**ЕКОНОМІКА,
ФІНАНСИ,
ПРАВО**

- ***П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк***
  ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк
  КОНСОЛІДОВАНИЙ КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ, ВЧИНЕНИХ В БАНКІВСЬКІЙ СИСТЕМІ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк
  ЗЛОЧИНИ В БАНКІВСЬКІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ СИСТЕМНИЙ АНАЛІЗ
- П. Біленчук, А. Кофанов, О. Кобилянський
  КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ
- П. Біленчук, А. Кофанов, О. Кобилянський
  КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНІВ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Цапко
  ПРАВОВИЙ СТАТУС І ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ ЗАСАДИ ДІЯЛЬНОСТІ ДЕРЖАВНОГО КАЗНАЧЕЙСТВА УКРАЇНИ
- П. Біленчук, А. Кофанов, О. Кобилянський
  ПРАВОВІ ОСНОВИ ДІЯЛЬНОСТІ ОРГАНІВ ПРАВОПОРЯДКУ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ
- П. Біленчук, А. Кофанов, О. Кобилянський
  ПРАВОВІ ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**П.Д. БІЛЕНЧУК
А.В. КОФАНОВ
О.Л. КОБИЛЯНСЬКИЙ
В.Д. ПОЛИВАНЮК**

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«НАУКОВА БІБЛІОТЕКА КРИМІНАЛІСТА» презентує підручники, монографії, навчальні посібники в таких галузях знань:

- Серія «Людина, право, суспільство»
- Серія «Економіка, фінанси, право»
- Серія «Безпека людини, суспільства, держави»
- Серія «Національна і міжнародна безпека»
- Серія «Міжнародне співробітництво»
- Серія «Мас-медіа»
- Серія «Криміналістична освіта XXI століття»
- Серія «Криміналістична наука в цивільному, арбітражному та кримінальному процесі»
- Серія «Міжнародна і вітчизняна злочинність»
- Серія «Запобігання, протидія, розслідування злочинів»
- Серія «Автоматизація, комп'ютеризація, інформатизація»
- Серія «Зброєзнавство і мисливствознавство»
- Серія «Інформація+Інтелект+Інновація»
- Серія «Електронна фотографія»
- Серія «Криміналістичне забезпечення»
- Серія «Культура, мистецтво, право»
- Серія «Власність, земля, право»
- Серія «Безпекознавство»

Відгуки, рекомендації та пропозиції просимо надсилати за адресою:
03150, Україна, м. Київ,
вул. П.Любченка, 15, оф. 219
або електронною поштою:
E-mail: peregin@mail.ru
Тел. (067) 573-83-07
Тел./факс: (044) 468-31-21

Навчальне видання

Петро Дмитрович БІЛЕНЧУК
Андрій Віталійович КОФАНОВ
Олег Леонідович КОБИЛЯНСЬКИЙ
Василь Дмитрович ПОЛИВАНЮК

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Навчальний посібник

В авторській редакції

Підписано до друку 27.12.2010.
Формат 60×84. Папір офсетний.
Тираж 300 прим.

Видавництво «КИЙ»
Адреса: 0436, Київ-136,
вул. Гречка, 13, кім. 216.

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовників
і розповсюджувачів видавничої продукції
серія ДК № 1168 від 24.12.2002 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ім. ТАРАСА ШЕВЧЕНКА
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПІДГОТОВКИ СЛІДЧИХ І КРИМІНАЛІСТІВ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ, БЕЗПЕКИ ТА ІНФОРМАЦІЙНО-ПРАВОВИХ ТЕХНОЛОГІЙ

П.Д. БІЛЕНЧУК
А.В. КОФАНОВ
О.Л. КОБИЛЯНСЬКИЙ
В.Д. ПОЛИВАНЮК

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Навчальний посібник

Київ 2011

ББК 67.52я73
Б 61

Схвалено та затверджено кафедрою криміналістичної техніки ННІПСК КНУВС та рекомендовано до друку вченою радою Європейського університету управління, безпеки та інформаційно-правових технологій (протокол № 12 від 20.12.2010 року).

