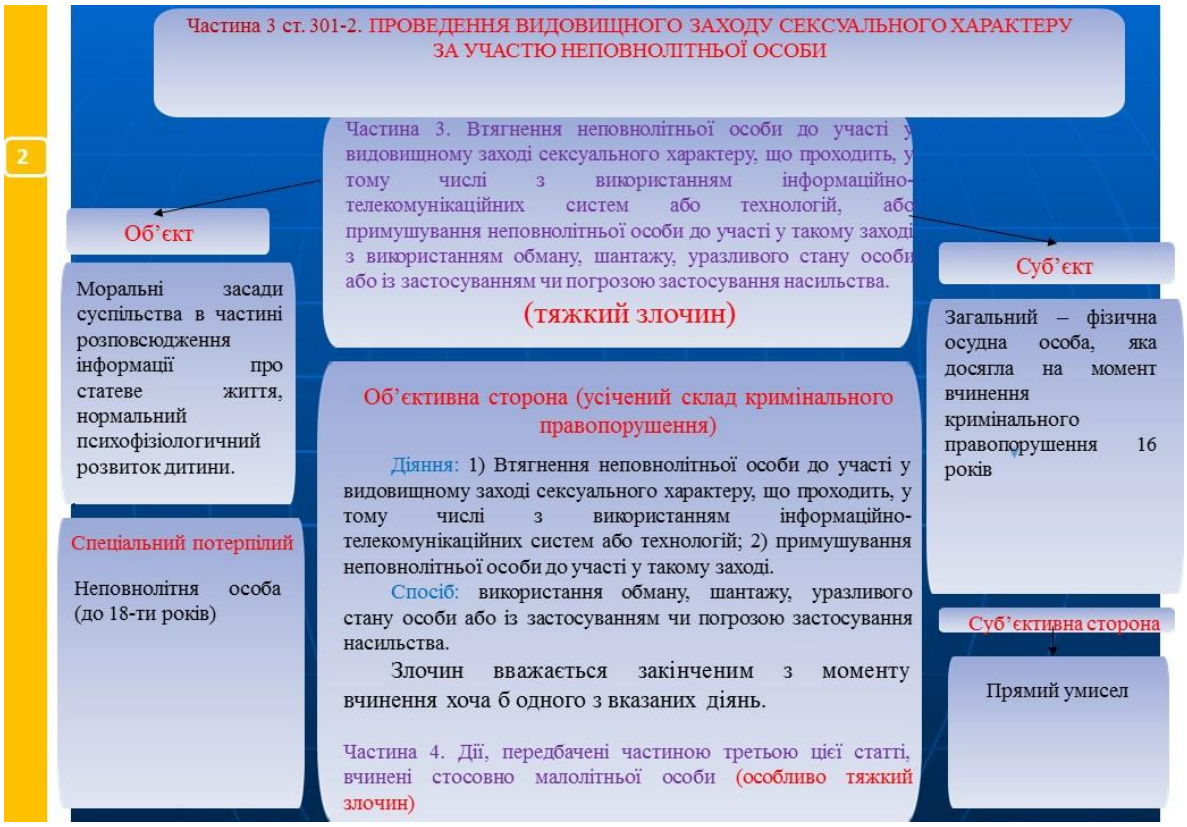


Рис. 1.25. Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ч. 3 ст. 301-2)

1.3. Удосконалення кримінального законодавства України як захід запобігання кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Серед проблем, що заважають створенню ефективно діючої системи протидії загрозам у кіберпросторі, слід виділити термінологічну невизначеність. Відмічається, що першочерговим завданням є створення за участю зацікавлених відомств базового документу із визначеннями основних понять у кібербезпековій сфері – «кіберпростір», «кібербезпека», «кібератака», «кібернапад», «кіберзахист», «кібертероризм», «кіберзлочин». Доцільно закласти ключові терміни кібербезпекової сфери (а заразом і сфери інформаційної безпеки в цілому) в нову редакцію Закону України «Про інформацію».

Стає очевидним, що правове забезпечення кібернетичної безпеки в Україні знаходиться на етапі свого розвитку, що вимагає активізації правотворчої діяльності відповідних відомств.

Крайнім та найдієвіших засобом забезпечення кібернетичної безпеки є кримінальний закон.

Розділ XVI Особливої частини КК «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» передбачає відповідальність за більшість так званих комп'ютерних кримінальних правопорушень.

На наш погляд, родовий об'єкт кримінальних правопорушень, передбачених розділом XVI Особливої частини КК, і, відповідно, назву цього розділу доцільно визначати спираючись на специфіку тієї сфери, у якій ці правопорушення вчиняються. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05 липня 1994 р. визначає поняття цих систем. Так, під інформаційною (автоматизованою) системою розуміється організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів, а під телекомунікаційною системою – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Вважаємо, що назва розділу XVI Особливої частини КК України у редакції «Кримінальні правопорушення у сфері інформаційних та

телекомунікаційних систем» буде узгоджуватись з іншими нормативно-правовими актами та відповідатиме тій сфері, у якій вчиняються передбачені цим розділом кримінальні правопорушення.

Аналіз диспозицій ст.ст. 361, 361^2, 362, 363 КК дозволяє стверджувати про формулювання у цих нормах законодавцем занадто неконкретизованих діянь, що дозволяє достатньо широко їх тлумачити і, відповідно, дезорієнтує практичного працівника при вирішенні питання щодо кваліфікації таких діянь і притягнення особи до відповідальності.

Так, ч. 1 ст. 361 КК встановлює відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

На сьогодні комп'ютери у своїй власності має чи не кожна родина. У кожному підприємстві, установі чи організації перебуває на балансі комп'ютерна техніка. Під ознаки ч. 1 ст. 361 КК підпадає будь-яке діяння, пов'язане з несанкціонованим втручанням в роботу будь-якого комп'ютера, що призвело до відповідного наслідку. Тому, наприклад, формально за ч. 1 ст. 361 КК слід кваліфікувати дії студента, який з ноутбука свого товариша без його відома шляхом вільного доступа «закачав» будь-яку інформацію (фільм, фотографію, курсову роботу тощо). Проте таке діяння, на нашу думку, не становить такого ступеня суспільної небезпеки, який потребує його криміналізації.

У зв'язку з цим вважаємо необхідним внесення змін до статей, які передбачають відповідальність за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку у напрямку деталізації діянь, за які встановлюється ця відповідальність.

Для досягнення цієї мети корисним буде вивчення досвіду криміналізації таких діянь зарубіжним законодавцем. Загалом зарубіжне законодавство, що встановлює відповідальність за комп'ютерні кримінальні правопорушення, за ступенем деталізації кримінально протиправних діянь у цій сфері можна поділити на два види: 1) з високим ступенем деталізації та 2) з низьким ступенем деталізації.

Нас, насамперед, цікавить законодавство першого виду. Для прикладу розглянемо кримінальне законодавство США. Захист комп'ютерної інформації розпочався у цій країні достатньо давно. Ще 1977 р. був розроблений законопроект про захист федеральних комп'ютерних систем. Він передбачав кримінальну відповідальність за: введення свідомо помилкових даних у комп'ютерну систему; незаконне

використання комп'ютерних пристроїв; внесення змін у процеси обробки інформації або порушення цих процесів; розкрадання коштів, цінних паперів, майна, послуг, коштовної інформації, вчинені з використанням можливостей комп'ютерних технологій або з використанням комп'ютерної інформації. На основі даного законопроекту у жовтні 1984 р. був прийнятий Закон про шахрайство й зловживання з використанням комп'ютерів – основний нормативно-правовий акт, що встановлює кримінальну відповідальність за кримінальні правопорушення у сфері комп'ютерної інформації. Надалі він неодноразово (в 1986, 1988, 1989, 1990, 1994 і 1996 р.) доповнювався.

Нині він включений у вигляді § 1030 у Титул 18 Зводу законів США. Цей закон встановлює відповідальність за діяння, предметом посягань яких є «захищений комп'ютер» (комп'ютерна інформація). Під ним розуміється (1) комп'ютер, що перебуває у винятковому користуванні уряду або фінансової організації, або комп'ютер, функціонування якого було порушено при роботі в інтересах уряду або фінансової організації, а також (2) комп'ютер, що є частиною системи або мережі, елементи якої розташовані більш ніж в одному штаті США. Одночасно закон установлює, що кримінальна відповідальність наступає у випадках (1) несанкціонованого доступу – коли стороння щодо комп'ютера або комп'ютерної системи людина вторгається в них ззовні й користується ними, або (2) перевищення санкціонованого доступу – коли законний користувач комп'ютера або системи здійснює доступ до комп'ютерних даних, на які його повноваження не поширюються.

Даний закон установлює відповідальність за сім основних складів кримінальних правопорушень: 1) комп'ютерне шпигунство, що полягає у несанкціонованому доступі або перевищенні санкціонованого доступу до інформації, а також одержання інформації, що має відношення до державної безпеки, міжнародних відносин і питань атомної енергетики (§ 1030 (a)); 2) несанкціонований доступ або перевищення санкціонованого доступу до інформації з урядового відомства США, з будь-якого захищеного комп'ютера, що має відношення до міжнародної або торгівлі між штатами, а також одержання інформації з фінансових записів фінансової установи, емітента карт або інформації про споживачів, що міститься у файлі управління обліку споживачів (§ 1030(a)); 3) вплив на комп'ютер, що перебуває у винятковому користуванні урядового відомства США, або порушення функціонування комп'ютера, використовуваного повністю або частково урядом США (§ 1030(a)); 4) шахрайство з використанням комп'ютера – доступ, здійснюваний із шахрайськими намірами, і використання комп'ютера з метою одержання будь-чого коштовного за допомогою шахрайства, у

тому числі незаконне використання машинного часу вартістю більше 5 тисяч доларів протягом року, тобто без оплати використання комп'ютерних мереж і серверів (§ 1030(a)); 5) умисне або з необережності пошкодження захищених комп'ютерів (§ 1030(a)); 6) шахрайство шляхом торгівлі комп'ютерними паролями або аналогічною інформацією, що дозволяє одержати несанкціонований доступ, якщо така торгівля впливає на торговельні відносини між штатами та іншими державами або на комп'ютер, що використовується урядом США (§ 1030(a)); 7) погроза, вимагання, шантаж та інші протиправні діяння, вчинені з використанням комп'ютерних технологій (§ 1030(a)).

Кримінальне законодавство республіки Польща в частині встановлення відповідальності за комп'ютерні кримінальні правопорушення слід, на нашу думку, також віднести до такого, яке має високий ступінь деталізації, хоча кількість таких норм є незначною і не виділена в окремий розділ.

