Розслідування кіберзлочинів: окремі аспекти діяльності прокурора і слідчих органів внутрішніх справ

Рогатюк І.В., кандидат юридичних наук, доцент, заслужений юрист України

За останні два десятиріччя людство здійснило величезний стрибок в галузі інформаційних технологій які глибоко вкоренилися в повсякденне життя суспільства. Переважна більшість людей вже не уявляє своє життя без різноманітних надбань науково-технічного прогресу, а всесвітня мережа Інтернет стала для багатьох основним засобом навчання, спілкування та навіть ділової активності. Однак правопорушники так само поступово розпочали використовувати інформаційно-технічний прогрес у свої власних злочинних цілях і сьогодні ми зустрічаємося з цілою низкою злочинів, що поступово трансформувалися і стали здійснюватися вже не в реальному світі, а у віртуальній мережі.

За даними МВС України упродовж 2012 року правоохоронцями до Єдиного реєстру досудових розслідувань було внесено відомості про 2 тисячі злочинів, учинених із використанням високих технологій. У першому півріччі 2013 року до ЄРДР внесено майже 1,9 тисячі заяв та повідомлень про такі злочини, а їхнє розкриття становить близько 50 відсотків.

Порівнюючи кіберзлочини з традиційними видами злочинів, слід зазначити, що кількість їх вчинення за останні роки збільшилася вдвічі. Разом з цим, відповідно до статистичних даних переважна більшість кіберзлочинів учиняються організованими злочинними групами та мають економічну мотивацію.

До кіберзлочинів відносять: розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем - і це далеко не повний перелік подібних злочинів.

Розслідування злочинів, учинених у сфері інформаційних технологій, ускладнюються тим, що органам розслідування важко виявити та зафіксувати сліди, які залишаються після вчинення комп’ютерного злочину, оскільки досвідчений «хакер» залишає за собою їх невелику кількість. Щоб його вирахувати і затримати, потрібна допомога провайдерів і обмін технічною інформацією з їх

закордонними партнерами та міжнародними правоохоронними органами.

Криміналістична особливість кіберзлочинів характеризується тим, що виявлення та розслідування цих злочинів неможливе без застосування та використання комп'ютерних технологій. Це пов'язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі.

Загалом, комп'ютерні сліди поділяють на дві великі групи: локальні (на носіях комп'ютерної інформації, що використовувалися при вчинені злочину або були предметом посягання) і мережні (на серверах і комунікаційному обладнанні, що створюють канал зв'язку між засобом і предметом злочину)[1].

Нині актуальним в процесі проведення розслідування кіберзлочинів є питання швидкого обміну інформацією, покращення якості розслідування за допомогою налагодження активної взаємодії між прокурорами і органами досудового розслідування для встановлення користувачів послуг зв'язку, збору відомостей про рух інформації та інших технічних під час проведення перевірки за заявами та повідомленнями, що внесені до Єдиного реєстру досудового розслідування, а також створення та використання спеціальних банків зберігання електронних доказів, проведення належного розслідування кримінальних проваджень про кіберзлочини.

В умовах нового Кримінального процесуального кодексу України наглядова діяльність прокурорів трансформувалась у процесуальне керівництво, а це передбачає безпосереднє керування процесом розслідування будь-яких злочинів, зокрема й кіберзлочинів. За підписом прокурора погоджуються всі найважливіші етапи розслідування, починаючи від негласних слідчих дій та закінчуючи обвинувальним актом. Він визначає напрям розслідування, бере участь у проведенні окремих слідчих дій, а потім підтримує державне обвинувачення в суді.

Саме наявність відповідних вмінь і навичок у сфері інформаційних технологій надають можливість прокурору забезпечити дієве процесуальне керівництво розслідуванням слідчими органів внутрішніх справ кіберзлочинів, зібрати належні докази та усунути процесуальні недоліки під час розслідування.

Наприклад, останнім часом поширилися випадки викрадення особистих даних із банківських карток за допомогою банкоматів. На останні встановлюють спеціальні пристрої – скімери і накладки, за

допомогою яких зчитуються дані, які згодом використовуються для доступу до банківських рахунків клієнтів і зняття з них коштів. У самих скімерних пристроях установлені спеціальні передатчики, які надсилають отриману інформацію на мобільний телефон чи комп'ютер.

У слідчих і прокурорів існують певні труднощі щодо процесуального затримання особи і оголошення їй про підозру (ст. 208, 276-279 КПК України) і обрання запобіжного заходу (ст. 176-178 КПК України) [2] за вчинення вказаного кіберзлочину (встановлення скімерного обладнання для зняття інформації з банківських магнітних карток). Так, без проведення технічної експертизи і отримання висновку про вилучене саме скімерного обладнання у слідчого та прокурора немає підстав для прийняття вказаних процесуальних рішень.

Аналізуючи практику розслідування кіберзлочинів, можна дійти висновку щодо необхідності запровадження нового підходу до виявлення та розслідування кіберзлочинів, оскільки використання заходів та методів, які використовуються для документування традиційних злочинів, не мають результативності у цій сфері. Так сфера високих технологій потребує наявності наукових, технічних та інших спеціальних знань не лише у спеціалістів, але й у слідчих органів внутрішніх справ, прокурорів, слідчих суддів та суддів. У зв'язку з цим, особливу увагу необхідно звернути на підвищення рівня професійної підготовки працівників органів досудового розслідування та прокурора. Це пов'язано з тим, що недостатній рівень зазначеної підготовки може призвести і призводить до помилок при застосуванні кримінально-процесуальних і кримінально-правових норм [3, с.136].

Тому, відсутність достатньої кількості кваліфікованих кадрів у органах прокуратури та внутрішніх справ ускладнює прийняття швидких і оперативних рішень у кримінальних провадженнях про кіберзлочини.

Крім зазначеного вище у прокурорів і слідчих виникають проблемні питання під час розслідування злочинів у наслідок:

– переходу більшості користувачів зі стаціонарного доступу до всесвітньо мережі Інтернет на мобільні пристрої (гаджети);

– використання членами міжнародних злочинних організацій закритих TOR-мереж, що унеможливлює отримання відповідних результатів шляхом проведення негласних слідчих (розшукових) дій.

– відсутності міжнародної бази даних про вчинені кіберзлочини.

– високої латентністю вказаних видів злочинів, оскільки фінансові установи (банки) не бажають афішувати факти незаконного втручання в роботу їхньої установи з метою збереження власного іміджу.

– недостатньої кількості державних експертів в області комп'ютерно-технічної експертизи.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України від 13.04.2012 р. №4651-VI // Голос України. – 19.05.2012. – №90-91.

2. Протидія кіберзлочинам: кримінально-правові та криміналістичні аспекти: посібник. – К., 2012. – 140 с.

3. Проблеми забезпечення ефективності діяльності органів кримінального переслідування в Україні : монографія / кол. авт. ; за заг. ред. В.І. Борисов, В.С. Зеленецький. – Х. : Право, 2010. – 400 с.