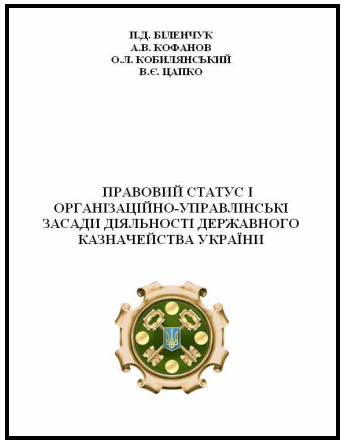
Рецензенти:
Дахно І.І. – доктор економічних наук, професор, завідувач кафедри Міжнародної академії управління персоналом
Котюк І.І. – доктор юридичних наук, професор, завідувач кафедри Київського національного університету імені Тараса Шевченка
Салтинський В.М. – віце-президент Поліцейської фінансово-правової академії, Заслужений юрист України

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Поливанюк В.Д.
Б 61 Основи методики розслідування фінансових злочинів, вчинених з використанням сучасних інформаційних технологій: криміналістичний аналіз банківської системи. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2011. – 80 с. – (Серія «Економіка, фінанси, право»).

В посібнику висвітлюється правове регулювання діяльності кредитно-фінансових установ України, а також системно викладені організаційно-тактичні основи розслідування фінансових злочинів, вчинених з використанням сучасних інформаційних технологій.

Для студентів і викладачів юридичних навчальних закладів.

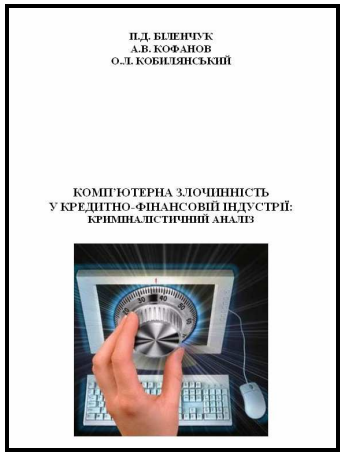
ББК 67.52я73



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Цапко В.Є. Правовий статус і організаційно-управлінські засади діяльності Державного казначейства України. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2011. – 76 с. – (Серія «Економіка, фінанси, право»).

У навчальному посібнику висвітлено правове регулювання і організаційні основи діяльності державного казначейства України.

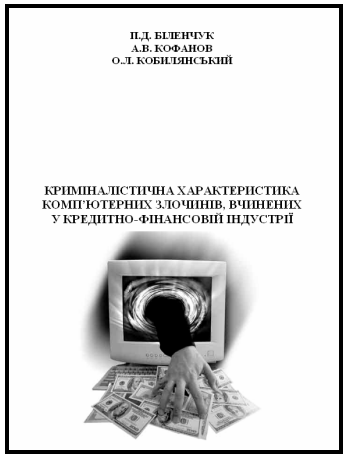
Для студентів і викладачів юридичних навчальних закладів.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л. Комп'ютерна злочинність у кредитно-фінансовій індустрії: криміналістичний аналіз. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2011. – 50 с. – (Серія «Економіка, фінанси, право»).

У навчальному посібнику подається криміналістичний аналіз комп'ютерної злочинності у кредитно-фінансовій індустрії.

Для студентів і викладачів юридичних навчальних закладів.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л. Криміналістична характеристика комп'ютерних злочинів, вчинених у кредитно-фінансовій індустрії. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2011. – 68 с. – (Серія «Економіка, фінанси, право»).

У навчальному посібнику аналізується криміналістична характеристика комп'ютерної злочинності.

Для студентів і викладачів юридичних навчальних закладів.

преступлений. // Вестник Московского государственного университета. Серия 11. Право. – 1999. – № 1.

270. Яблоков Н.П. Основы методики расследования финансовых преступлений. // Вестник Московского государственного университета. Серия 11. Право. – 1999. – № 2.

271. Яблоков Н.П., Колдин В.Я. Криминалистика: Учебник. – М.: МГУ, 1990. – 846 с.

