

самостійна складова криміналістичного забезпечення. Зважаючи на це, основний зміст техніко-криміналістичного забезпечення розслідування кримінальних правопорушень становлять відповідні спеціальні знання і технічні засоби, а також суспільні відносини, що виникають у процесі їх застосування. Розвиток суспільних відносин, вплив науково-технічного прогресу, удосконалення засобів та методів злочинної діяльності вимагають постійної уваги до вказаних питань [2, с. 221].

При розслідуванні кримінальних правопорушень проти власності спеціальні знання використовують переважно у таких формах: безпосереднє використання спеціальних знань слідчим, прокурором (у тому числі криміналістом) при виконанні своїх процесуальних функцій щодо збирання, дослідження та оцінки доказів; участь спеціалістів при провадженні окремих слідчих (розшукових) та процесуальних дій; призначення і провадження судових експертиз.

Проведення слідчих (розшукових) дій без залучення відповідних спеціалістів або поверхневе використання спеціальних знань переважно призводить до того, що переважна кількість кримінальних правопорушень проти власності залишаються не розкритими, а злочинці продовжують (відновлюють) свою протиправну діяльність.

1. Костира О. М. Криміналістична характеристика та особливості розслідування грабежів і розбоїв, учинених раніше засудженими особами : дис. ... канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2019. 212 с.

2. Черноус Ю. М. Криміналістичне забезпечення розслідування злочинів: наукові засади та напрями реалізації. *Сучасні тенденції розвитку криміналістики та кримінального процесу* : тези доп. Міжнар. науково-практ. конф. до 100-річчя від дня народження проф. М. В. Салтевського (м. Харків, 8 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. С. 220–222.

Єфімов Микола Миколайович
професор кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ,
доктор юридичних наук, професор

ДО ПИТАННЯ РЕАЛІЗАЦІЇ ПРОФІЛАКТИЧНИХ ЗАХОДІВ ПРИ РОЗСЛІДУВАННІ ШАХРАЙСТВ У МЕРЕЖІ «ІНТЕРНЕТ» ПІД ЧАС ВІЙСЬКОВОГО СТАНУ В УКРАЇНІ

Кіберзлочинність під час дії військового стану в Україні наразі продовжує розвиватися. Це зумовлено різними факторами. По-перше, це й військова агресія нашого східного «сусіда», по-друге, безперервний розвиток

комп'ютерної техніки, по-третє, постійне удосконалення хакерами своїх професійних навичок. Серед найбільш поширених протиправних діянь, які вчиняються кіберзлочинцями різного рівня, безумовно треба виокремити шахрайство у мережі «Інтернет». Вказане кримінальне правопорушення може вчинюватися багатоманітними способами та за допомогою різноманітних засобів. Треба наголосити на тому, що одним із важливих напрямів діяльності правоохоронних органів є профілактика кримінальних правопорушень. Реалізація профілактичних заходів при розслідуванні шахрайств у мережі «Інтернет» також наявна з-поміж інших.

Щодо загальних засад та характеристик профілактики правопорушень ми підтримуємо судження О. М. Макаренка, який визначив її як «... методологічно складне суспільне явище, що пояснюється таким. По-перше, профілактика правопорушень – багаторівнева система заходів, що проводяться державними, недержавними органами та установами, громадськими формуваннями та окремими громадянами для мінімізації дії або нейтралізації причин, що породжують правопорушення або сприяють їх вчиненню. По-друге, профілактика правопорушень – це особливий вид соціального управління, що має за мету зниження інтенсивності процесів детермінації правопорушень, нейтралізацію дії її причин та умов для обмеження правопорушень до соціально прийняттого рівня. По-третє, профілактика правопорушень – це різноманітна за формами діяльність, яка спрямована на пошук шляхів, засобів та інших можливостей ефективного впливу на правопорушення» [1, с. 119].

У розрізі досліджуваного питання необхідно згадати й про Департамент кіберполіції Національної поліції України, на який покладено обов'язки як з розслідування кіберзлочинів, так і з їх попередження. Наприклад, серед обов'язків працівників вказаного підрозділу визначено розслідування правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а також правопорушень, які вчиняються за допомогою комп'ютерних технологій [2]. Інакше кажучи, до цієї категорії протиправних діянь можна віднести і шахрайство, передбачене ч. 3 ст. 190 КК України, та заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку [3, с. 134].

С. В. Самойлов обґрунтовує думку про те, що ефективність профілактики шахрайств, учинених із використанням мережі «Інтернет», можна значно підвищити лише за комплексного підходу до означеної проблеми із залученням не лише можливостей правоохоронних органів, а й інших суб'єктів впливу. Дослідник впорядкував профілактичні заходи в такій структурі: «...заходи, що використовуються державою на законодавчому рівні (розробка, апробація та прийняття законів та підзаконних актів, які врегульовують відносини в мережі «Інтернет» та сприяють створенню таких умов, за яких вчинення аналізованих шахрайств буде унеможливлено або дуже ускладнено); заходи, що застосовуються постачальниками послуг (у межах їх

власної ініціативи); заходи, що використовуються правоохоронними органами (заходи роз'яснювального та запобіжного характеру); заходи, що застосовуються користувачами мережі (активна позиція пересічного користувача мережі «Інтернет», що полягає у: правомірній поведінці безпосередньо в мережі; відстоюванні своїх прав та законних інтересів через установлені законодавством механізми); заходи, що використовуються спільними зусиллями різних суб'єктів» [4, с. 11–12].

Також ми підтримуємо позицію А. Е. Жиліна, який серед профілактичних заходів, які необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів, виділив такі: «... повідомлення громадянам через засоби масової інформації про юридичну відповідальність за шахрайську діяльність в сфері використання банківських електронних платежів; виявлення осіб, схильних до антисуспільної поведінки в сфері комп'ютерної діяльності (хакери, фішери) та подальша їх постановка на облік у підрозділах Кіберполіції; інформування населення через засоби масової інформації, месенджери та соціальні мережі про випадки вчинення шахрайських дій у сфері використання банківських електронних платежів (фішинг, кардинг, сніфферінг)» [5, с. 214].

Підсумовуючи, зазначимо, що реалізація профілактичних заходів при розслідуванні шахрайств у мережі «Інтернет» під час військового стану в Україні є досить важливим аспектом в діяльності правоохоронних органів. Адже без ефективної профілактики протиправних діянь кількість випадків їх вчинення лише буде збільшуватись.

1. Макаренко О. М. Щодо з'ясування терміну «профілактика правопорушень» та суміжних з ним понять. *Право і безпека*. 2004. № 3. Ч. 1. С. 118–120.

2. Кіберполіція. Кібербезпека України. URL: https://wiki.legalaid.gov.ua/index.php/Кіберполіція._Кібербезпека_України (дата звернення: 12.09.2023).

3. Сфімов М. М., Павлова Н. В., Чучко С. В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу Інтернет: теоретичні та праксеологічні засади : монографія. Одеса : Видавничий дім «Гельветика», 2022. 200 с.

4. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. ... канд. юрид. наук : 12.00.09. Донецький юридичний інститут. Донецьк, 2014. 18 с.

5. Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020. № 2. Т. 2. С. 209–215.