– наявності та ролі осіб посередників;
– обставин, що передували вчиненню корупційного діяння;
– часу, місця та обстановки передачі неправомірної вигоди, або ж пропозиції чи обіцянки її надання;
– результатів та наслідків злочинної «угоди»;
– наявності чи відсутності інших осіб, що проінформовані про злочинну подію;
– наявності чи відсутності певних документів, записок, повідомлень, фотографій, аудіо- чи відеозаписів, що б підтверджували слова заявника.

Послідовне та повне з'ясування зазначених блоків питань дозволить слідчому належним чином організувати процес розслідування, мінімізувавши можливість виникнення тактичних ризиків.

Список використаної літератури:

1. Кримінальний кодекс України [Електронний ресурс] / Закон України від 05 квітня 2001 року. № 2341-III: станом на 01 листопада 2014 р. № 3718-17. – Електрон. тек ст. дані: http://zakon1.rada.gov.ua.

Ключові слова: допит, слідча (розшукова) дія, корупція, органи місцевого самоврядування, розслідування.
Ключевые слова: допрос, следственное (розыскное) действие, коррупция, органы местного самоуправления, расследование.
Key words: interrogation, investigative (search) action, corruption, local self-government bodies, investigation.

ПАНАСЮК АРТУР ОЛЕКСІЙОВИЧ

Національна академія прокуратури України,
слухач Інституту спеціальної підготовки

АЛГОРИТМ ПОШУКУ КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Досліджуючи сутність і цінність мережі Інтернет для криміналістики, зазначаємо, що мережа Інтернет – це високий ступінь впливу та технологічна матриця на даний момент. Саме алгоритмічний характер мережі Інтернет, можливість її багаторазового використання у розв'язанні подібних завдань, досягнення заданих результатів і визначає її специфічність та унікальність. Даний процес не обминув й досудове розслідування, оновлюючи зміст виявлення та розслідування злочинів за допомогою мережі Інтернет. Вище зазначене дозволяє зробити висновок, що у всіх випадках мережа Інтернет розуміється у двох взаємодоповнюючих аспектах, як:

1) процедурно організована форма впливу на досудове розслідування за допомогою спеціальної сукупності засобів та методів такого впливу;

2) технологія, що досліджує чи описує відповідну операцію впливу.

Загальний алгоритм пошуку криміналістично значущої інформації в мережі Інтернет складається з наступних етапів:

1. Формулювання пошукового запиту відповідно до обставин, які підлягають встановленню в кримінальному провадженні. Переформулювання, вже сформованого пошукового запиту, на синоніми та антоніми, з метою формування нових пошукових запитів;

2. Окремий пошук за кожним сформованим пошуковим запитом. Застосування прийомів: розширення чи звуження пошукового запиту; помилкового написання; нових словоформ; додаткових описань; зміни мови;

3. Пошук за метапошуком;

4. Пошук в мережі Інтернет з великим об'ємом індексу (національні та всесвітні системи);

5. Пошук в найбільших соціальних мережах (наприклад: Фейсбук, Твіттер, Інстаграм, Вконтакті та ін.);

6. Пошук в спеціалізованих та профільних соціальних мережах (наприклад, Однокласники, ОК та ін.);

7. Перше покрокове опрацювання отриманої інформації (види: реєстри, запити, дані, бази; характеристики: часові, місцеві; джерело розміщення) та виявлення кола проблемних даних з формулюванням для них власних пошукових запитів;

8. Пошук проблемних даних за результатами вибірки п. 7 за п.п. 2-6;

9. Друге покрокове опрацювання отриманої інформації (види: реєстри, запити, дані, бази; характеристики: часові, місцеві; джерело розміщення);

10. Виділення зі знайденого криміналістично значущої інформації, його криміналістичне опрацювання та за потреби процесуальне закріплення відповідно до КПК України.

Застереження слідчому при роботі в мережі Інтернет та використанні інформації для виявлення та розслідування злочинів полягає у дотриманні ним наступного правила: "Вся інформація в мережі Інтернет не достовірна, поки слідчий не доведене зворотне". Тобто, вся інформація без виключень перевіряється на достовірність. Така перевірка відбувається різними шляхами з обов'язковою фіксацією процесу та отриманого результату.

Завданнями перевірки інформації з мережі Інтернет є:

1) пізнання змісту;

2) аналіз реквізитів інформації (тип, обсяг, дата створення, дата зміни, дата відкриття та ін.);

3) перевірка достовірності інформації за допомогою встановлення механізму виникнення (джерела).

Рекомендовано при перевірці інформації з мережі Інтернет використовувати консультативну діяльність спеціаліста або професійну діяль-

ність експертів. Судження спеціаліста і експерта вбирається в форму його укладення, також може бути проведено допит спеціаліста або експерта. Перевірка інформації з мережі Інтернет може здійснюватися шляхом отримання нових доказів (наприклад, висновок експерта, допит потерпілого), а також шляхом їх зіставлення.

Таким чином, загальний алгоритм пошуку криміналістично значущої інформації в мережі Інтернет уявляється етапним та складається з взаємообумовлених дій, що ґрунтуються на інформаційно-комунікаційному та техніко-технологічному підходах.

Ключові слова: джерело інформації, криміналістична інформація, аналітична робота, кіберпростір, мережа Інтернет.

Ключевые слова: источник информации, криминалистическая информация, аналитическая работа, киберпространство, сеть Интернет.

Key words: source of information, criminalistics information, analytical work, cyberspace, Internet network.

СТАУРСЬКА ОЛЕКСАНДРА МИКОЛАЇВНА

Національний університет «Одеська юридична академія»,
аспірант кафедри криміналістики

ПРОБЛЕМИ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ У КОНТЕКСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

На сьогоднішній день, проблема боротьби із кіберзлочинністю набуває все більш великих масштабів. Законодавче регулювання даної проблеми на міжнародному рівні розглядається багатьма вченими. Впровадження комп'ютерних технологій у різноманітні сфери життя українського суспільства відкриває широкі перспективи його соціально-економічного і духовного розвитку. Але разом із цим результати науково-технічного прогресу створюють нові можливості для вчинення різноманітних злочинів.

Аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності. Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж.

Основна проблема боротьби зі злочинністю в мережі Інтернет полягає в транснаціональності самої мережі і у відсутності механізмів контролю, необхідних для правозастосування. Коли мережа Інтернет створювалася технологічно як структура без ієрархії і без якогось «ядра», зруйнувавши які, можна було б паралізувати її роботу, навряд чи хтось міг уявити масштаби розвитку проекту,