272. Ясинов И.И., Мацько И.Г., Зубова Н.О., Чугуров И.Н. О предмете экспертизы средств электронно-вычислительной техники и программного обеспечения // Тезисы научно-практической конференции. – К., 1993. – С. 213.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АБС	Автоматизована банківська система
АРМ	Автоматизоване робоче місце
БЕЗ	Боротьба з економічними злочинами
БСУ	Банківська система України
ДНДЕКЦ	Державний науково-дослідний експертно-криміналістичний центр
ЕОМ	Електронна обчислювальна машина
ЕЦП	Електронний цифровий підпис
ЖМД	Жорсткий магнітний диск
ЗЕОТ	Засоби електронно-обчислювальної техніки
ІС	Інформаційна система
КК	Кримінальний кодекс
КПК	Кримінально-процесуальний кодекс
КР	Кримінальний розшук
МВС	Міністерство внутрішніх справ
МНІ	Машинний носій інформації
НБУ	Національний банк України
НІТ	Науково-інформаційні технології
НСД	Несанкціонований доступ
НЦБ	Національне центральне бюро
ОВС	Органи внутрішніх справ
ОДБ	Операційний день банку
ОЗГ	Організована злочинна група
ОЗУ	Оперативний запам'ятовуючий устрій
ОРЗ	Оперативно-розшукові заходи
ПЕМВН	Побічне електромагнітне випромінювання і наводки
ПЕОМ	Персональна електронно-обчислювальна машина
ПКНСД	Потенційні канали несанкціонованого доступу
РРП	Регіональна розрахункова палата
СБУ	Служба безпеки України
СЕП	Система електронних платежів
СКР	Спеціальний картковий рахунок
СОГ	Слідчо-оперативна група
СУБД	Система управління базою даних
ТЗІ	Технічний захист інформації
ЦРП	Центральна розрахункова палата

Навчально-практичний посібник. – К.: Кантрі Лайф, 2003. – 65 с.

253. Чернявський С.С. Злочини у сфері банківського кредитування (проблеми розслідування та попередження): Навч. посіб. / О.М. Джужа (заг.ред.). – К.: Юрінком Інтер, 2003. – 264 с.

254. Шевченко Б.И. Теоретические основы трассологической идентификации в криминалистике. М.: МГУ, 1975.

255. Шепитько В.Ю. Тактика расследования преступлений, совершаемых организованными группами и преступными организациями. – Харьков, 2000. – 88 с.

256. Шепитько В.Ю. Теория криминалистической тактики: Монография. – Харьков: Гриф, 2002. – 349 с.

257. Шепітько В.Ю. Криміналістика: криміналістична практика і методика розслідування злочинів: Підручник для студентів юридичних вузів і факультетів. – Х., 1998. – 375 с.

258. Шепітько В.Ю. Тактика огляду місця події: Конспект лекції. – Х., 1994. – 19 с.

259. Шилан Н.Н., Кривонос Ю.М., Г.М. Бирюков Компьютерные преступления и проблемы защиты информации. – Луганск: РИО ЛИВД, 1999. – 64 с.

260. Шурухнов Н.Г. Криминалистическая характеристика преступлений // Криминалистика (актуальные проблемы). Под ред. Е.И. Зуева. – М., 1988. – С. 119.

261. Шурухнов Н.Г. Расследование краж: Практ. пособие. – М.: Юристъ, 1999. – 112 с.

262. Шурухнов Н.Г., Левченко И.П., Лучин И.Н. Специфика проведения обыска при изъятии компьютерной информации // Актуальные проблемы совершенствования деятельности ОВД в новых экономических и социальных условиях. – М., 1997. – С.28-30.

263. Щелгунов В.Г. Виды компьютерных преступлений // Российский следователь. – 2003. – №1. – С. 20-21.

264. Щербаковский М.Г., Кравченко А.А. Применение специальных знаний при раскрытии и расследовании преступлений. – Х., 1999. – 78 с.

265. Щербаковський М.Г., Коршенко В.А. Проблеми залучення фахівця при розкритті та розслідуванні комп'ютерних злочинів // Теорія та практика криміналістичного забезпечення розкриття та розслідування злочинів у сучасних умовах: Тези доп. міжнарод.наук.-практ. конференції. – К.: НАВСУ,2001. – Ч. 1. – С. 110-113.