Насамперед, слід зазначити ст. 269 КК РП, яка міститься у розділі XXXIII «Злочини проти охорони інформації». Відповідно до неї злочином є неправомірне знищення, пошкодження, блокування або зміна комп'ютерної інформації, що спричинило шкоду для діяльності із забезпечення оборони країни, безпеки комунікацій, функціонування органів державної влади й управління, інших органів управління й самоврядування, або спричинило неможливість використання комп'ютерної інформації у такій діяльності. За такі діяння передбачене покарання у вигляді позбавлення волі на строк від 6 місяців до 8 років.

У розділі XXXV «Злочини проти власності» КК РП містить норми, що встановлюють відповідальність за: таємне викрадення чужого майна шляхом несанкціонованого використання для цих цілей комп'ютерних програм (§ 2 ст. 278) «карається позбавленням волі на строк від 3 місяців до 5 років; заподіяння шкоди шляхом несанкціонованого безкоштовного використання засобів телекомунікацій (§ 1 ст. 285) – карається позбавленням волі на строк до 3 років з відшкодуванням суми заподіяної шкоди; викрадення шляхом шахрайства, якщо це супроводжувалося знищенням, зміною, модифікацією або копіюванням комп'ютерної інформації (§ 1 ст. 287) – карається позбавленням волі на строк від 3 місяців до 5 років з відшкодуванням суми заподіяної шкоди; збут з корисливою метою комп'ютерних програм, що не належать на правах власності винній особі (ст. 293) – карається позбавленням волі на строк від 3 місяців до 5 років, а при пом'якшувальних обставинах –

обмеженням волі на строк до 1 року» [6].

Таким чином вважаємо, що кримінальне законодавство України у частині встановлення відповідальності за комп'ютерні кримінальні правопорушення потребує внесення змін та доповнень, спрямованих на деталізазацію діянь, передбачених відповідними нормами, з урахуванням позитивного зарубіжного досвіду. Конкретизація суспільно небезпечних наслідків у матеріальних складах кримінальних правопорушень цього розділу (наприклад, неможливість користування інформаційно-телекомунікаційними системами протягом одного тижня або одного місяця; матеріальна шкода, значна матеріальна шкода, велика матеріальна шкода) дозволить уникнути оціночних понять у диспозиціях норм та сприятиме однозначному тлумаченню Закону і правильній кваліфікації кримінально протиправних дій.

Визначення форми вини до спричинюваних наслідків у диспозиціях норм також сприятиме однозначному тлумаченню Закону і правильній кваліфікації злочинних дій. При цьому у аналізованих злочинах вид умислу може бути як прямим, так і непрямим, а вид необережності – як злочинною самовпевненістю, так і злочинною недбалістю.

Передбачення у всіх нормах вказаного розділу такої альтернативної санкції як штраф та зменшення санкцій, що передбачають позбавлення волі на певний строк, відповідатиме загальній тенденції українського законодавця щодо гуманізації кримінальної відповідальності. Посилення ж відповідальності саме за кіберзлочини може полягати у розширенні кола кримінально-караних діянь у цій сфері.

Під ознаки ч. 1 ст. 361 КК підпадає будь-яке діяння, пов'язане з несанкціонованим втручанням в роботу будь-якого комп'ютера, що призвело до відповідного наслідку.

Пропонуємо викласти ч. 1 ст. 361 КК у наступній редакції:

«Стаття 361. Незаконні дії з комп'ютерними даними

5. Незаконне знищення, блокування, порушення цілісності, порядку маршрутування чи спотворення процесу обробки комп'ютерних даних, що призвело до неможливості користування інформаційно-телекомунікаційними системами протягом одного тижня, або спричинило умисну матеріальну шкоду окремим фізичним особам, або державним, громадським чи іншим організаціям».

У інших частинах ст. 361 КК передбачити відповідальність за такі діяння: 1) комп'ютерне шпигунство, що полягає у незаконному доступі до інформації, а також незаконне одержання інформації, яка має

[6] Волеводз А. Г., Волеводз Д. А. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран. *Правовые вопросы связи*. 2004. № 1. С. 37-48.

відношення до державної безпеки, міжнародних відносин і питань атомної енергетики України; 2) незаконний доступ до інформації Офісу Президента України, Кабінету Міністрів України, Верховної Ради України, міністерств та відомств України, а також незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку цих органів.

Суттєвої шкоди розвитку та впровадженню комп'ютерних технологій у всіх сферах діяльності людини завдають незаконні дії з так званими шкідливими програмними чи технічними засобами. Відповідальність за такі дії передбачена у ст. 361^1 КК «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут».

Проте сучасна редакція цієї норми не виключає можливості її неоднозначного тлумачення, не охоплює всі можливі злочинні діяння з предметом цього злочину, що, безумовно, знижує ефективність кримінально-правової охорони суспільних відносин у охоронюваній ст. 361^1 КК сфері. Так, диспозицією ч. 1 ст. 361^1 КК передбачено кримінальну відповідальність за створення шкідливих програмних чи технічних засобів з метою їх використання, але не криміналізоване таке використання, що є, на наш погляд, нелогічним, оскільки це діяння має більшу суспільну небезпечність, ніж створення вказаних засобів з метою використання.

Поняття «розповсюдження» є складовою поняття «збут», а тому не потребує окремої криміналізації.

Побудова ч. 1 ст. 361^1 КК як формального складу злочину не відповідає, на наш погляд, ступеню його суспільної небезпеки, оскільки останній буде підвищеним і достатнім для криміналізації лише у випадку спричинення суспільно небезпечних наслідків. Крім того, формальний склад аналізованого злочину значною мірою знижує можливість документування цієї злочинної діяльності. Також, на нашу думку, з метою однозначного тлумачення і, відповідно, застосування цієї норми є доцільним повне формальне визначення у ч. 2 такого оціночного поняття як «значна шкода». Тому вважаємо, що конкретизація суспільно небезпечних наслідків (неможливість користування інформаційно-телекомунікаційними системами протягом одного тижня або одного місяця; матеріальна шкода, значна матеріальна шкода, велика матеріальна шкода) і, відповідно, уникнення оціночних понять сприятиме однозначному тлумаченню Закону і правильній кваліфікації злочинних дій.

Передбачення у всіх частинах вказаної норми такої альтернативної

санкції як штраф та зменшення санкцій, що передбачають позбавлення волі на певний строк, відповідатиме загальній тенденції українського законодавця щодо гуманізації кримінальної відповідальності.

На підставі викладеного пропонуємо наступні зміни та доповнення до КК України:

5) Статтю 361-1 викласти у наступній редакції:

«Стаття 361-1. Незаконне використання або збут шкідливих програмних чи технічних засобів

5. Незаконне використання або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем, що призвело до неможливості користування цими системами протягом одного тижня, або спричинило матеріальну шкоду окремим фізичним особам, або державним, громадським чи іншим організаціям, –

караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк від двох до п’яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Ті самі дії, що призвели до неможливості користування інформаційно-телекомунікаційними системами протягом одного місяця, або вчинені повторно, або за попередньою змовою групою осіб, або якщо вони заподіяли значну матеріальну шкоду, – караються штрафом від двох до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

3. Ті самі дії, якщо вони спричинили велику матеріальну шкоду, -

караються штрафом від одинадцяти до двадцяти п’яти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до шести років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.»

2) Примітку до ст. 361 викласти у наступній редакції:

«Примітка. 1. У статтях 361 – 361-2, 363-1 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу.

2. У статтях 361 – 361-3 матеріальною шкодою окремим фізичним

особам вважається шкода фізичній особі, заподіяна через обмеження або виключення можливості реалізації нею своїх прав, свобод чи законних інтересів, яка в два або більше разів перевищує неоподатковуваний мінімум доходів громадян.

3. У статтях 361 – 361-3 матеріальною шкодою державним, громадським чи іншим організаціям вважається шкода, яка складається з витрат, які зазнає організація у зв'язку з порушенням її діяльності, а також витрат, які вона мусить зробити для відновлення своєї діяльності, яка в десять або більше разів перевищує неоподатковуваний мінімум доходів громадян.

4. Значною матеріальною шкодою у статтях 361 – 363 вважається шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

5. Великою матеріальною шкодою у статтях 361 – 363 вважається шкода, яка у п'ятсот і більше разів перевищує неоподатковуваний мінімум доходів громадян.»

Крім того, пропонуємо: 1) надати нормативне визначення поняття «комп'ютерні кримінальні правопорушення», до яких віднести не лише кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363[1] КК України), а й ряд кримінальних правопорушень, передбачених іншими розділами Особливої частини КК України (ст. 301 «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів» та ін.); 2) класифікувати поширені види шкоди у сфері інформаційних технологій та передбачити відповідальність за її заподіяння залежно від ступеня тяжкості у кваліфікованих та особливо кваліфікованих складах кримінальних правопорушень розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України.

1.4. Окремі кримінально-правові заходи запобігання іншим комп'ютерним кримінальним правопорушенням

Точне встановлення об'єктивних та суб'єктивних ознак вчиненого діяння та їх співставлення з ознаками складу конкретного комп'ютерного кримінального правопорушення, тобто його правильна кваліфікація, є одним з дієвих заходів запобігання кримінальним правопорушенням взагалі, й комп'ютерним, зокрема. У практичній діяльності правоохоронних органів виникають спірні питання щодо визначення ознак окремих комп'ютерних кримінальних правопорушень. Зупинимось на окремих з них.

Зображення в мережі Інтернет у режимі «онлайн» як предмет кримінального правопорушення, передбаченого ст. 301 КК України

У науковій літературі та практиці діяльності правоохоронних органів виникають питання щодо віднесення інформації порнографічного характеру, яку передають в мережі Інтернет у режимі «онлайн», до предмета кримінального правопорушення, передбаченого ст. 301 КК України.

Диспозиція ст. 301 КК України предметом цього кримінального правопорушення визначає твори, зображення або інші предмети порнографічного характеру. При цьому у літературі до останніх відносять відповідні зображення чи дії, зафіксовані на матеріальних носіях – речі (книги, картини, кінофільми, фотопродукцію, голограми, скульптури, носії інформації, яка існує у цифровій формі). Але окремо зазначають, що не може бути віднесена до предмета аналізованого кримінального правопорушення інформація, що не зафіксована на носіях, а передається мережами зв'язку (зокрема, відповідні сайти в мережі Інтернет). Однак будучи зафіксованою на матеріальних носіях (жорстких дисках комп'ютерів, оптичних дисках, картах пам'яті) така інформація набуває фізичної ознаки предмета кримінального правопорушення, передбаченого ст. 301 КК України.

