дження або знищення медичного транспорту, лікарень, обладнання, пошкодження або знищення культових споруд (храмів, мечетей, синагог), використання окупантом цивільного одягу, однострою ЗСУ, емблем гуманітарних та медичних установ, інше.

5. Персональні дані ворога

Інформація про подію:

– місце (розташування) (регіон, місто, вулиця, під'їзд, квартира тощо);

– жертви і свідки, їхня кількість, імена, вік, завдані поранення тощо;

– якщо інформація стосується військовополонених або засобів ведення війни, вкажіть ім'я та посаду особи, ідентифікуючі відомості стосовно військової техніки чи боєприпасів (тип, назва, серійний номер).

Таким чином, Офіс Генерального прокурора разом з українськими та міжнародними партнерами створив цей ресурс для належного документування воєнних злочинів та злочинів проти людяності, вчинених російською армією в Україні, подальшого їх повного і об'єктивного розслідування та притягнення винних осіб до кримінальної відповідальності.

Список використаних джерел:

1. Офіційне інтернет-представництво Президента України [Електронний ресурс]. – https://www.president.gov.ua/news/administration .
2. Офіс Генерального Прокурора України [Електронний ресурс]. – Режим доступу : https://warcrimes.gov.ua/
3. Офіс Президента України [Електронний ресурс]. – Режим доступу : https://www.president.gov.ua/news/administration

Ключові слова: військовий стан, збройна агресія, Президент України, Генеральний Прокурор України, публічна інформація.

Key words: martial law, armed aggression, President of Ukraine, Prosecutor General of Ukraine, public information.

ВЕЙЦ АРКАДІЙ МИХАЙЛОВИЧ

Національний університет «Одеська юридична академія», аспірант кафедри криміналістики

ДО ПИТАННЯ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ ЗА УЧАСТЮ СЛУЖБОВОЇ ОСОБИ АБО ТАКОЇ, ЯКА ЗДІЙСНЮЄ ПРОФЕСІЙНУ ДІЯЛЬНІСТЬ, ПОВ'ЯЗАНУ З НАДАННЯМ ПУБЛІЧНИХ ПОСЛУГ

Сьогодні службова особа або така, яка здійснює професійну діяльність, пов'язану із наданням публічних послуг, знаходиться у пріоритеті серед учасників організованої злочинної групи осіб, що діє у кіберпросторі.

Втім, прямих статистичних показників участі такої категорії осіб у означеної злочинній діяльності немає. За звітні періоди органами Національної поліції України були закінчені кримінальні провадження стосовно наступних категорій осіб: особи, що раніше вчинили аналогічний злочин (2019 р. – 177 осіб; 2020 р. – 215 осіб; 9 місяців 2021 р. – 156 осіб); особи, що вчинили злочин в групі осіб (2019 р. – 135 осіб; 2020 – 58 осіб; 9 місяців 2021 – 200 осіб); за участю неповнолітніх осіб (2019 р. – 9 осіб; 2020 – 51 особа; 9 місяців 2021 – 11 осіб). Разом з тим станом на 1 жовтня 2021 р. близько на 70 % збільшилась активність кіберполіції щодо протидії кримінальним правопорушенням, учиненим організованими групами. Так, якщо в 2020 р. кіберполіцією виявлено 14 організованих груп, участь яких доведена у вчиненні 197 епізодів злочинної діяльності, то вже за 9 місяців 2021 р. – 21 організована група та відповідно 613 епізодів злочинної діяльності [1].

Результати ознайомлення з матеріалами судово-слідчої практики щодо вчинення кіберзлочинів групою осіб свідчіть, що у більше половини з них залучалися особи, які виконують організаційно-розпорядчі чи адміністративно-господарські функції, або функції за спеціальними, наданими державою, повноваженнями. Саме ці особи є носіями інформації з обмеженим доступом, часто інформації про особу (персональні дані), інформації для службового користування; професійної таємниці (лікарська, адвокатська, нотаріальна, страхова, банківська та деякі інші види таємниці).

Найбільш поширим механізмом вчинення злочинів в цьому сенсі є збут інформації з обмеженим доступом. Як правило, такі злочини вчиняє особа, шо має доступ до такої інформації в результаті наявних в неї повноважень, виконання службових (професійних) обов'язків. Так, працівник ПАТ КБ «ПриватБанк» копіював інформацію, що становить банківську таємницю, за грошову винагороду та через мессенджер Telegram надсилав її замовнику. Або ж в Херсоні протягом тривалого часу гр. К, працівник юридичної компанії, використовуючи вільний доступ до інформації за місцем роботи, згідно з вироком Херсонського міського суду Херсонської області від 09 серпня 2018 року, здійснював продаж інформації з обмеженим доступом, а саме баз даних Національної поліції, Державної фіскальної служби, Головного сервісного центру МВС України, Інтерполу (міжнародної організації кримінальної поліції), Державної міграційної служби України, Державної прикордонної служби України, ПАТ КБ «Приватбанк», ПАТ «Укрпошта», ТОВ «Нова пошта», а також деталізовані телефонні розмови; єднання мобільних операторів України ПрАТ «Водафон», ПрАТ «Київстар», ТОВ «Лайфселл».