266. Щербаковський М.Г., Коршенко В.А. Проблеми застосування спеціальних знань при розкритті та розслідуванні комп'ютерних злочинів // Матеріали міжвузівської науково-практичної конференції. – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 171.

267. Эриашвили Н.Д. Банковское право: Учебник для вузов. – М.: Закон и право, ЮНИТИ – ДАНА, 1999. – 383 с.

268. Юридична енциклопедія. – К.: Українська енциклопедія, 1998, Т.1. – 670 с.

269. Яблоков Н.П. Криминалистическая характеристика финансовых

// Применение специальных познаний в борьбе с преступностью. – Свердловск, 1983. – С. 3-10.

237. Старушкевич А.В. Організація огляду місця події // Вісник прокуратури. – 2003. – № 13. – С. 77-87.

238. Сушко Ю. Використання спеціальних знань судових експертів-економістів для профілактики правопорушень в сфері економіки. // Право України. – 1997. – № 7.

239. Танасевич В.Г. Криминалистическое понятие раскрытия преступления. // Социалистическая законность. – 1975. – № 10. – С. 57-58.

240. Танасевич В.Г., Образцов В.А. О криминалистической характеристике преступлений. // Вопросы борьбы с преступностью. – М., 1976. – Вып.25. – С. 94-105.

241. Тіньова економіка та організована економічна злочинність: Навчальний посібник. – К., 1999. – 462 с.

242. Толеубекова Б.Х. Использование специальных бухгалтерских познаний при расследовании уголовных дел о хищениях социалистического имущества. – М., 1988. – 21 с.

243. Указ Президента України № 1229 від 27.09.1999 «Про положення Про технічний захист інформації в Україні» Із змінами, внесеними згідно з Указом Президента України № 1120 від 06.10.2000.

244. Указ Президента України № 928 від 31 липня 2000 року «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпеченню широкого доступу до цієї мережі в Україні» // Офіційний вісник України. – 2000. – №31. – ст. 1300.

245. Устинова Т. Ответственность за незаконную предпринимательскую и банковскую деятельность. // Законность. – 1999. – № 7.

246. Федоров В.В. Компьютерные преступления: выявление, расследование и профилактика // Законность. – 1994. – № 6. – С. 45-46.

247. Финансово-кредитный словарь: В 3-х т. – Т. 2./ Гл. ред. В.Ф. Гарбузов. – М.: Финансы и статистика, 1986. – 511 с.

248. Цимбалюк В. Проблеми латентності комп'ютерної злочинності // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2000. – С. 57-61.

249. Цимбалюк В.С. Кримінологічні аспекти вчинення правопорушень у сфері міжнародних економічних відносин із застосуванням інформаційних комп'ютерних технологій // Збірник наукових праць Харківського центру з виявлення організованої злочинності спільно з Американським університетом м. Вашингтон. – Х., 2002. – Випуск № 6. – 308 с. – С. 234-260.

250. Цимбалюк В.С. Латентність комп'ютерної злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 3. – С. 178.

251. Цимбалюк В.С., Іванова Т.С. Захист електронних засобів від несанкціонованого доступу: Навчально-методичний посібник. – Ірпінь: УФЕІ, 1998.

252. Ціркаль В.В. Участь спеціаліста при проведенні слідчих дій. Кримінально-процесуальні, організаційні й криміналістичні аспекти.

ПЕРЕДМОВА: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ДІЯЛЬНОСТІ КРЕДИТНО-ФІНАНСОВИХ УСТАНОВ

Дослідження окремих аспектів методики розслідування злочинів, вчинених у кредитно-фінансовій системі з використанням сучасних інформаційних технологій проводилися А.Б. Агаповим, Н.М. Ахтирською, П.Д. Біленчуком, В.Б. Вєховим, В.К. Весельським, В.Д. Гавловським, В.О. Голубєвим, М.В. Гуцалюком, Р.А. Калюжним, В.Є. Козловим, В.В. Криловим, В.А. Мінаєвим, О.І. Мотняхом, Л.П. Паламарчук, О.Р. Росинською, О.П. Снігерьовим, В.С. Цимбалюком, В.М. Черкасовим, С.С. Чернявським, М.Г. Шурухновим, О.М. Юрченком та іншими.

