

- розміщення орієнтувань та іншої інформації з метою розшуку осіб, які переховуються від органів досудового розслідування та суду або тих, які пропали безвісти;
- використання тактичних прийомів дезінформації щодо стратегії розслідування конкретного кримінального правопорушення з метою наступального та ефективного проведення оперативно-розшукових заходів та слідчих розшукових дій;
- встановлення за допомогою розміщення окремої інформації в ЗМІ очевидців та свідків кримінального правопорушення, які невідомі працівникам оперативного підрозділу та слідчому тощо.

Список використаної літератури:

1. Стеценко Ю.В. Науково-методичні засади використання засобів масової інформації при розслідуванні злочинів: автореф. дис... канд. юрид. наук.: 12.00.09. К. 2006. 20 с.
2. Мокряк М.О. Вплив засобів масової інформації на формування суспільної думки, ставлення до закону та злочинність. *Право і суспільство*. 2016. С.111-116
3. Искендеров А.Ф. Взаємодія слідчих та оперативних підрозділів із засобами масової інформації в протидії організований злочинній діяльності: типові ситуації та форми. *Південноукраїнський правничий часопис*. 2014. №3. С. 247-250

Ключові слова: засоби масової інформації, слідчий, оперативні підрозділи, взаємодія.

Ключевые слова: средства массовой информации, следователь, оперативные подразделения, взаимодействие.

Key words: mass media, investigator, operative divisions, interaction.

ВЕЙЦ АРКАДІЙ МИХАЙЛОВИЧ

*Національний університет «Одеська юридична академія»,
аспірант кафедри криміналістики*

ПРОБЛЕМИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ, ВЧИНЕНИХ ЗА УЧАСТЮ СЛУЖБОВОЇ ОСОБИ АБО ТАКОЇ, ЯКА ЗДІЙСНЮЄ ПРОФЕСІЙНУ ДІЯЛЬНІСТЬ, ПОВ'ЯЗАНУ З НАДАнням ПУБЛІЧНИХ ПОСЛУГ

Ідея електронної держави ставить перед суспільством нові завдання щодо боротьби зі службовими злочинами у кіберпросторі. Згідно даних Департаменту організаційно-аналітичного забезпечення Національної поліції України на тлі загального зростання рівня кіберзлочинності показник розкриття таких злочинів має тенденцію до зниження: у 2014 р. слідчі Національної поліції України склали 797 обвинувальних актів; у 2015 р. – 756; у 2016 р. – 453; у 2017 р. – 764; у 2018 р. – 666; майже

у кожному кримінальному провадженні фігурують невстановлені особи, які мали доступ до державних інформаційних систем, а відповідно до інформації з обмеженим доступом, що була використана при вчиненні кіберзлочину. При цьому офіційний облік щодо вчинення таких злочинів за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, не ведеться жодним підрозділом. Метою цієї доповіді є формулювання проблем розслідування кіберзлочинів, за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. Останніми роками в Україні розроблено велику кількість криміналістичних методик розслідування окремих видів кіберзлочинів, використання яких практиками слідчих підрозділів правоохоронних органів відіграє важливу роль для виявлення та розслідування здебільше конвенційних складів злочинів, тобто тих ще містяться в Конвенції про кіберзлочинність. Втім теоретичних напрацювань щодо боротьби з кіберзлочинами, вчиненими службовою особою відсутні. До того ж постійно відчується брак необхідної сучасної наукової літератури, яка б ґрунтувалася на узагальненнях сучасної української практики виявлення та розслідування такої групи злочинів. Метою цієї доповіді є формулювання проблем розслідування кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг.

Ознайомлення з матеріалами судово-слідчої практики, змістом реєстру судових рішень та офіційних публікацій на сторінках Департаменту кіберполіції Національної поліції України дозволяє сформулювати та обґрунтувати наступні проблеми розслідування кіберзлочинів, що стали предметом нашого дослідження.

По-перше, сьогодні поширеним способом вчинення кіберзлочину є створення підроблених (фіктивних) Інтернет-сторінок державних органів, підприємств, електронних платіжних систем, відомих фірм та компаній. Як правило, в планах розслідування таких злочинів основна версія щодо способу вчинення таких злочинів пов'язана із шахрайським обманом шляхом вчинення фіктивного представництва. Для слідчого в такому випадку винний не співвідноситься з установою-жертвою, створюється враження про свою неналежність до того чи іншого державного підприємства або установи, банка тощо. Втім, це не завжди відповідає дійсності, якщо слідчий уважно ставиться до збору матеріалів, що характеризують особу злочинця, то він часто встановлює у колі спілкування останнього осіб, що мають або мали доступ до інформації щодо особливостей функціонування певної установи, специфіки оформлення її логотипів, печаток, електронних документів тощо. За такої обставини розслідування повинно тривати до моменту встановлення складу всіх учасників групи, що надасть можливість попередити наступний епізод злочинної діяльності із участю спеціального суб'єкту.