В діяльності окремих підрозділів Національної поліції України виникали питання щодо кваліфікації діянь осіб, які організували студію з передачі зображень порнографічного характеру в мережі Інтернет у режимі «онлайн»: 1) жінок, які вчиняли дії порнографічного характеру та передавали їх зображення в мережі Інтернет у режимі «онлайн»; 2) осіб, які забезпечували таку передачу за допомогою комп'ютерної техніки; 3) осіб, які підшукували жінок-моделей, навчали їх працювати перед веб-камерою, але безпосередньо не приймали участі в онлайн-трансляціях дій

порнографічного характеру; 4) осіб, які створили студії з розповсюдження в мережі Інтернет у режимі «онлайн» зображень порнографічного характеру, підшукали пособників, або ж самі здійснювали підбор моделей, їх навчання, забезпечення комп'ютерною технікою.

Вважаємо, що інформацію порнографічного характеру, яку передають в мережі Інтернет у режимі «онлайн», слід визнавати зображенням порнографічного характеру і, відповідно, предметом кримінального правопорушення, передбаченого ст. 301 КК України, оскільки під зображенням у загальному розумінні мається на увазі об'єкт, образ, явище, більш або менш подібне (але не ідентичне) тому, що зображується, або сам процес його створення. Подібність досягається внаслідок фізичних законів одержання зображення (оптичне зображення тощо) або є результатом праці творця зображення (малюнок, живопис, скульптура, сценічний образ тощо). Наприклад, фотографія є носієм зображення певного оригіналу, проте не є точною копією усіх його точок. Відповідність об'єкту досягається, коли кожна його точка зображується точкою хоча б приблизно.

Таким чином, трансляція дій порнографічного характеру в мережі Інтернет у режимі «онлайн» є зображенням порнографічного характеру, подібність якого до оригіналу досягнута внаслідок фізичних законів одержання зображення (перетворення відповідних точок оригіналу в електронний сигнал та приблизне відтворення цих точок на моніторі іншого комп'ютера, підключеного до мережі Інтернет, з використанням комп'ютерної техніки та програмного забезпечення (веб-камер, програми Skype та ін.).

Від трансляції дій порнографічного характеру в мережі Інтернет у режимі «онлайн», як предмета кримінального правопорушення, передбаченого ст. 301 КК України, слід відрізняти спостереження за діями порнографічного характеру під час безпосереднього спілкування особи, яка спостерігає, та особи, яка вчиняє ці дії. У цьому випадку предмет аналізованого кримінального правопорушення відсутній, оскільки відсутнє саме зображення, а є оригінал.

Отже, дії осіб, зазначених у вищезазначених пунктах 1 та 2, слід кваліфікувати як виготовлення з метою збуту та збут зображень порнографічного характеру, вчинені повторно (за наявності декількох кримінальних правопорушень), за попередньою змовою групою осіб, тобто за ч. 3 ст. 301 КК України. Дії осіб, вказаних у п. 3, слід кваліфікувати як пособництво у виготовленні з метою збуту та збуті зображень порнографічного характеру, вчинені повторно (за наявності декількох кримінальних правопорушень), за попередньою змовою

групою осіб, тобто за ч. 5 ст. 27, ч. 3 ст. 301 КК України. Дії осіб, зазначених у п. 4, слід кваліфікувати як організаторів виготовлення з метою збуту та збуту зображень порнографічного характеру, вчинені повторно (за наявності декількох кримінальних правопорушень), за попередньою змовою групою осіб, тобто за ч. 3 ст. 27, ч. 3 ст. 301 КК України.

Проведене опитування молодих людей у віці 18-20 років у м. Дніпрі свідчить, що 92 % з них дивились твори порнографічного змісту. До того ж, 26% опитаних вважають розповсюдження порнографії фактором, який найбільше сприяє поширенню кримінальних правопорушень проти статевої свободи та недоторканості особи в Україні.

Диспозиція ст. 301 КК України предметом цього кримінального правопорушення визначає твори, зображення або інші предмети порнографічного характеру, кіно- та відеопродукцію, комп'ютерні програми такого ж характеру.

КК пострадянських країн містять як спільні з КК України (ст. 255 КК Грузії, ст. 262 КК Киргизької Республіки), так і дещо відмінні визначення предмета ввезення, виготовлення, збуту і розповсюдження порнографічних предметів. Так, КК окремих з цих країн предметом цього кримінального правопорушення визначають порнографічні матеріали (в тому числі друковані видання) (ст. 242 КК Азербайджанської Республіки, ст. 343 КК Республіки Білорусь, ст. 263 КК Республіки Вірменія, ст. 273 КК Республіки Казахстан, ст. 166 КК Латвійської Республіки, ст. 242 КК РФ, ст. 241 КК Республіки Таджикистан). КК Литовської Республіки (ст. 309), Республіки Узбекистан (ст. 130) визначають предмет цього кримінального правопорушення лише як предмети порнографічного змісту, КК Республіки Молдова – фотографії чи інші зображення, у тому числі в електронній формі (ст. 208-1), КК Туркменістану – порнографічні друковані видання та інші предмети (ст. 164).

Для усунення суперечностей кваліфікації аналізованого діяння доцільно внести доповнення до ст. 301 КК України, використавши при цьому досвід криміналізації цього діяння окремих пострадянських країн. Так, ч. 2 ст. 263 КК Республіки Вірменія передбачає обов'язковою ознакою цього кримінального правопорушення подання дитячої порнографії через комп'ютерну систему; ч. 2 ст. 343 КК Республіки Білорусь – виготовлення та розповсюдження порнографічних матеріалів чи предметів порнографічного характеру з використанням глобальної комп'ютерної мережі Інтернет, іншої мережі електрозв'язку загального користування чи виділеної мережі електрозв'язку; п. б ч. 3 ст. 242 КК РФ – з використанням засобів масової інформації, у тому числі інформаційно-телекомунікаційних мереж (включно з мережею

«Інтернет»). Пропонуємо передбачити у ст. 301 КК України таку кваліфікуючу ознаку як вчинення цього кримінального правопорушення з використанням засобів масової інформації, у тому числі глобальної комп'ютерної мережі Інтернет, іншої мережі електрозв'язку загального користування чи виділеної мережі електрозв'язку.

Електронно-обчислювальна техніка як знаряддя кримінального правопорушення, передбаченого ч. 3 ст. 190 КК України

Обов'язковою ознакою шахрайства, вчиненого шляхом використання незаконних операцій з використанням електронно-обчислювальної техніки, є знаряддя цього злочину, а саме електронно-обчислювальна техніка. На нашу думку, поняття електронно-обчислювальної техніки, яке використовується у ч. 3 ст. 190 КК, співпадає з поняттям «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку», що використовується у розділі XVI Особливої частини КК України.

Підхід до визначення поняття «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку», в світі є неоднаковим. В теорії кримінального права України щодо цього поняття висловлюються різні точки зору.

На нашу думку, електронно-обчислювальна машина (комп'ютер) – це сукупність технічного та програмного забезпечення, призначених для автоматичної обробки інформації, яка частково керована оператором.

Під автоматизованими системами маються на увазі системи, які здійснюють автоматизовану обробку даних і до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки), а також методи і процедури, програмне забезпечення. Згідно Державного стандарту України автоматизована система є організаційно-технічною системою, яка складається із засобів автоматизації певного виду (чи кількох видів), діяльності людей та персоналу, який виконує цю діяльність[7].

Під комп'ютерною мережею слід розуміти дві або більше електронно-обчислювальні машини з наявними, обладнаних робочими місцями, які пов'язані налагодженими каналами зв'язку, що забезпечує можливість в автоматизованому порядку обробляти та обмінюватись даними та інформацією, а також використовувати спільні електронні ресурси.

Держстандарт України каналом або лінією зв'язку визначає фізичні

[7] П. 1.1 ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Київ: Держстандарт України, 1994.

канали або середовище зв'язку між технічними засобами інформаційної мережі [8].

Вважаємо, що під узагальнюючим поняттям електронно-обчислювальної техніки, доцільно розуміти термін «комп'ютерні системи», який у повному обсязі охоплює поняття електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку.

Використання електронно-обчислювальної техніки як спосіб вчинення кримінального правопорушення, передбаченого ч. 3 ст. 190 КК України

Найбільш розвиненою формою шахрайства в Інтернеті є фішинг. За визначенням фахівців компанії Dr. Web, фішинг (phishing) – технологія інтернет-шахрайства, що полягає в крадіжці особистих конфіденційних даних, таких як паролі доступу, дані банківських і ідентифікаційних карт та ін. За допомогою спамерських розсилок або поштових черв'яків потенційним жертвам відправляються підроблені листи нібито від імені легальних організацій, в яких їх просять зайти на підроблений злочинцями сайт такої установи і підтвердити паролі, PIN-коди і іншу особисту інформацію, використовувану згодом зловмисниками для крадіжки грошей з рахунку жертви і в інших злочинах.

Зловмисники використовують перехоплювачі клавіатури, поштові повідомлення, складені за всіма правилами соціальної інженерії, спеціально розроблені веб-сайти. Дедалі вище рівень стає підготовленості атак на комп'ютерні системи.

За даними звіту APWG (Anti-Phishing Work Group), щомісячно виявляється понад 20 тис. фішингових розсилок і близько 12 тис. фішерських веб-сайтів[9]. За словами авторів дослідження, кожний такий лист може бути надісланий сотням тисяч інтернет-користувачів. Середній термін існування фішерських сайтів – п'ять днів, але його цілком досить для шахрайства. У середньому за місяць під загрозою виявляються клієнти 137 організацій.

Протягом останнього часу фіксується різке зростання числа фішингових сайтів – на 65%. На думку експертів APWG, це викликане появою так званих phishing kit – утиліт, що дозволяють у короткі терміни створити фішинг-сайт. За відомостями компанії Websense, один з найбільш популярних інструментів для конструювання фішинг-ресурсів

[8] П. 7.19. «Лінія зв'язку». ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Київ: Держстандарт України,1994.

[9] Хакерские атаки. URL : http:// www. patent. net. Ua / intellectus / patentbureau_news /clear_up /2228/ua.html/.

називається Rock Phish Kit. У цей час ситуація з фішингом нагадує ту, що існувала раніше під час написання вірусів у момент появи конструкторів вірусів [10].

