Юридичний вісник. 2013. № 2 (27). С. 156-160.

2. Лобойко Л.М. Методи кримінально-процесуального права: монографія. Дніпропетровськ: Дніпропетр. держ. ун-т. внутр. справ, 2006. 352 с. С. 38-39.

3. Гурдин С.В. Обеспечения прав участников уголовного процесса при производстве следственных действий. *Вестник зкономической безопасности*. 2016. № 5. С. 76-78.

4. Гловюк І.В. Стаття 233 КПК України: питання практичної реалізації. *Молодий вчений*. 2015. № 2 (17). С. 216-218.

5. Вегера-Іжевська І.В. Забезпечення права на недоторканність житла чи іншого володіння особи в кримінальному провадженні: автореф. дис. … канд. юрид. наук. Харків, 2018. 22 с.

УДК 343.9(043.2)

Дрозд В.П., студентка,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Грекова Л.Ю., асистент

СПОСОБИ СКОЄННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

У XXI сторіччі, незважаючи на зручність і швидкість сучасних засобів зв'язку, використання інформаційних технологій викликало новий вид злочинів, які в цілому можна окреслити як комп'ютерні злочини. Проте слід зазначити, що кіберзлочинність не обмежується рамками злочинів вчинених у мережі Інтернет, вона поширюється на всі інші різновиди злочинів, вчинені в інформаційно-телекомунікаційній сфері, де інформація може виступати предметом посягань, засобом або знаряддям злочину.

Дане питання є важливим і на державному рівні, адже часто під ударами кібератак опиняються об'єкти критичної інфраструктури: транспорт, банківський сектор тощо. На жаль, сьогодні законодавство України є недосконалим у сфері боротьби із кіберзлочинами.

Проблему скоєння злочинів за допомогою комп'ютерів, їх способи досліджували та вивчали такі українські та зарубіжні вчені, як: В.Д. Куришина, Ю.М. Батурін, І.З. Карась, В.П. Бахін, М.В. Гуцалюк, К.В. Тітуніва та інші.

Відповідно до Конвенції про кіберзлочинність, яка імплементована українським законодавством з 11.10.2005 р., та Протоколом до неї, кіберзлочини умовно поділяються на п'ять видів: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; пов'язані з комп'ютерами; пов'язані зі змістом та порушенням авторських та суміжних прав, а також поширення расистського та ксенофобного матеріалу через комп'ютерні системи [2, с. 2-10]. Зрозуміло, що з часу ратифікації Конвенції пройшло чимало часу, кіберзлочинність набувала

нових форм, внаслідок чого з'явилися нові види злочинів, вчинених в інформаційному просторі Інтернет.

Сучасні дослідники, які вивчають дану проблему, пропонують поділяти кіберзлочини на види залежно від об'єкта та предмета злочинного посягання. Зокрема, О.Ю. Довженко, пропонує наступну класифікацію: злочини проти конституційних прав і свобод, такі як порушення недоторканності житла, таємниці листування; злочини проти честі та гідності особи (розповсюдження наклепницької інформації); злочини проти власності (Інтернет-шахрайство); злочини у сфері комп'ютерної інформації (неправомірний доступ та створення шкідливих програм); злочини проти суспільної моральності (розповсюдження аморальної продукції); злочини проти безпеки держави (нелегальний доступ до державної таємниці); кібертероризм [1, с. 9].

У спеціальній літературі також зазначається, що найпоширенішими видами таких злочинів є: кардинг; фішинг; вішинг; онлайн-шахрайство; піратство; кард-шарінг; соціальна інженерія; рефайлінг; протиправний контент та мальваре [3].

Зважаючи на величезний спектр кіберзлочинів, існує чимало способів їх здійснення. Під способом вчинення злочину розуміють систему поведінки суб'єкта до, в момент і після вчинення злочину, що залишає різного роду характерні сліди, за допомогою яких можна отримати уявлення про суть події та дані про злочинця. Сьогодні немає чіткої класифікації способів здійснення даних злочинів, оскільки доктринальні підходи до її розуміння є різними [4, с. 113]. Узагальнивши, можемо виокремити й описати деякі з них.

Перша група способів – вилучення засобів комп'ютерної техніки. Це так званий некомп'ютерний вид злочину, де електронно-обчислювана машина виступає лише як предмет злочинного посягання (крадіжка чужого майна).

До другої групи можемо віднести способи отримання інформації шляхом перехоплення. Із безпосереднім перехопленням стикаємось, коли злочинець, намагаючись отримати паролі чи будь-яку секретну інформацію, підключається до кабелю. Негативне перехоплення полягає у тому, що при використанні багатьох засобів комп'ютерної техніки виділяється випромінювання, яке у подальшому фіксує та зберігає особа. Що стосується відео- та ауді перехоплення - такі злочини вчиняються із використанням усім відомих «жучків», «таблеток» (різновидів прослуховуючих апаратів), відеооптичної техінки тощо.