Незаконні дії із банківськими платіжними засобами (банківськими картами) також досить часто пов'язані із залученням службових осіб або таких, які здійснюють професійну діяльність. Наведемо цікавий приклад: судовою палатою з розгляду кримінальних справ Апеляційного суду Києва у справі № 11-сс/796/6258/2017 організатор злочину використовував ідентифікаційні дані, з магнітних стрічок платіжних карток. Цих даних було достатньо для створення дублікатів таких карток

та проведення за їх допомогою платежів. Без згоди та відома законного власника. Втім, такі картки могли бути використані лише на території США та тільки для придбання товарів без прямого зняття готівки. Саме тому організатор знайшов кількох співучасників, які були на території США, де вони повинні були придбати дампи, магнітні стрічки, пристрій для їх запису, а також зробити дублікати карток. Виготовлені картки обмінювалися на подарункові сертифікати, коди подарункових сертифікатів – на біткойни, а біткойни обмінювались на гроші. При цьому в складі організованої групи не було встановлено хакера або іншу особу, яка саме й могла отримувати ідентифікаційні дані карток. Це саме й наводить на думку про участь в злочинній групі особи, яка мала доступ до даних через свої службові повноваження.

Виходячи з загальновизнаній криміналістичній концепції злочинних технологій [2 – 5], ми приходимо до думки, що з криміналістичної точки зору злочинна діяльність у кіберпросторі за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану із наданням публічних послуг можна розглядати через призму технології або комплексу органічно взаємопов'язаних злочинних дій з єдиною корисливою метою.

Ключове місце в технології досліджуваної злочинної діяльності займають кіберзлочини у широкій інтерпритації поняття як такі діяння, об'єктом злочину яких є комп'ютерні дані або системи, а також діяння, за яких використання комп'ютерних або інформаційних систем є невід'ємною складовою способу вчинення злочину [6].

Отже, для конкретизації сутності досліджуваного виду злочинів є потреба у розробленні його криміналістичної класифікації. Це буде корисним як для науковців з метою подальшого вдосконалення криміналістичної методики, так й для практиків з метою правильної організації процесу розслідування кіберзлочинів, що не дозволить уникнути кримінальної відповідальності особам, які причетні до вчинення кіберзлочинів.

Список використаних джерел:

1. Аналітична довідка Національної поліції України, 2021.
2. Барцицька А. А. Криміналістичні технології : дис. … канд. юрид. наук : 12.00.09.Одеса, 2012. 194 с.
3. Шмонин А. В. Методология криминалистической методики. М. : Юрлитинформ, 2010. 416 с.
4. Криминалистика : учебник / под. ред. Н. П. Яблокова. 2-е изд. М. : Юристъ, 2002. 718 с.
5. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів. О. : Фенікс, 2007. 260 с.
6. Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное

сотрудничеств : справочный док. 13 Конгресс ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апр. 2015 г. (A/CONF.222/12). URL: http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf

Ключові слова: кіберзлочин, особа злочинця, службові злочини, службові обов'язки, протидія.
Key words: cybercrime, the person of the criminal, official crimes, job responsibilities, counteraction.

ЧЕРНОВ ОЛЕКСАНДР ВІТАЛІЙОВИЧ

Національний університет «Одеська юридична академія», аспірант кафедри криміналістики

КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ПЕРЕШКОД ЗДІЙСНЕННЮ ЕФЕКТИВНОГО РОЗСЛІДУВАННЯ УМИСНИХ ВБИВСТВ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ ТА В УМОВАХ МАСОВИХ ЗБРОЙНИХ КОНФЛІКТІВ

Наразі, внаслідок складної та критичної ситуації в Україні внаслідок повномасштабного вторгнення країни агресора в нашу країну, що ускладнюється соціально-економічними та політичними умовами, досить гостро постає питання щодо здійснення ефективного розслідування злочинів, а зокрема вбивств працівників правоохоронних органів, що скоюються під час війни. Як наслідок цього, з'являється проблема пов'язана із зростанням кількості вчинених злочинів проти життя і здоров'я особи за допомогою застосування різноманітних способів та засобів вчинення злочинів цієї категорії. В даному контексті, питання підіймається досить гостро, оскільки саме працівники правоохоронного органу є тією групою осіб, що здійснює підтримання правопорядку у країні під час дії воєнного стану та відповідно знаходиться у підвищеній бойовій готовності до виконання завдань щодо недопущення вчинення кримінальних правопорушень, наслідком чого, вони є найбільш вразливою категорією жертв щодо вчинення проти них таких злочинів.

Внаслідок широкомасштабної військової агресії на території України одним із основних чинників, що суттєво позначається на індексі безпеки, слід вважати збільшення незаконних потоків вогнепальної зброї, бойових припасів, вибухових речовин і вибухових пристроїв в Україні. У той же час, є також і загальні проблеми у здійсненні розслідування, які, притаманні розслідуванню саме зазначеній категорій злочинів та вказують на те, що недостатня якість розслідування є наслідком не виключно обставин війни, але й загальною проблемою нездатності органів досудового слідства діяти ефективно.