Коротко суть фішингу можна звести до наступного. Шахрай, одурюючи користувача, примушує його надати свою конфіденційну інформацію: дані для виходу в Інтернет (ім'я і пароль), відомості про кредитні картки і т.п. Причому всі дії жертва виконує абсолютно добровільно, не розуміючи суті того, що відбувається. Для забезпечення цього зловмисники використовують технології соціальної інженерії. Як правило, тема та текст у листах, що є спробами «фішингу», погано відформатовані й містять багато помилок. До того ж лист починається з безособового привітання, наприклад – «Дорогий Клієнте», тоді як реальні компанії, зазвичай, звертаються до адресата по імені.

Ознакою шахрайства також може бути надто турботливий чи тривожний тон листа, що сповіщає про втрату багатьма клієнтами їхніх облікових даних і можливість повторення такої ситуації з адресатом.

Зараз фішинг можна розділити на три види: поштовий, онлайновий та комбінований. Найстаріший з них – поштовий: електронною поштою надсилається спеціальний лист з вимогою вислати які-небудь дані. При онлайновому фішингу зловмисники копіюють які-небудь сайти (найчастіше інтернет-магазини), використовуючи схожі доменні імена та аналогічний дизайн. Жертва, що потрапила у такий магазин, вирішує придбати товар. Причому число покупців тут достатньо велике, адже ціни в неіснуючому магазині суттєво занижені, а всі підозри зникають через популярність копійованого сайту. Набуваючи товару, покупець реєструється, вводить номер та інші дані своєї кредитної картки. За даними MarkMonitor, більшість нелегальних сайтів, що займаються розкраданням брендів, зареєстровані у Сполучених Штатах Америки, Німеччині та Великій Британії.

Такі способи фішери застосовують досить давно. Проте, завдяки розповсюдженню знань в області інформаційної безпеки вони поступово перетворюються на неефективні способи «відбирання грошей».

Третій вид фішинга – комбінований. Суть його полягає у тому, що створюється підроблений сайт якої-небудь організації, а потім туди заманюються потенційні жертви. Тут шахраї пропонують користувачам (з урахуванням знання психології) провести якісь операції самостійно.

Численні попередження, що практично щодня з'являються в Інтернеті, роблять подібні методи шахрайства досить відомими. Тому тепер зловмисники стали частішими вдаватися до застосування key-

[10] Комп'ютерне шахрайство. URL : http://www.e-sat.com.ua/shahrajstvo.html.

loggers – спеціальних програм, що відстежують натиснення клавіш та посилають отриману інформацію за наперед призначеними адресами.

Другим розповсюдженим способом шахрайства з використанням електронно-обчислювальної техніки є вішинг (vishing). Це технологія інтернет-шахрайства, різновид фішингу, що полягає у використанні war diallers (автонабирачів) і можливостей інтернет-телефонії (VOIP) для крадіжки особистих конфіденційних даних, таких як паролі доступу, номери банківських та ідентифікаційних карт і т.п.

Схема обману аналогічна: клієнти якої-небудь платіжної системи отримують повідомлення електронною поштою нібито від адміністрації або служби безпеки даної системи з проханням вказати свої рахунки, паролі і т.п. Але, якщо у разі фішингу, посилання в повідомленні відправляє на підроблений сайт, де і відбувається крадіжка інформації, то у разі вішингу у повідомленні міститься прохання подзвонити на певний міський номер. При цьому зачитується повідомлення, в якому потенційну жертву просять видати свої конфіденційні дані. Власників такого номеру знайти не легко, оскільки з розвитком інтернет-телефонії дзвінок міського номеру може бути автоматично перенаправлений у будь-яку точку земної кулі на віртуальний номер, про що особа, яка дзвонить, не здогадується.

Компанія Secure Computing зіткнулася з витонченішим способом обману, коли електронна пошта взагалі не використовується. Злочинці програмують комп'ютер так, щоб він набирав телефонні номери з довгого списку і програвав записане повідомлення будь-кому, хто відповідає на дзвінок. У цьому повідомленні людину попереджають, що інформація про його кредитну карту потрапила до шахраїв, і просять ввести з клавіатури телефону номер.

Застосування протоколу VOIP допомагає понизити витрати на телефонний зв'язок, але разом з тим робить мережі компаній більш уразливими для атак. Банки і інші організації, що використовують для голосового зв'язку IP-телефонію, ризикують піддати себе вішинг-атакам, для профілактики яких поки немає ніяких засобів. Зловмисники дістануть доступ до персональних даних, зокрема до номерів кредитних карт і облікової банківської інформації, і лише невелика кількість фахівців в області інформаційної безпеки зможе їм перешкодити.

Згідно інформації від Secure Computing шахраї конфігурують war dialler, який набирає номери в певному регіоні, і в той момент, коли на дзвінок відповідають, відбувається наступне:

– автовідповідач попереджає споживача, що з його картою проводяться шахрайські дії і пропонує негайно передзвонити за певним номером. Це може бути номер 0800, часто з вигаданим ім'ям, що дзвонив

від імені фінансової організації;

– коли за цим номером передзвонюють, то на іншому кінці дроту відповідає типово «комп'ютерний» голос, який повідомляє, що людина повинна пройти звірку даних і ввести 16-значний номер карти з клавіатури телефону;

– як тільки номер введений, вішер стає володарем всієї інформації (номер телефону, повне ім'я, адреса), необхідної для того, щоб, наприклад, обкласти карту штрафом;

– потім, використовуючи цей дзвінок, можна зібрати і додаткову інформацію, таку як PIN-код, термін дії карти, дата народження, номер банківського рахунку і т.п.

Проте, поки серйозних інцидентів такого роду ще не відмічено. Алан Нунн, старший фахівець, за технологіями компанії Newport Networks, що займається продажами технологій VOIP, визнав, що, ймовірно, між фахівцями, які намагаються зупинити розповсюдження нового виду шахрайства, і злочинцями, що шукають нові жертви, розвернеться «гонка озброєнь»: «Зловмисники поки знаходяться на стадії експериментування. Але одночасно з цим відбувається і реальне шахрайство». Ясно, що компанії, які займаються інтернет-телефонією, поступово повинні будуть зробити ряд технічних заходів для вирішення нових проблем. Як відомо, багато інтернет-провайдерів мають чорні списки адрес, з яких розсилається спам. Повинні бути складені аналогічні списки абонентів, які займаються вішингом, щоб будь-який вихідний від них дзвінок блокувався до того, як він дійде до абонента, який викликається.

Наступним способом шахрайства з використанням електронно-обчислювальної техніки є фармінг (pharming). Це перенаправлення жертви за помилковою адресою. Зловмисник псує навігаційну інфраструктуру, від якої залежить функціонування браузера, і опановує деякою її частиною. Це може бути локальна версія, файл hosts або система доменних імен (domain name system, DNS), використовувана інтернет-провайдером для наведення браузера на потрібний об'єкт.

Механізм фармінгу має багато загального із стандартним вірусним зараженням. Жертва відкриває непрошене поштове послання або відвідує якийсь веб-сервер із файлом, який таємно запускається у фоновому режимі. При цьому спотворюється файл hosts1. Операція займає лише секунду, але шкідливе програмне обладнання може містити URL багатьох банківських структур. Механізм перенаправлення активізується в той момент, коли користувач набирає знайому довірену адресу, відповідну його банку, і потрапляє на один з помилкових сайтів.

Спеціальних механізмів захисту від фармінгу зараз не існує, так що

необхідно уважно контролювати вхідну пошту, регулярно оновлювати антивірусні бази, закривати вікна попереднього перегляду в поштовому клієнті і т.д.

В Україні останнім часом почастішали випадки наступного способу шахрайства з використанням електронно-обчислювальної техніки – скіммінгу – особливого виду шахрайства з пластиковими картками. Діють шахраї приблизно так: на щілину банкомату, куди вставляється карта, а також на клавіатуру поміщаються спеціальні пристрої-накладки. Перша копіює інформацію з магнітної смуги карти, друга – запам'ятовує пін-код. Буває і так, що пін-код фіксує мініатюрна камера, яка також непримітно розміщується на банкоматі. Потім досить швидко (буквально після першого зчитування даних з чужої карти) шахраї знімають накладки з банкомату і виготовляють дублікат карти, за допомогою якої знімають гроші з рахунку потерпілого.

Шахрайство з платіжними пластиковими картками, як серйозна проблема, постало у 90-і роки минулого століття і пов'язане з неправомірним використанням як кредитних, так і дебітних карток.

Найвідоміші компанії з випуску кредитних карток – Visa International і MasterCard International, причому Visa охоплює більшу частину існуючого ринку. Фінансові заклади, які є філіалами цих двох компаній, тільки в одній Канаді випустили майже 25 млн. кредитних карток, із яких 55475 штук вже були використані для вчинення шахрайських дій.

Найбільшу загрозу для системи платежів з використанням пластикових карток становить їх підробка. Ця форма шахрайства найдинамічніше розвивається і створює великі труднощі як при розслідуванні, так і при підрахунку збитків.

Підроблені картки досить легко транспортуються. Таким чином, немає географічного регіону, який вважався б захищеним від розповсюдження підробок. За даними Інтерполу, 42% підробних карток мають походження з Азіатсько – Тихоокеанського регіону, 36% – із країн Європи та 19% – із Північної Америки. Тому підробка кредитних карток – це глобальна проблема, яка не знає державних кордонів. Правоохоронні органи різних країн, навпаки, мають безліч юридичних перешкод, що ускладнюють їх роботу. Наприклад, кредитна інформація (дані про власників карток, стан їх рахунків, номери діючих карточок тощо) може бути зібрана злочинцями у Канаді, і надіслана до Європи чи кудись ще для подальшого використання. У той же час, така інформація може бути зібрана в Австралії, США чи Японії, після чого використана у Канаді. Підроблені картки, які були вироблені та використані в одній країні, можуть після цього швидко переправлятися і використовуватись в іншій

країні. Такий стан речей значно ускладнює роботу поліції, особливо, коли у злочинну діяльність втягнуто декілька злочинних угруповань, працюючих у різних країнах і навіть на різних континентах [11].

