4. Живко З.Б. Комплексный подход к управлению безопасностью предприятия: взаимодействие подсистем и роль менеджера [Текст] / З.Б. Живко // Научный диалог. – 2013. – №1 (13): История. Социология. Экономика. – С. 177-187.
5. Одинцов А. А. Экономическая и информационная безопасность предпринимательства / А.А. Одинцов. – М.: Академия, 2006. – 336 с.

Падалка А. М.
к.ю.н., в.о. завідувача кафедри фінансових розслідувань
факультету підготовки, перепідготовки та підвищення
кваліфікації працівників податкової міліції
Університет державної фіскальної служби України

РОЗСЛІДУВАННЯ ОРГАНІЗОВАНОЇ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ У СФЕРІ ОПОДАТКУВАННЯ, ЗДІЙСНЮВАНОЇ З ВИКОРИСТАННЯМ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

1. Ефективність розслідування організованої злочинної діяльності у сфері оподаткуваання ще залишається досить низькою. Це зумовлено: складним процесом доказування таких кримінальних правопорушень, потужною протидією розслідуванню з боку учасників організованих злочинних угруповань, проблемами з організацією використанням криміналістичних комплексів, недоліками професійної підготовки слідчих та певною мірою незнанням ними особливостей використання спеціальних знань в ході розслідування зазначеної організованої злочинної діяльності, особливо здійснюваної з використанням сучасних комп'ютерних технологій.

2. Як свідчать здійснені нами узагальнення, поширеними формами використання спеціальних знань, під час розслідування організованої злочинної діяльність у сфері оподаткування, здійснюваної з використанням комп'ютерних технологій є: а) призначення судово-економічної експертизи та комп'ютерно-технічних експертиз; б) звернення слідчого за письмовою консультацією до відповідного спеціаліста; в) залучення спеціаліста до участі у слідчих (розшукових) діях; г) призначення документальних перевірок на вимогу слідчого; ґ) проведення ревізій; д) безпосереднє використання спеціальних знань самим слідчим, під час проведення слідчих (розшукових) дій.

3. Розслідування організованої злочинної діяльності у сфері оподаткування, здійснюваної з використанням сучасних комп'ютерної техніки не можливе без проведення комп'ютерно-технічної експертизи. Серед проблем, які виникають у слідчих, під час призначення такої експертизи слід відмітити: 1) зумовлені недостатнім фінансуванням виконання даних експертиз на договірній основі; 2) зумовлені недостатньою кількістю і підвищеною завантаженістю експертів; 3) зумовлені визначенням завдань експертизи та формулюванням питань експерту; 4) зумовлені визначенням переліку об'єктів, які доцільно направляти на експертизу; 5) зумовлені відсутністю відповідної експертної методики для вирішення тих чи інших питань, що поставлені перед експертом.

4. Залучення спеціалістів до проведення слідчих (розшукових) дій є досить поширеною формою використання спеціальних знань, під час розслідування організованої злочинної діяльності у сфері оподаткування, здійснюваної з використанням сучасних комп'ютерних технологій. У даному випадку спеціалісти залучаються з метою: – визначення переліку об'єктів, які підлягають вилученню; – для виявлення необхідних об'єктів серед інших; – для встановлення призначення об'єктів, що підлягають вилученню; – для визначення віднесення об'єктів, які вилучаються до події, що розслідується і т. ін. Серед зазначених об'єктів можна вказати: системні комп'ютерні блоки, жорсткі диски, флеш пам'ять у вигляді карток, ноутбуки, принтери, карманні персональні компютери і т. ін.

5. Хоча слідчі інколи безпосередньо самі використовують спеціальні знання, під час проведення слідчих (розшукових) дій (наприклад, фотографування, аудіозапис), однак недостатність криміналістичного забезпечення та відповідних навичок є перешкодою для використання такої форми спеціальних знань.