Існує спосіб «прибирання сміття», за якого злочинець використовує технічні відходи інформаційного процесу, що залишені користувачем після роботи з комп'ютерною технікою [4, с. 117].

Спроби вивчення і систематизації способів учинення таких видів злочинів були проведені ще наприкінці минулого століття. Поміж безлічі

способів вчинення комп'ютерних злочинів, приміром, Ю.М. Батурін у 1991 році виокремлює наступні, зокрема, пов'язані з отриманням несанкціонованого доступу до чужих обчислюваних машин: 1) спосіб «за хвіст» - законний користувач працює у звичайному режимі, не підозрюючи про те, що у цей самий час злочинець підключається до лінії зв'язку та чекає сигналу, що означає кінець користування системою. Після цього здійснює автоматично доступ до неї; 2) спосіб «за дурнем» - цей спосіб використовується злочинцем шляхом підключення комп'ютерного терміналу до каналу зв'язку через комунікаційну апаратуру в той момент часу, коли працівник, відповідальний за роботу засоби комп'ютерної техніки, короткочасно залишає своє робоче місце, залишаючи термінал в активному режимі; 3) спосіб «комп'ютерний абордаж» - випадковий перебір абонентського номеру; 4) спосіб «неспішний вибір» - метод, який поширений серед хакерів, які шукають уразливі місця системи та використовують її у своїх цілях (наприклад, купівля, обмін на просторах Інтернету); 5) спосіб «маскарад» - злочинець видає себе за законного користувача. При цьому способі найбільш страждають ті дані та системи, які не мають автентифікації користувача.

Крім того, Ю.М Батурін, керуючись тим, що в якості основної ознаки систематизації способів виступає дія злочинця, спрямована на отримання доступу до засобів комп'ютерної техніки, виділяв ще одну групу способів, пов'язаних із злочинами щодо маніпуляції даних: підміна даних чи коду; незаконне введення програм, які виконують незаплановані дії; впровадження вірусів чи тимчасових атак; неправомірне отримання й використання власних облікових даних на чужих електронних приладах; копіювання програм з подоланням засобів захисту, який передбачає незаконне створення копії ключової дискети, модифікацію коду системи захисту, моделювання звернення до ключової дискети, зняття системи захисту з пам'яті ЕОМ [5, с. 116].

Отже, можна зробити висновок, що комп'ютерні злочини охоплюють ті дії суб'єктів їх вчинення, у яких комп'ютер є безпосередньо знаряддям злочину (розтрата, саботаж, шпигунство), та ті, які пов'язані з незаконним втручанням та проникненням у чужі системи. Способів та методів досягнення цих цілей безліч. На жаль, у руках комп'ютерних злочинців сьогодні забагато можливостей – фінансових, організаційних, технічних. А оскільки комп'ютерні злочини мають характер латентності, то можливо вже існують й інші способи їх вчинення, які ще невідомі та не виявлені правоохоронними органами.

Таким чином, із розвитком комп'ютерних технологій розвиваються й способи вчинення комп'ютерних злочинів. Потрібно прикладати чимало зусиль, вдосконалювати законодавчу базу та проводити профілактичні заходи для запобігання проявам даних злочинів.

Література

1. Довженко О.Ю. Класифікація кіберзлочинів у криміналістиці. Протидія злочинності: проблеми практики та науково-методичне забезпечення. 2019. С. 22.
2. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 28.03.2020).
3. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення 01.04.2020).
4. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дисс. … канд. юрид. наук: 12.00.12. Волгоградский государственный университет, 2008. 233 с.
5. Батурин Ю.М. Проблемы компьютерного права. Москва: Юрид. лит., 1991. С. 116.

УДК 344.65(043.2)

Дроншкевич Є. О., студентка,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Ландецова Ю. О., к.ю.н., доцент

СУД ПРИСЯЖНИХ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стаття 5 Конституції України закріплює, що єдиним джерелом влади в Україні є народ [1]. Дія цієї конституційної норми відображається і стосовно гілки судової влади, а саме в участі народу у здійсненні правосуддя у кримінальному провадженні у формі суду присяжних відповідно до статті 127 Конституції України та статті 5 Закону України «Про судоустрій і статус суддів». Особливості статусу присяжного визначаються Главою 3 Закону України «Про судоустрій і статус суддів» [2].

Слід звернути увагу на факт того, що інститут присяжних у кримінальному провадженні України не відповідає класичній моделі лави присяжних. Присяжні здійснюють свою діяльність нарівні з суддями, які, на відміну від присяжних, мають вищу юридичну освіту, здійснюючи правосуддя на професійній основі. Згідно зі статтею 384 Кримінального процесуального кодексу України право на розгляд справи у суді присяжних передбачено лише для обвинувачених у вчиненні злочину, за який передбачено покарання у виді довічного позбавлення волі [3]. Виходячи з цього, постає питання, чи дійсно достатньо цих вимог до присяжних для кваліфікації та оцінки діяння, що містить ознаки особливо тяжкого злочину.

Науковці мають різний погляд на цей аспект. І.В. Юревич