Скіммінг вчиняється за допомогою скімера – спеціального пристрою, який кріпиться до щілини банкомату, у яку вводиться картка, зчитує дані з магнітної стрічки картки, після чого виготовлення копії – справа кількох хвилин. PIN-код отримують за допомогою мініатюрної веб-камери, яка кріпиться над банкоматом або маскується під якийсь звичний предмет (блок з листівками тощо). Інший варіант – накладна клавіатура, яка зчитує PIN-код. В мережі Інтернет можна знайти пропозиції продажу скімера за $ 200. Необхідний зчитувач PIN-коду – накладка на клавіатуру або камера коштуватиме ще $ 3000. Комплект порожніх карток 500 штук – $30. Після цього можна іти грабувати наївних громадян. Скімери можуть бути різними: маленький пристрій або ціла накладна панель. Поліція Швеції зафіксувала випадки наклеювання цілої панелі поверх справжньої. Після цього правоохоронні органи рекомендують користувачам уважно шукати підозрілі елементи на банкоматах і навіть перевіряти цілісність за допомогою фізичної сили.

Ще одним способом шахрайства з використанням електронно-обчислювальної техніки є обман у мережі Інтернет, коли надсилають пропозиції такого типу: «Організації потрібні співробітники для обробки листів вдома, вік, стать значення не мають. Заробіток від 300 $. Важлива наявність комп'ютера та Інтернету. Заявки приймаються на e-mail». Після того, як особа відправляє заявку, їй надходить електронний лист, у якому пропонується зробити оплату за «матеріали», необхідні для роботи, або оплату за інструкції, або реєстраційний внесок, що підтверджує чесність намірів. Після оплати потерпілий отримує інструкцію, в якій написано, що треба робити теж саме, що і «працедавець», тобто давати оголошення про роботу вдома, заробіток в Інтернеті, обробку листів вдома, потім відповідати на запити, а після отримання грошей висилати таку ж «інструкцію». Ця схема до цих пір працює лише тому, що, фактично, ніхто не звертається до правоохоронних органів, оскільки потрібний час на розбирання, гроші, як правило, на це необхідні більші ніж віддані шахраям [12].

Шахрайство з використанням електронно-обчислювальної техніки можливе із залученням різних приладів, які впливають на електронно-обчислювальну техніку. Так, СБУ відкрила кримінальне провадження за фактом телефонного шахрайства з міжнародними дзвінками в Києві. За даними прес-служби СБУ співробітники Головного управління

[11] Комп'ютерне шахрайство. URL : http://www.e-sat.com.ua/shahrajstvo.html.

[12] Там само.

контррозвідувального захисту економіки СБУ одержали інформацію про незаконне втручання в маршрутизацію міжнародного й міжміського трафіку і його електронний облік. Спецслужба встановила, що в приміщенні одного з інститутів Національної академії наук встановлений прилад, за допомогою якого міжнародні дзвінки відображалися в комп'ютерній системі як міські. За даними прес-служби, таким чином співробітники інституту, які встановили цей прилад, порушили закон, що забороняє використання на комерційній основі кінцевого обладнання й абонентських ліній для надання послуг третім особам. В результаті такого порушення державний бюджет через несплату послуг одному з державних телекомунікаційних операторів втратив десятки тисяч доларів, тоді як зловмисники щомісяця одержували в результаті шахрайства до 200 тис. гривень[13].

Окремо хотілося розглянути використання мобільних телефонів при вчиненні шахрайства. Виникає питання, чи слід визнавати це використання як особливо кваліфікуючу ознаку шахрайства, передбачену ч. 3 ст. 190 КК, тобто як використання електронно-обчислювальної техніки. Наведемо приклади можливих шахрайських дій з використанням мобільних телефонів.

Одним з «найдієвіших» і сучасніших видів шахрайства можна визнати переказ грошових коштів з рахунку. Абоненти-потерпілі страждають, перш за все, через технічну необізнаність і неуважність. Так, користувач мобільного телефону отримує SMS-повідомлення про те, що хтось переказав на його рахунок певну суму грошей. Найчастіше вона невелика – 10-15 гривень. Через декілька хвилин приходить й інше SMS з повідомленням про помилку і проханням повернути гроші назад. Найчастіше такі повідомлення відправляються з офіційних сайтів операторів. У цьому випадку номер відправника не повідомляється, а замість нього на дисплеї адресата з'являється короткий номер, максимально схожий на службове повідомлення. Природно, грошей на рахунку абонента не додалося, а жалісліва історія про фатальну помилку під час передачі грошей другу – не більше ніж шахрайство. Утім, такий прийом якраз і розрахований на порядність людей, які захочуть повернути гроші неуважному абонентові.

Ще один вид шахрайства пов'язаний з розсилкою повідомлень про необхідність знайти рідкісну групу крові для порятунку дитини. У повідомленні вказується номер телефону, дзвінки на який автоматично знімають з рахунку людини, яка телефонувала, 20-30 гривень. Не рідкісні також SMS і дзвінки, які просто шокують одержувача: найчастіше в них

[13] Шахрайство з використанням електронно-обчислювальної техніки. URL: http://www.dp.ukrtelecom.ua/presscenter/news/official?id=39448

повідомляється, що близькі або друзі абонента потрапили в біду.

Самі по собі мобільні телефони, виходячи з проведеного вище аналізу поняття знаряддя шахрайства з використанням електронно-обчислювальної техніки, не відносяться до останньої. Саме тому, якщо шляхом використання мобільного телефону не відбувається втручання у комп'ютерні системи, останній не є знаряддям шахрайства, передбаченого ч. 3 ст. 190 КК. Тому шахрайство з використанням мобільного телефону слід кваліфікувати за іншими ознаками, передбаченими ст. 190 КК, не як шахрайство шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

Розділ 2
СПЕЦІАЛЬНО-КРИМІНОЛОГІЧНІ ЗАХОДИ ЗАПОБІГАННЯ КОМП'ЮТЕРНИМ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

Спеціально-кримінологічне запобігання – це сукупність заходів боротьби зі злочинністю, змістом яких є різноманітна робота державних органів, громадських організацій, соціальних груп і громадян, спрямована на усунення причин та умов, що породжують і сприяють злочинності, а також недопущення вчинення кримінальних правопорушень на різних стадіях кримінально-протиправної поведінки. Спеціально-кримінологічне запобігання кримінальним правопорушенням складається із трьох напрямів діяльності: кримінологічної профілактики; відвернення кримінальних правопорушень; припинення кримінальних правопорушень.

Засоби і методи криміналістичної техніки використовуються для припинення комп'ютерних кримінальних правопорушень, тобто є одними зі спеціально-кримінологічних заходів запобігання цієї категорії правопорушень. Розглянемо окремі з них.

Результати аналізу практичної діяльності правоохоронних органів щодо розслідування комп'ютерних кримінальних правопорушень свідчать, що дослідження комп'ютерної техніки доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою.

Докази, пов'язані з комп'ютерними кримінальними правопорушеннями, вилучені з місця події, можуть бути легко змінені, як у результаті помилок при їх вилученні, так і в процесі самого їх дослідження. Представлення таких доказів для використання у судовому процесі вимагають спеціальних знань і відповідної підготовки. Тут не можна недооцінювати роль експертизи, яка могла б дати кваліфікований висновок щодо поставлених у ході розслідування питань[14].

Однак експертиза вимагає деякого часу не тільки на її проведення, але і на пошук відповідних фахівців, а при вилученні комп'ютерної техніки часто важливим фактором, що дозволяє зберегти необхідну доказову інформацію, є раптовість та оперативність. Саме тому вилучення комп'ютерів та інформації доводиться проводити тими

[14] Голубєв В.О., Хряпінський П.В. Особливості проведення слідчих дій на початковому етапі розслідування комп'ютерних злочинів. URL : https://www.crime-research.ru/library/gol&hry.htm.

силами, які є на момент проведення слідчої дії. У цьому випадку слідчий не застрахований від помилок, обумовлених недостатністю знань, що пізніше може використовуватись стороною захисту у суді.

Поставлена проблема має два аспекти: загальні помилки, що допускаються працівниками правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних з комп'ютерами, і захист інформації, встановленої на комп'ютерах їх безпосередніми користувачами.

Як відомо виявлення, огляд і вилучення комп'ютерної інформації, як і самих комп'ютерів у ході слідчих дій можуть здійснюватися не тільки під час слідчого огляду, але й у процесі обшуку, тимчасовому доступі до речей і документів, слідчому експерименті.

Розглянемо деякі типові помилки, які часто вчиняються при проведенні слідчих дій що до комп'ютерної інформації або самих комп'ютерів. Можна виділити деякі правила роботи з комп'ютерами, вилученими при розслідуванні комп'ютерних кримінальних правопорушень, а також запропонувати загальні рекомендації, що можуть бути корисні при обробці комп'ютерних доказів, здобутих в операційних системах DOS чи Windows.

Помилкова робота з комп'ютером

Перше правило полягає в наступному: ніколи, за жодних умов не працювати на вилученому комп'ютері. Це правило припускає, що вилучений комп'ютер – насамперед об'єкт дослідження фахівців. Тому його бажано навіть не включати до передачі експертам, оскільки категорично заборонено виконувати будь-які програми на вилученому комп'ютері без вживання необхідних заходів безпеки (наприклад, захисту від модифікації або створення резервної копії). Якщо на комп'ютері встановлена система захисту на вході в нього (наприклад – пароль), то його включення може викликати знищення інформації, що знаходиться на жорсткому диску. Не допускається завантаження такого комп'ютера з використанням його власної операційної системи.

Такі заходи пояснюються досить просто: кримінальному правопорушнику не становить особливих труднощів встановити на своєму комп'ютері програму для знищення інформації на жорсткому магнітному диску, записавши такі «пастки» через модифікацію операційної системи. Наприклад, проста команда DIR, яка використовується для відображення каталогу диска, може легко бути змінена, щоб відформатувати жорсткий диск.

Після того як дані і сама руйнуюча програма знищені, ніхто не зможе вірогідно сказати, чи був «підозрюваний» комп'ютер спеціально

оснащений такими програмами, чи це результат недбалості при дослідженні комп'ютерних доказів.

Допуск до комп'ютера власника (користувача) комп'ютера

Серйозною помилкою є допуск до досліджуваного комп'ютера власника для допомоги при його експлуатації. У багатьох зарубіжних літературних джерелах описуються випадки, коли підозрюваному на допиті, пов'язаному з комп'ютерними доказами, було надано доступ до вилученого комп'ютера. Пізніше вони розповідали своїм знайомим, як шифрували файли «прямо під носом у поліцейських», а ті при цьому навіть не здогадувалися. Враховуючи таки наслідки, дуже швидко комп'ютерні фахівці стали робити резервні копії комп'ютерної інформації перш, ніж надавати доступ до них.