Тому в даному навчальному посібнику зроблена спроба комплексного дослідження особливостей методики розслідування злочинів, вчинених у кредитно-фінансовій системі України з використанням сучасних інформаційних технологій, що грунтується на теоретичних концепціях криміналістики і узагальненнях слідчої, експертної та судової практики. У роботі пропонуються нові теоретичні положення та практичні рекомендації щодо організації запобігання, протидії, розслідування даних злочинів.

Основними методами дослідження, що використовувалися при підготовці даної праці є: метод системного аналізу, який використовувався, зокрема, у процесі вивчення законодавчих норм, що регулюють банківську діяльність та діяльність у сфері обігу інформації та інформаційних технологій; історико-правовий метод, використання якого дало можливість показати розвиток законодавства України та ряду зарубіжних країн у сфері захисту банківської інформації на різних етапах розвитку суспільства; статистичний метод забезпечив обґрунтування теоретичних положень роботи зі статистичною інформацією; соціологічний метод застосовувався при вивченні архівних кримінальних справ, проведенні анкетування серед працівників дізнання та досудового слідства й обробці отриманих даних.

Теоретичним підґрунтям дослідження стали праці провідних науковців: О.Я. Баєва, Т.В. Варфоломеєвої, А.Ф. Волобуєва, В.Г. Гончаренка, Ю.М. Грошевого, А.Я. Дубинського, Н.І. Клименко, І.П. Козаченка, В.О. Коновалової, М.В. Костицького, В.Г. Лукашевича, В.Т. Маляренка, Г.А. Матусовського, О.Р. Михайленка, М.М. Міхеєнка, М.В. Салтевського, М.Я. Сегая, В.В. Тіщенка, В.Ю. Шепітька, М.Є. Шумила та ін.

Метою даної праці є розроблення на основі теорії криміналістичної методики, узагальнення практики банківської діяльності, аналізу слідчої практики основних положень методики розслідування злочинів, вчинених у кредитно-фінансовій системі з використанням сучасних інформаційних технологій.

Зазначена мета зумовила визначити такі завдання дослідження:

– вивчити основні положення правового регулювання банківської діяльності в Україні та в ряді країн світу, провести їх порівняльний аналіз;

– узагальнити нормативно-правові акти, що регулюють банківську

діяльність та регламентують діяльність в сфері інформаційних технологій;

– на підставі вивчення і узагальнення матеріалів кримінальних справ, аналізу судових експертиз, опублікованої слідчої практики, статистичних даних дослідити та виявити механізм і способи вчинення злочинів в кредитно-фінансовій системі України з використанням інформаційних технологій, встановити їх основні ознаки;

– розробити рекомендації щодо висунення слідчих версій, організації та планування розслідування;

– сформулювати пропозиції щодо системи тактичних прийомів, особливості проведення окремих слідчих дій;

– розробити основні положення особливості методики розслідування злочинів, вчинених у кредитно-фінансовій системі України з використанням сучасних інформаційних технологій.

Архітектоніка роботи складається з двох розділів.

У підрозділі 1.1. «Особливості порушення кримінальної справи та проведення першочергових слідчих дій при розслідуванні фінансових злочинів, вчинених з використанням сучасних інформаційних технологій» виділені деякі типові слідчі ситуації, версії та алгоритми проведення першочергових слідчих дій.

На основі проведеного аналізу наукових праць та узагальнення слідчої і судової практики нами виділені такі типові слідчі ситуації, а саме:

Ситуація 1. Власник або користувач комп'ютерної мережі (бази даних) або кредитної картки власними силами виявив факт незаконного проникнення та інших протиправних дій, виявив винну особу і заявив про це в правоохоронні органи.

Ситуація 2. Власник або користувач комп'ютерної мережі (бази даних) інформаційної системи або кредитних карток виявив факт незаконного проникнення та інших протиправних дій, але не зміг встановити винну особу і заявив про це в правоохоронні органи.