Набути спеціальні знання, слідчі можуть шляхом: – отримання другої вищої освіти, зокрема технічної (у галузі ком'пютерних технологій); – технічної самоосвіти; – під час відповідного консультування у спеціалістів; – на заняттях по службовій підготовці; – отримання відповідних навичок, в ході занять за участю досвідченого спеціаліста у сфері комп'ютерних технологій.

Крім цього, джерелами набуття спеціальних знань слідчим, можна визначити: – поради колег по роботі; – самостійне вивчення відповідної комп'ютерної літератури; – опрацювання методичних рекомендацій розміщених у навчальних посібниках, бюлетенях та оглядах слідчої практики; – консультування у досвідчених спеціалістів у сфері комп'ютерних технологій; – отримання методичної допомоги з боки досвідчених слідчих вищестоящих підрозділів; – навчання на курсах підвищення кваліфікації.

6. Під час розслідування організованої злочинної діяльності у сфері оподаткування, досить часто у слідчих виникає необхідність у залученні до проведення слідчих (розшукових) дій, перевірок та з метою консультування спеціалістів в області комп'ютерних технологій.

Більшість бухгалтерської та податкової документації слідчими вилучається на цифрових носіях, тому спеціалісти у сфері комп'ютерних технологій можуть допомогти слідчому уникнути можливих програмних пасток, які здатні приховати інформацію від несанкціонованого доступу або знищити її.

7. Слідчий вирішуючи питання про визначення компетенції спеціаліста у сфері комп'ютерних технологій, який залучається для участі у слідчих (розшукових) діях, наданні відповідної консультації, повинен визначити дві суттєві обставини: 1) наявність в особи, яка залучається спеціальних знань саме у тій області технічних знань, відомості з якої необхідно використати слідчому під час розслідування конкретного правопорушення у сфері оподаткування; 2) ступінь володіння спеціалістом методикою застосування спеціальних знань, необхідних для ефективного проведення тих чи інших слідчих (розшукових) дій.

8. Керівникам слідчих підрозділів, необхідно періодично здійснювати заходи спрямовані на підвищення кваліфікації підлеглих слідчих, які розслідують організовану злочинну діяльність у сфері оподаткування, здійснюваної з використанням сучасних комп'ютерних технологій. Такі заходи можуть здійснюватися у формах організації короткострокових зборів,

на базі спеціалізованих навчальних закладів або у формі планових стажувань осіб. Під час таких заходів повинні відпрацьовуватися питання застосування сучасних методів дослідження об'єктів із сфери сучасних комп'ютерних технологій; розкриватися сучасні можливості комп'ютерно-технічної експертизи; даватися криміналістичні рекомендації по збиранню та упорядкуванню об'єктів, які направляють на дослідження експертам тощо.

9. Аналіз законодавства, літературних джерел та матеріалів кримінальних справ (проваджень) показує, що при значній увазі до використання спеціальних знань різних категорій кримінальних правопорушень, проблема повноцінного використання спеціальних знань під час розслідування організованої злочинної діяльності у сфері оподаткування недостатньо досліджена, що зумовлює недоліки та суттєві труднощі при розслідуванні зазначених кримінальних правопорушень, а тому дана проблематика залишається актуальною. Основні завдання, які повинна вирішувати криміналістика в зазначеному напрямі – це актуалізація наукового і методичного забезпечення при використанні спеціальних знань, підвищення результативності шляхом впровадження в діяльність органів досудового розслідування найновіших наукових досліджень і передового досвіду.

УДК 336.7

Окряк М. А.
судовий розпорядник, Господарський суд Тернопільської області, аспірант кафедри економічної безпеки та фінансових розслідувань ЮФ ТНЕУ
Науковий керівник: д.е.н., професор, професор кафедри економічної безпеки та фінансових розслідувань ЮФ ТНЕУ, Мартинюк В. П.

ПРОТИДІЯ КІБЕРЗАГРОЗАМ У НАПРЯМІ ЗАБЕЗПЕЧЕННЯ ГРОШОВО-КРЕДИТНОЇ БЕЗПЕКИ ДЕРЖАВИ

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ. Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

– невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;

– недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;