Інша проблема пов'язана з можливістю спростувати у суді ідентичність пред'явленого в судовому процесі програмного забезпечення тому, що знаходилося в даному комп'ютері на момент вилучення. Щоб уникнути таких ситуацій комп'ютер необхідно опечатати у присутності понятих без його включення. Якщо ж працівник правоохоронних органів приймає рішення оглянути комп'ютер на місці, перше, що варто зробити, це зняти копію з жорсткого магнітного диску та інших електронних носіїв інформації (USB-флеш-накопичувачі тощо), що будуть вилучатись як речовий доказ. Це означає, що до проведення будь-яких операцій з комп'ютером необхідно зафіксувати його стан на момент проведення слідчих дій.

Відсутність перевірки комп'ютера на наявність вірусів і програмних закладок

Для перевірки комп'ютера на наявність вірусів і програмних закладок необхідне завантаження комп'ютера не з операційною системи, яка знаходиться на ньому, а зі свого, заздалегідь підготовленого, електронного пристрою. Перевірці підлягають усі носії інформації – жорсткий диск та інші носії інформації. Цю роботу варто робити залученому для участі в слідчих діях фахівцю за допомогою спеціального програмного забезпечення.

У іншому випадку у ході судового розгляду справи з'явиться можливість обвинуватити працівників правоохоронних органів у навмисному зараженні комп'ютера вірусами, чи у некомпетентності при проведенні слідчих дій або просто у недбалості, оскільки довести, що вірус був у комп'ютері до початку дослідження навряд чи можливо, а

подібне обвинувачення поставить під сумніви всю працю експерта та вірогідність його висновків й надасть підстави для визнання цих доказів недопустимими.

Наведені типові помилки, що зустрічаються при дослідженні комп'ютера у справах, пов'язаних з розслідуванням комп'ютерних кримінальних правопорушень. Однак цей перелік не охоплює всіх помилок, що виникають у процесі вилучення і дослідження комп'ютерної інформації.

Для запобігання помилок при проведенні слідчих дій на початковому етапі розслідування, які можуть призвести до втрати чи руйнування комп'ютерної інформації, потрібно дотримуватись деяких запобіжних заходів:

5. Спочатку слід виконати резервне копіювання інформації.

При вилученні комп'ютера, магнітних носіїв та інформації виникає ряд загальних проблем, пов'язаних зі специфікою технічних засобів, що вилучаються. Так, необхідно передбачати заходи безпеки, що здійснюються злочинцями з метою знищення комп'ютерної інформації. Наприклад, вони можуть використати спеціальне обладнання, яке у критичних випадках утворює сильне магнітне поле, що стирає магнітні записи.

Протягом проведення відповідної слідчої дії усі електронні докази, які знаходяться у комп'ютері чи комп'ютерній системі, повинні бути зібрані таким чином, щоб у подальшому їх визнали допустимими доказами. Світова практика свідчить, що у великій кількості випадків під тиском представників захисту у суді електронні докази не приймаються до уваги. Для того, щоб гарантувати їх визнання у якості доказів, необхідно суворо дотримуватися вимог кримінального процесуального законодавства, а також стандартизованих прийомів та методик їх вилучення.

Звичайно комп'ютерні докази зберігаються шляхом створення точної копії з оригіналу (первісного доказу), перш ніж виконується будь-який їх аналіз. Але робити копії комп'ютерних файлів, використовуючи тільки стандартні програми резервного копіювання, недостатньо. Речові докази можуть існувати у формі знищених або прихованих файлів, а дані, пов'язані з цими файлами, можна зберегти тільки за допомогою спеціального програмного забезпечення (у найпростішому виді це можуть бути програми типу SafeBack).

Магнітні носії, на які передбачається копіювати інформацію, повинні бути заздалегідь підготовлені (необхідно впевнитись, що на них немає ніякої інформації). Носії потрібно зберігати у спеціальних упаковках або загортати у чистий папір. Слід пам'ятати, що інформація може бути зіпсована вологістю, температурним впливом або електростатичними (магнітними) полями.

5. Знайти і виконати копіювання тимчасових файлів.

Багато текстових редакторів і програм управління базами даних створюють тимчасові файли як побічний продукт нормальної роботи програмного забезпечення. Більшість користувачів комп'ютера не усвідомить важливості створення цих файлів, тому що вони звичайно знищуються програмою наприкінці сеансу роботи. Однак дані, що містяться усередині цих знищених файлів, можуть виявитися найбільш корисними. Особливо якщо вихідний файл був шифрований чи документ підготовки текстів був надрукований, але ніколи не зберігався на диску, такі файли можуть бути відновлені.

5. Обов'язковість перевірки Swap File.

Swap File працюють як дискова пам'ять або величезна база даних, і багато різних тимчасових фрагментів інформації, або навіть весь текст документу може бути знайдено у цьому Swap файлі.

4. Необхідно порівнювати дублі текстових документів.

Часто дублі текстових файлів можна знайти на жорсткому магнітному диску. Це можуть бути незначні зміни між версіями одного документу, які можуть мати доказову цінність. Ці розходження можна легко ідентифікувати за допомогою найбільш сучасних текстових редакторів.

Приступаючи до огляду комп'ютера, слідчий і фахівець, що безпосередньо робить усі дії на ЕОМ, повинні дотримуватись наступних правил:

– перед вимиканням комп'ютера потрібно по можливості закрити усі використовувані програми. Треба пам'ятати, що некоректний вихід з деяких програм може викликати знищення інформації або зіпсувати саму програму;

– необхідно прийняти заходи щодо встановлення пароля доступу у захищені програми;

– при активному втручанні співробітників підприємства, які намагаються протидіяти слідчій групі, потрібно відключити електроживлення всіх комп'ютерів на об'єкті, опечатати їх і вилучити разом з магнітними носіями для дослідження інформації у лабораторних умовах;

– при необхідності консультацій у персоналу підприємства, варто одержувати їх у різних осіб шляхом опитування чи допиту. Такий метод дозволить одержати максимально правдиву інформацію та уникнути умисної шкоди;

– при вилученні технічних засобів доцільно вилучати не тільки системні блоки, але й додаткові периферійні пристрої (принтери, стрімери, модеми, сканери тощо);

– за наявності локальної обчислювальної мережі необхідно мати

потрібну кількість фахівців для додаткового дослідження інформаційної мережі;

– вилучати усі комп'ютери (системні блоки) і магнітні носії;

– потрібен ретельний огляд документації, звертаючи особливу увагу на робочі записи операторів ЕОМ, тому що часто саме в цих записах недосвідчених користувачів можна знайти коди, паролі й іншу дуже корисну інформацію;

– варто скласти список усіх позаштатних і тимчасово працюючих фахівців організації (підприємства) з метою виявлення програмістів та інших фахівців галузі інформаційних технологій, що працюють у даній установі. Бажано установити їх паспортні дані, адреси і місце постійної роботи;

– потрібно записати дані всіх людей, що знаходяться у приміщенні в момент приходу слідчої групи, незалежно від пояснення причини перебування їх у даному; приміщенні;

– варто скласти список усіх співробітників підприємства, що мають доступ до комп'ютерної техніки або часто перебувають у приміщення, де знаходяться ЕОМ.

Якщо безпосередній доступ до комп'ютера можливий і всі небажані ситуації виключені, приступають до огляду, причому слідчий і фахівець повинні чітко пояснювати всі свої дії понятим.

При огляді повинні бути встановлені:

– конфігурація комп'ютера з чітким описом усіх пристроїв;

– номера моделей і серійні номери кожного з пристроїв;

– інвентарні номери, що привласнюються бухгалтерією при постановці обладнання на баланс підприємства;

– інша інформація з фабричних ярликів (на клавіатурі ярлик звичайно знаходиться на зворотній стороні, а на моніторі і процесорі – на задній). Така інформація, заноситься до протоколу огляду обчислювальної техніки і може виявитися важливої для слідства.

5. Треба перевірити і проаналізувати роботу комп'ютерної мережі.

Комп'ютери можуть бути зв'язані між собою у комп'ютерну мережу (наприклад, локальну), які, в свою чергу, можуть бути з'єднані через глобальні комп'ютерні мережі (Internet). Тому не виключена ситуація, коли певна інформація (яка може бути використана як доказ) буде передана через мережу в інше місце. Не виключений також випадок, що це місце буде знаходитись за кордоном або на території декількох країн. В такому разі необхідно використати всі можливості (документацію, опитування, технічні можливості системи) для встановлення місцезнаходження іншої комп'ютерної системи, куди була передана інформація. Як тільки це буде зроблено, необхідно

терміново надіслати запит, з виконанням встановлених вимог, про надання допомоги (або правової допомоги, якщо така необхідна для виконання поставлених у запиті питань) у компетентний правоохоронний орган відповідної країни (по встановленим офіційним каналам, наприклад, Інтерпол). Саме на цьому етапі виникають найбільші труднощі в організації роботи щодо розслідування злочину, який вчиняється за допомогою комп'ютерних технологій та кримінального переслідування злочинців.

Будь-які дії, пов'язані з розслідуванням кримінальних правопорушень у сфері використання комп'ютерних технологій (особливо вилучення інформації і комп'ютерного обладнання), доцільно з самого початку залучення фахівця у галузі інформаційних технологій. До початку слідчих дій необхідно також мати певну інформацію щодо: марки, моделі комп'ютеру, операційної системи, периферійних пристроїв, засобів зв'язку та будь-які інші відомості про систему, яка є об'єктом розслідування[15].

Практика показує, що розслідування кримінальних проваджень щодо кримінальних правопорушень, вчинених з використанням комп'ютерних технологій, представляє значні труднощі. У цій області криміналістичної техніки, яка перетинається з областю захисту інформації, завжди буде існувати розрив між розвитком способів вчинення цих кримінальних правопорушень і здатністю методів і засобів захисту інформації, а також методики розслідування цієї категорії проваджень виконувати свої функцій.

Цей розрив обумовлений декількома причинами. Способи вчинення кримінально-протиправних дій динамічно розвиваються у двох напрямках: по-перше, удосконалюються вже існуючі методи, а по-друге, з'являються нові. Засоби комп'ютерної техніки цікаві зловмисникам своєю ефективністю – малими витратами у порівнянні з великими можливостями. Яскравим тому свідченням можуть бути щоденні звіти організацій, які фіксують появу вірусів та інших шкідливих програм, виявлення нових недоліків програмного забезпечення, що використовуються для вчинення кримінальних правопорушень і т.п.