Ситуація 3. Інформація про незаконне проникнення в комп'ютерну мережу та інші вчинені протиправні дії стали загальновідомими або були встановлені в ході проведення оперативно-розшукових заходів.

Виходячи з позначених типових слідчих ситуацій пропонуємо висунути такі загальні слідчі дії.

Версія 1. Злочин вчинений співробітником даної установи або особою, що входить у коло родичів, друзів, знайомих співробітників установи, іншою особою, що має доступ до комп'ютерної техніки в даній установі.

Версія 2. Злочин вчинений за попередньою змовою групою осіб або злочинним співтовариством за участю співробітника даної установи.

Версія 3. Злочин вчинений особою або групою осіб, не пов'язаних з діяльністю даної установи.

На підставі проведеного дослідження ми прийшли до висновку, що на початковому етапі розслідування необхідно проводити такі першочергові слідчі дії:

– огляд місця події, що включає й огляд програмного продукту та комп'ютерної техніки;

внутрішніх справ. - 1998. - №1. – С.160-167.

221. Салтевский М.В., Щербаковский М.Г., Губанов В.А. Осмотр компьютерных средств на месте происшествия: Методологические рекомендации. – Харків.: Нац. юрид. акад. України, 1999. – 38 с.

222. Салтевський М.В., Губанов В.А. Использование следов сети интернет в раскрытии экономических преступлений // Вісник Луганського інституту внутрішніх справ: Спеціальний випуск. – 1999. Частина 1. – С. 67-74.

223. Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ: Навчальний посібник. – Х., 2000. – 35 с.

224. Самойленко О.А. Особливості предмета корисливих злочинів, вчинених із використанням комп'ютерних технологій // Підприємництво, господарство та право. – К.: ТОВ «Гарантія», 2005. – № 8. – С. 153-155.

225. Самойленко О.А. Особливості розслідування викрадень майна, вчинених із використанням комп`ютерних технологій: Дис... канд. юрид. наук: 12.00.09. – Донецьк, 2006. – 250 с.

226. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью // Законность. – 1993. – № 8. – С. 36-40.

227. Семенов Н.В., Мотуз О.В. Судебно-кибернетическая экспертиза - инструмент борьбы с преступностью XXI века // Конфидент. – СПб, 1999. – № 1-2. – С. 11.

228. Сергеев В.В. Компьютерные преступления в банковской сфере //Банковское дело. – 1997. – № 2. – С. 27-28.

229. Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Селиванова Н.А., Снеткова В.А. – М.: БЕК, 1997. – 432 с.

230. Снігерьов О.П., Голубєв В.О. Проблеми класифікації злочинів у сфері комп'ютерної інформації // Вісник університету внутрішніх справ. – Вип. 5. – Харків., 1999. – С. 25-28.

231. Снігерьов О.П., Кухарьонок М.А. Визначення можливих каналів витоку інформації в автоматизованих системах // Інформаційні технології та захист інформації. – Запоріжжя: Юридичний інститут МВС України, 1998. – № 1. – С. 59.

232. Советская криминалистика: методика расследования отдельных видов преступлений. / Под ред. Лисиченко В.К.. – К., 1988. – 405 с.

233. Сокиран Ф.М. Научно-технические средства как элемент психологического воздействия на предварительном следствии // Актуальные проблемы обеспечения следственной практики научно-техническими достижениями: Межвуз. сб-к научн. тр. – К.: НИ и РИО Киевской высшей школы МВД СССР им. Ф.Э. Дзержинского, 1987. – С. 63-66.

234. Сологуб Н.М., Евдокимов С.Т., Данилова Н.А. Хищения в сфере экономической деятельности: механизм преступления и его выявление: Методическое пособие. – М.: ПРИОР, 2002. – 256 с.

235. Сорокин В.С. Обнаружение и фиксация следов на месте происшествия. – М., 1966. – 103 с.

236. Сорокотягин И.Н. Системно-структурная характеристика специальных познаний и формы их использования в борьбе с преступностью.

205. Попович В.М. Тіньова економіка як предмет економічної кримінології. – К., 1998. – 447 с.