По-друге, у криміналістичному аспекті злочинна діяльність у кіберпросторі являє собою систему об'єднаних загальними мотивами і цілями злочинних дій, операцій та епізодів, розраховану на відносно

тривалий період і підготовку, що включає в себе планування, здійснення, маскування та протидію її викриттю [1]. Тому в системі злочинної діяльності злочинці змушені піклуватися про свою безпеку не лише в період здійснення злочинних акцій, але й у процесі всієї їх «трудової діяльності», в цілому – існування [2, с.5]. З цією метою вони вдало застосовують технології анонімізації доступу до ресурсів електронних інформаційних мереж, зокрема мережі Інтернет (проксі-сервісів (комплекси програм), віртуальних приватних мереж (VPN-технологій, або Virtual Private Network) інших засобів-анонімайзерів). Для подолання такого способу приховання злочинної діяльності слідчий повинен активно застосовувати міжнародну співпрацю з країнами ЄС та США, які на сьогодні мають численні центри протидії кіберзлочинам, що можуть відслідковувати трафік від певного користувача та здійснювати моніторинг потоку інформації в цілому з тим, щоб встановити кінцeve обладнання, що використовується як знаряддя вчинення злочину.

По-третє, тиск на слідчого чи прокурора з боку корумпованих представників влади підчас розслідування кіберзлочинів, також не можна залишати без уваги як проблему розслідування кіберзлочинів, вчинених за участю службової особи. Серед засобів подолання такої протидії знані науковці називають тактичні операції «Слідча таємниця» або «Анти корупція» [3]. Однак, ми хочемо підкреслити, що використання фактору раптовості при проведенні слідчих (розшукових) дій, максимально розширене використання допомоги спеціалістів Департаменту кіберполіції та спеціальних експертних установ Служби безпеки України, а також швидке та якісне вилучення інформації на відділених носіях електронної інформації в комплексі із дослідженням останньої значно ускладнює процес впливу на процес розслідування зацікавлених осіб.

Таким чином, визначення проблем розслідування досліджуваної категорії кіберзлочинів дозволить в подальшому конкретизувати напрямки розслідування злочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, а також запропонувати вибір тактики проведення слідчих дій.

Список використаної літератури:

1. Самойленко О. А. До питання механізму вчинення злочинів у кіберпросторі. Теорія та практика судової експертизи і криміналістики: матеріали Всеукраїнської науково-практичної конференції з нагоди 85-річчя доктора юридичних наук, професора Ніни Іванівни Клименко (м. Київ, 27 лютого 2018 року). Київ, Маріуполь, 2018. 412 с. С. 297-298
2. Бахин В. П. Преступная деятельность как объект криминалистического изучения: лекция. К.: б.и, 1991 С. 5
3. Волобуев А.Ф. Розслідування і попередження розкрадань майна у сфері підприємництва: Навч. посібник // За ред. О.М. Бандурки. – Х.: Ун-т внутр. справ, 1999. – 245 с. – С.117.

Ключові слова: кіберзлочини, електронна держава, розслідування кіберзлочинів.
Ключевые слова: киберпреступления, электронное государство, расследование киберпреступлений.
Key words: cybercrimes, e-state, investigation of cybercrimes.

ВИНОГРАДОВ ВАДИМ ІГОРОВИЧ

*Національний університет «Одеська юридична академія»,
аспірант кафедри криміналістики*

ОКРЕМІ ВИДИ ЕКСПЕРТИЗ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ У СФЕРІ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ

Виявлення істини під час розслідування злочинів у сфері публічних закупівель часто потребує залучення спеціальних знань у формі експертиз. Відповідно до ч. 1 ст. 69 КПК України експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань. В ч. 5 ст. 69 КПК України закріплено, що експерт зобов'язаний особисто провести повне дослідження і дати обґрунтований та об'єктивний письмовий висновок на поставлені йому запитання.

У сфері публічних закупівель неможливо виокремити один об'єкт злочинних посягань, як і один певний вид злочину. Ця сфера відрізняється насамперед тим, що кримінальні правопорушення, що вчиняються у її межах, підлягають кваліфікації за різними статтями Кримінального кодексу України. Зазвичай це взаємопов'язані злочини, що об'єднані метою і виконавцями, що можуть вчиняти певний злочин на певному етапі.

Волобуєв А.Ф. виділяє такі злочини як комплекс, де виокремлено основні та підпорядковані (вторинні, допоміжні) злочини [1, с. 38]. А.М. Меденцев пропонує основними злочинами у сфері публічних закупівель вважати шахрайство (ст. 190 КК України); привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем (ст. 191 КК України); прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою (ст. 368 КК України) [3, с. 109]. Підпорядкованими (допоміжними) злочинами у залежності від певних обставин, можуть бути легалізація (відмивання) майна, одержаного злочинним шляхом (ст. 209 КК України), підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів (ст. 358 КК України), зловживання владою або службовим становищем (ст. 364 КК України), службове підроблення