Що стосується правоохоронної діяльності, то її розвиток сповільнюється різними факторами, перший з яких – недостатнє матеріально-технічне забезпечення системи. У перспективі, на наш погляд, подібного роду ситуація збережеться у силу того, що для виявлення, аналізу та розробки відповідних заходів щодо запобігання потрібні значні часові витрати, що обмежує швидкість реакцій системи

[15] Голубєв В.О., Хряпінський П.В. Зазнач. твір.

на умови навколишнього середовища, які змінюються.

Зазначене обумовлює труднощі не тільки у виявленні криміналістично значимої інформації, а й у її фіксації, вилученні та дослідженні.

Умовою успішного розкриття і розслідування таких кримінальних правопорушень, їх судового розгляду є в першу чергу ефективне збирання та дослідження комп'ютерної інформації, яка містить сліди кримінального правопорушення. Ця діяльність неможлива без використання спеціальних знань.

Існує ряд як теоретичних, так і практичних проблем, особливо в питаннях застосування спеціальних знань при проведенні слідчих дій. Найчастіше ці проблеми пов'язані організацією роботи зі слідами кримінальних правопорушень, які зберігаються на носіях інформації засобів комп'ютерної техніки.

Спеціальні знання – це наукові, технічні та інші професійні знання, набуті у результаті навчання, а також навички, здобуті в процесі роботи у певних сферах практичної діяльності, які використовуються разом з науково-технічними засобами при пошуку, фіксації та дослідженні слідів кримінального правопорушення з метою отримання доказової інформації, необхідної для встановлення істини у кримінальному провадженні.

Спеціальні знання під час розслідування комп'ютерних кримінальних правопорушень становлять відомості з таких областей знань, як електроніка, електротехніка, інформаційні системи і процеси, радіотехніка і зв'язок, обчислювальна техніка (зокрема, програмування) і автоматизація виробництва.

Форми використання спеціальних пізнань класифікуються за різними підставами. Залежно від доказового значення спеціальні пізнання поділяються на дві основні форми – процесуальну і непроцесуальну. Процесуальні форми використання спеціальних знань можуть бути диференційовані на обов'язкові і факультативні у разі їх використання при проведенні процесуальних дій. Крім того, процесуальні форми використання спеціальних знань поділяються за характером дій, при проведенні яких вони застосовуються, на слідчі та інші процесуальні дії. Непроцесуальні форми використання спеціальних знань можуть бути поділені за ознакою сфери та суб'єкта їх використання.

Кримінальне процесуальне законодавство пов'язує використання спеціальних знань і навичок у вирішенні питань, які виникають у ході розслідування, перш за все при призначенні експертизи, а також у разі залучення спеціаліста при проведенні слідчих дій.

Щодо суб'єкта доказування (слідчого, прокурора, суду) можливі дві

форми використання, спеціальних знань: безпосередня та опосередкована.

Оскільки рівень знань слідчих, прокурорів і суддів у зазначених вище областях недостатній в силу складності комп'ютерних технологій і різноманітності спеціальних знань в цій області, слід зробити висновок, що суб'єктами застосування спеціальних знань при розслідуванні комп'ютерних кримінальних правопорушень в основному є фахівець та експерт, а суб'єкт доказування лише опосередковано бере участь у цьому.

Крім того, немає такої процесуальної форми застосування спеціальних знань, як самостійне використання їх слідчим. Всі спеціальні пізнання у кримінальному судочинстві використовуються за допомогою обізнаних осіб.

Форма використання спеціальних знань суб'єктом доказування визначається:

– процесуальним становищем обізнаної особи (експерт, спеціаліст і т. п.);

– метою застосування (пошук, виявлення, вилучення, дослідження слідів кримінального правопорушення);

– значенням (доказове або орієнтуюче) отриманих результатів.

У виборі форми застосування спеціальних знань у процесі доказування пріоритетним, безумовно, є процесуальне значення результатів їх використання.

Під час розслідування комп'ютерних кримінальних правопорушень спеціальні знання застосовуються в обох формах.

Спеціаліст як процесуальна фігура бере участь у проведенні слідчих дій, і тоді його допомога і її результати фіксуються у протоколі і набувають значення доказу. При проведенні перевірочних і попередніх досліджень та надання консультаційної допомоги результати його допомоги мають значення для відкриття кримінального провадження і ходу розслідування, але не є доказами.

Залучення фахівця – право слідчого, а не обов'язок. Винятками є слідчі дії, під час проведення яких законом обов'язково визначена участь спеціалістів конкретного профілю. Список таких слідчих дій вичерпний, і в законі немає вказівки на обов'язковість залучення фахівця при роботі із засобами комп'ютерної техніки: проте, щодо розслідування комп'ютерних кримінальних правопорушень однозначно існує необхідність залучення фахівця під час проведення слідчих дій.

Серед дослідників проблем комп'ютерної злочинності немає однозначної думки з приводу відмежування компетенції спеціаліста від компетенції експерта при роботі з комп'ютерними доказами. Одні

припускають можливість втручання у роботу комп'ютерної техніки та комп'ютерну інформацію на місці події. Інші припускають тільки вилучення комп'ютерної техніки та носіїв комп'ютерної інформації з подальшим призначенням експертизи, оскільки будь-які дослідницькі дії на місці можуть випадково внести зміни до носія слідової інформації, а тому вважають неприйнятними будь-які інші операції в ході проведення слідчої дії.

Останні пропонують обмежити функції спеціаліста збиранням носіїв доказів і здійсненням довідково-консультаційної діяльності та визнати в якості одного з основних процесуальних способів отримання доказів у цій категорії справ судову експертизу засобів комп'ютерної техніки, документів та іншої інформації на машинних магнітних носіях.

Проте таке обмеження дій спеціаліста на наш погляд, має і зворотній бік.

По-перше, на фіксацію, вилучення засобів комп'ютерної техніки, призначення та проведення експертизи потрібен час (в НДЕКЦ експертиза проводиться протягом 15 днів, а складні дослідження – протягом місяця). Цього цілком вистачить зловмисникам, щоб знищити всі інші сліди і зникнути. Тому доцільно розслідувати такі кримінальні правопорушення по гарячих слідах.

Окрім того, сліди в одному комп'ютерному засобі можуть вказати на інші носії слідів цього ж кримінального правопорушення, що відразу слід оглядати та фіксувати. Найчастіше це відбувається у разі вчинення кримінального правопорушення в мережі. Наприклад, під час поширення порнографії на носії комп'ютерної інформації можуть знаходитись не лише самі порнографічні матеріали, що будуть фактичною підставою для відкриття кримінального провадження, але й інформація про канал збуту цього матеріалу (адреси сайтів, номери телефонів провайдерів, відомості про розповсюджувачів і т.п.), яку негайно потрібно використовувати, оскільки часу на знищення компрометуючої комп'ютерної інформації, закриття сайту і знищення інших слідів злочинцям потрібно дуже мало.

По-друге, часто немає очевидних підстав для відкриття кримінального провадження. Достатні дані у більшості випадків вчинення кримінального правопорушення можуть з'явитися тільки після виявлення слідів у комп'ютерній техніці, а тому почати розслідування та призначити експертизу неможливо.

Не забороненим законом способом подолання цієї проблеми є проведення попередніх досліджень.

До методів, що використовуються під час перевірочних та попередніх досліджень, висуваються більш суворі вимоги, пов'язані з необхідністю збереження властивостей та параметрів об'єктів для їх

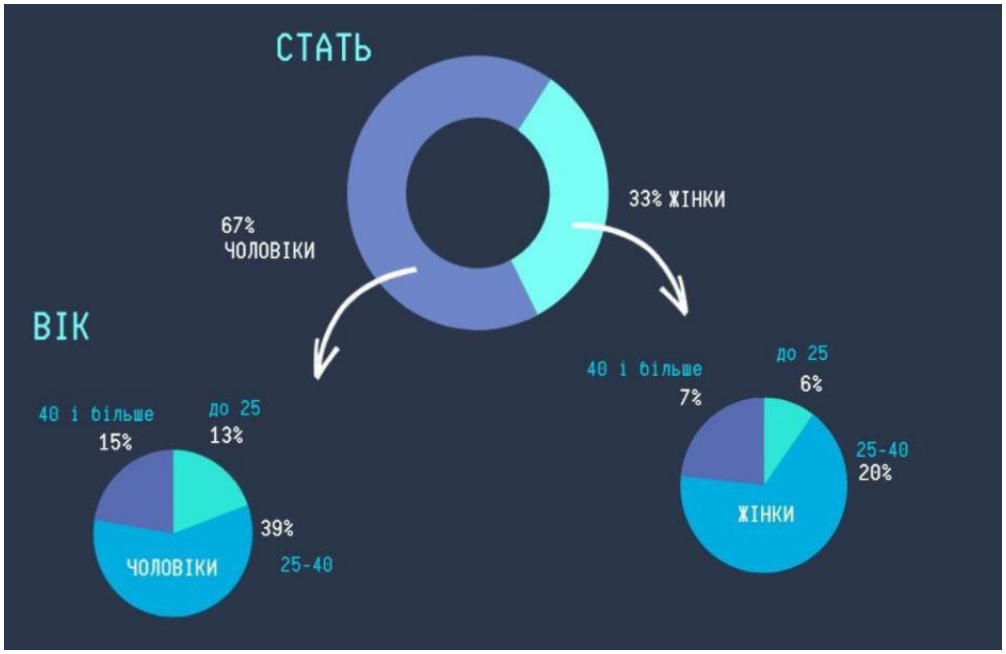
подальшого експертного дослідження.

Дотримання цієї вимоги також є проблемою. У розпорядженні експертних підрозділів відсутні в достатній кількості науково розроблені, затверджені та сертифіковані методики й техніко-криміналістичні засоби (особливо програмні) збирання та дослідження слідів кримінальних правопорушень на носіях комп'ютерної інформації, що відповідали б загальним вимогам до методів і засобів проведення судових досліджень.