206. Постанова Кабінету Міністрів України «Про деякі питання захисту інформації, охорона якої забезпечується державою» від 13 березня 2002 року № 281.

207. Постанова Кабінету Міністрів України № 1126 від 08.10.97 «Про затвердження Концепції технічного захисту інформації в Україні» // Збірка нормативних документів системи технічного захисту інформації. – 1997. – № 4. – С. 2-13.

208. Постанова Кабінету Міністрів України № 632 від 09.09.94 «Про затвердження Положення про технічний захист інформації в Україні» // Збірка нормативних документів системи технічного захисту інформації. – 1997. – № 4. – С. 14-41.

209. Постанова Правління Національного Банку України «Про затвердження положення про порядок емісії платіжних карток і здійснення операцій з їх застосуванням».

210. Постанова Правління Національного банку України № 135 від 29 березня 2001р. «Про затвердження Інструкції про безготівкові розрахунки в Україні в національній валюті».

211. Постанова Правління Національного банку України № 621 від 27 грудня 1999р. «Про затвердження Інструкції про міжбанківські розрахунки в Україні».

212. Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие / Под ред. Шурухнова Н.Г. – М. : Щит-М, 1999. – 254 с.

213. Расследование хищений государственного или общественного имущества (Проблемы тактики и методики). – Х: Вища школа, 1987. – 168 с.

214. Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Дис. ... канд. юрид. наук. Волгоград: ВЮИ МВД России, 1998. – 286 с.

215. Розенфельд Н. Загальна характеристика умисних комп'ютерних злочинів // Право України. – 2002. – № 10. – С. 88-93.

216. Россинская Е.Р. Судебная экспертиза в уголовном, гражданском, арбитражном процессе. – М.: Право и закон, 1996. – 224 с.

217. Рябов О.А. Особливості фіксації та вилучення комп'ютерних засобів при проведенні слідчих дій // Матеріали міжвузівської науково-практичної конференції. – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 176.

218. Савченко А.А., Лазуренко Ю.В. Особенности выявления и раскрытия корыстных преступлений, совершаемых с использованием автоматизированных систем // Матеріали міжвузівської науково-практичної конференції. – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 19.

219. Салтевский М.В. Основы методики расследования легализации денежных средств, нажитых незаконно: Конспект лекций. – Х.: Б.и., 2000. – 18 с.

220. Салтевский М.В., Дьяченко А.Ф., Губанов В.А. Проблемы судебной компьютерно-технической экспертизы // Вісник Луганського інституту

– огляд і аналіз наявної інформації в програмних продуктах, машинних носіях та кредитних картках;

– допити свідків, потерпілих, підозрюваних (обвинувачуваних);

– обшук;

– призначення експертизи.

У підрозділі 1.2. «Тактичні особливості проведення окремих слідчих дій при розслідуванні фінансових злочинів, вчинених з використанням сучасних інформаційних технологій» нами розглянуті основні першочергові слідчі дії, які необхідно проводити при розслідуванні злочинів, вчинених у кредитно-фінансовій системі України з використанням сучасних інформаційних технологій.

По справах про комп'ютерні злочини в кредитно-фінансовій сфері дуже важливо правильно вирішити питання про вихідну точку огляду місця події. У тактичному відношенні найбільш доцільною виправною точкою, на нашу думку, буде конкретний (встановлений оперативним або іншим шляхом) засіб електронно-обчислювальної техніки (ЗЕОТ) із комп'ютерною інформацією, що виступає як предмет або знаряддя вчинення злочину, що має максимально інформативні й численні сліди злочинної діяльності.

В роботі зазначається, що важливою слідчою дією при розслідуванні такого виду злочинів є обшук. Основна проблема, що виникає в ході проведення обшуку полягає в тому, що суб'єкт, який проводить обшук, не може безпосередньо оглянути вміст машинного носія, оскільки останнє являє собою, як правило, деяку намагнічену частину магнітного носія. Для вирішення даного завдання потрібно використовувати деяку проміжну ланку, що дозволяє суб'єкту, який проводить обшук, всебічно й об'єктивно оцінити інформацію, що міститься на машинному носієві, тому питання про використання в ході проведення слідчих дій програмних засобів є важливими.