ДОДАТКИ

Додаток 1

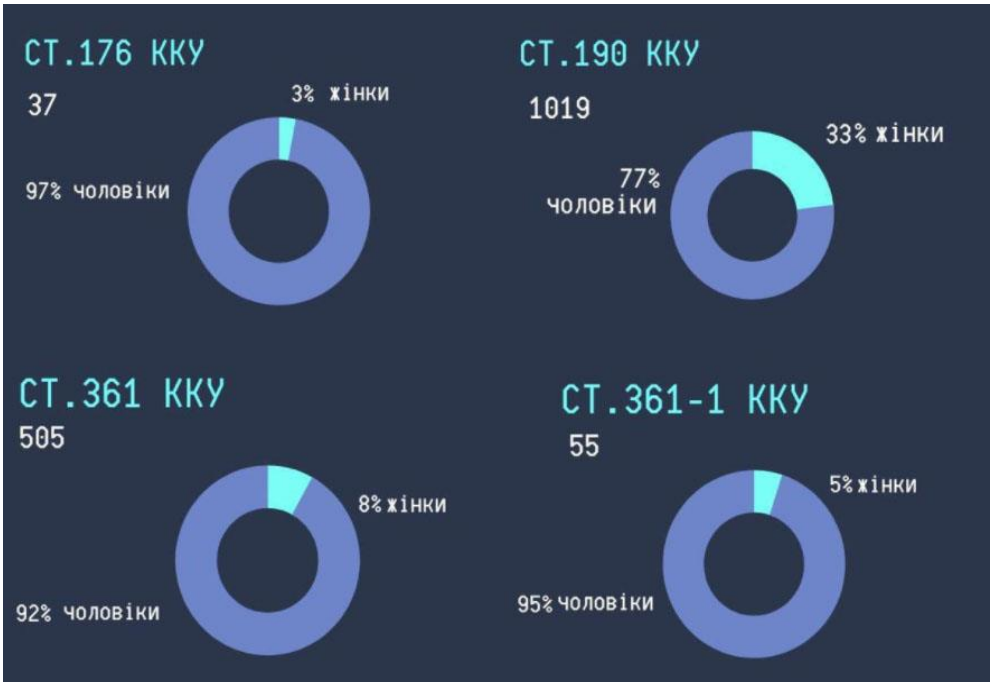
ОЗНАКИ ОСОБИ КІБЕРЗЛОЧИНЦЯ (за статтю та віком)



За даними кіберполіції (див. URL: https://cyberpolice.gov.ua/results/2018/)

Додаток 2

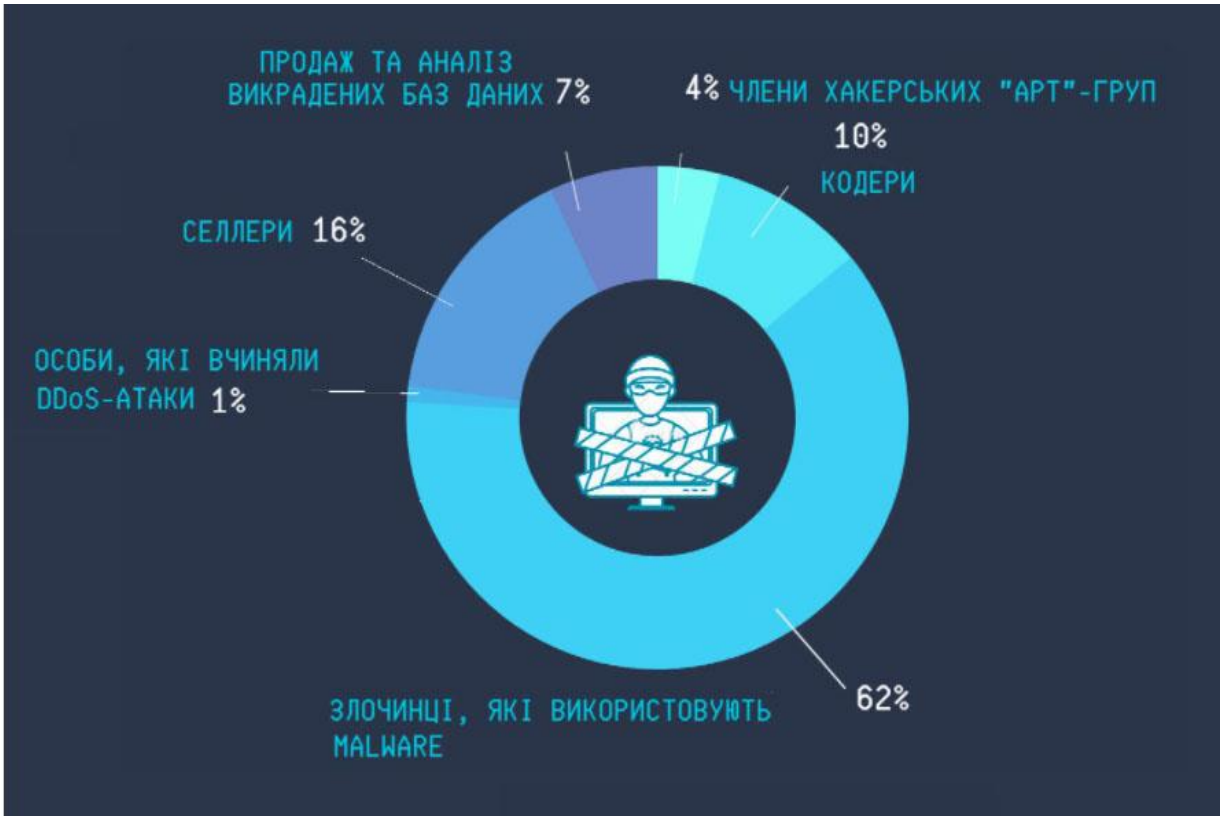
ОЗНАКИ ОСОБИ КІБЕРЗЛОЧИНЦЯ (за статтю та видом кримінальних правопорушень)



За даними кіберполіції (див. URL: https://cyberpolice.gov.ua/results/2018/)

Додаток 3

ОЗНАКИ ОСОБИ КІБЕРЗЛОЧИНЦЯ
(за способом вчинення кримінальних правопорушень)



За даними кіберполіції (див. URL: https://cyberpolice.gov.ua/results/2018/)

Додаток 4

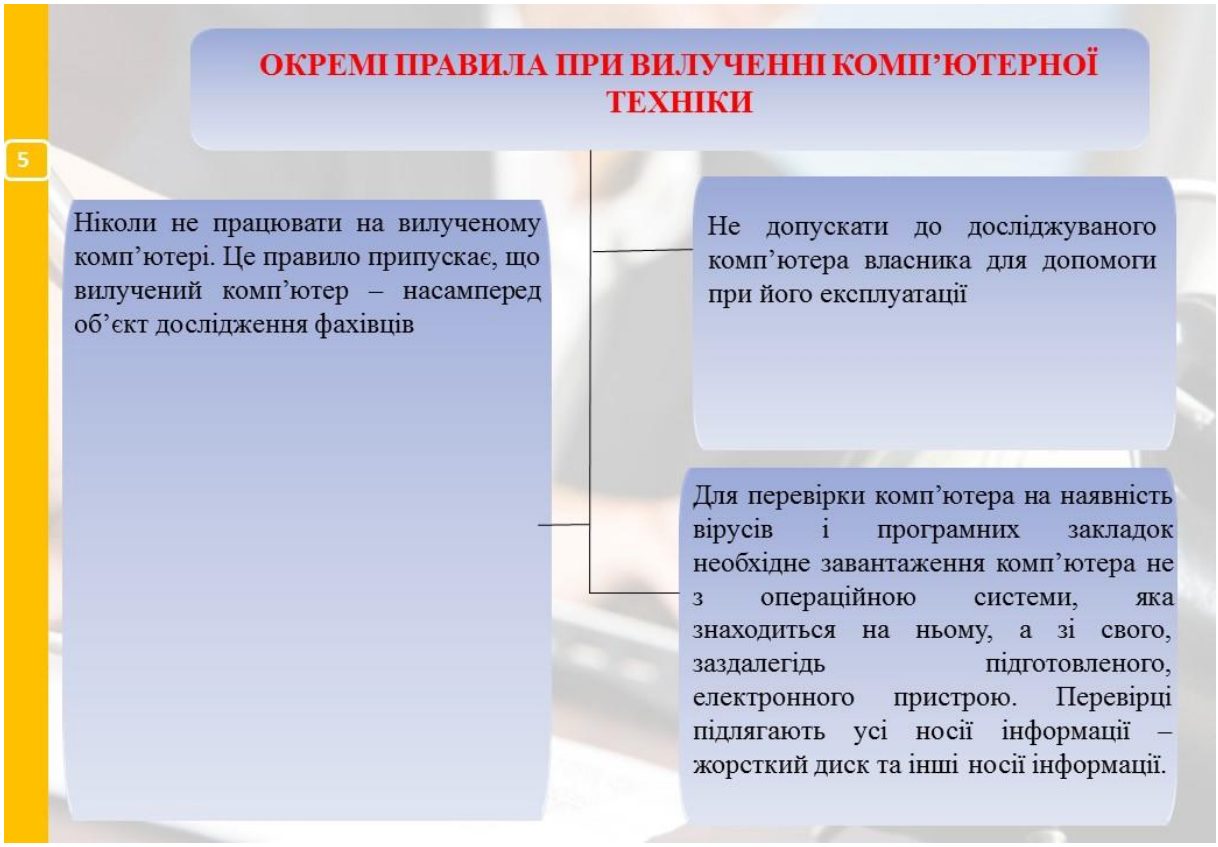
СТРУКТУРА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ (2020 РІК)

За даними кіберполіції

Додаток 5

МОЖЛИВІ СПОСОБИ ВЧИНЕННЯ КОМП'ЮТЕРНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Додаток 6



Додаток 7

Додаток 8

Додаток 9

ЗАВДАННЯ ТА ОРІЄНТОВНИЙ ПЕРЕЛІК ПИТАНЬ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

1

Основні завдання:

- установлення робочого стану комп'ютерно-технічних засобів;
- установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;
- виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;
- установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

1

Орієнтовний перелік питань:

Чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить) і у якому вигляді?

Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача?

Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?

Чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія?

Яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)?

Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)?

Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст)?

Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме - встановлене, не встановлене) програмне забезпечення?

Які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

Чи можливо виконання певних дій за допомогою даного програмного продукту?

Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Наукове видання

Бабанін Сергій Володимирович

ЗАПОБІГАННЯ КОМП'ЮТЕРНИМ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

Науково-практичний посібник

Редактори, оригінал-макет –
Є. В. Коваленко-Марченкова, А. В. Самотуга
Редактор *О.І. Галушко*

Підп. до друку 17.05.2022. Формат 60х84/16. Друк – цифровий. Гарнітура – Times.
Ум.-друк. арк. 3,25. Обл.-вид. арк. 3.40. Тираж – 30 прим. Зам. № 7/22-нп

Дніпропетровський державний університет внутрішніх справ
49005, м. Дніпропетровськ, просп. Гагаріна, 26, rvv_vonr@dduvs.in.ua
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018