На підставі узагальнення слідчої практики нами виділені такі особливості проведення допиту свідків. Коло осіб та послідовність їх допиту залежить від обсягу даних, які вони можуть мати, і сформованої на даний момент слідчої ситуації.

Позитивних результатів можна домогтися шляхом участі у допиті відповідних спеціалістів і експертів. У ході його проведення вони можуть відігравати активну роль – давати кваліфіковані пояснення по всіх виникаючих спеціальних питаннях; задавати з дозволу слідчого відповідні питання допитуваному, не виходячи за межі своєї компетенції.

В посібнику детально розглядаються особливості призначення деяких видів судових експертиз, зокрема, техніко-криміналістична експертиза документів, виготовлених з використанням друкуючих засобів електронно-обчислювальної техніки і нових технологій, є новим видом експертних досліджень, які успішно використовуються в слідчо-судовій практиці із середини 90-х років минулого століття.

Розглянута експертиза комплексна, оскільки для вирішення деяких питань у процесі дослідження об'єктів необхідно застосовувати методики, що ґрунтуються на знаннях криміналістики, сучасної поліграфії, матеріалознавства, інформатики, електроніки, кібернетики й нейробіоніки.

В роботі визначені завдання, які може вирішувати програмно-технічна експертиза:

– відтворення та роздрукування усієї або частини комп'ютерної інформації, що міститься на машинних носіях, у тому числі та, яка знаходиться в нетекстовій формі;

– відновлення комп'ютерної інформації, що раніше містилася на машинних носіях, але згодом стертої (знищеної) або зміненої (модифікованої) з різних причин;

– встановлення дати й часу створення, зміни (модифікації), стирання, пошкодження, знищення або копіювання тієї чи іншої інформації;

– розшифровка закодованої інформації, підбирання паролів і розкриття системи захисту ЗЕОТ;

– дослідження ЗЕОТ щодо наявності в них програмно-апаратних модулів і модифікацій, що приводять до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі (шкідливих засобів або вірусів);

– встановлення авторства, місця підготовки і способу виготовлення документів (файлів, програм), що знаходяться на машинному носієві інформації;

– з'ясування можливих каналів витоку інформації з комп'ютерної мережі, конкретних ЗЕОТ і приміщень; встановлення можливих несанкціонованих способів доступу до охоронюваної законом комп'ютерної інформації та її носіїв;

– з'ясування технічного стану, справності ЗЕОТ, оцінки їх зношування, а також індивідуальних ознак адаптації ЗЕОТ під конкретного користувача;

– встановлення рівня професійної підготовки окремих осіб, що проходять у справі, в галузі програмування та як користувача;

– встановлення конкретних осіб, що порушили правила експлуатації ЕОМ, системи ЕОМ або їх мережі;

– встановлення причин і умов, що сприяють вчиненню даного виду злочину.

Варто зверну увагу на ту обставину, що специфічними об'єктами дослідження даної експертизи є спеціальні технічні засоби, запрограмовані для негласного одержання інформації, а також цифрові засобі електрозв'язку.

В роботі зазначається, що комплексна судово-бухгалтерська і програмно-технічна експертиза є типовою слідчою дією у справах про комп'ютерні злочини в кредитно-фінансовій сфері та повинна призначатися для вирішення таких завдань:

– перевірка і процесуальна фіксація даних, викладених у матеріалах ревізій, інвентаризацій та інших контрольно-перевірочних актах;

– встановлення часу утворення (виникнення) шкоди;

– встановлення конкретної особи, якій була заподіяна шкода;

– перевірка обґрунтованості автоматизації тих чи інших операцій, технологічних циклів або процесів;

– використання тих чи інших ЗЕОТ з цією метою;

– перевірка правильності проведення бухгалтерсько-документальних операцій з використанням ЗЕОТ;

// Вісник Запорізького юридичного інституту МВС України. – Запоріжжя, 2001. – № 2. – С. 200-207.

195. Поливанюк В.Д. Основи банківської діяльності щодо автоматизації електронних розрахунків // Держава та регіони. Серія: Право. – Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. – № 1. – С. 62-66.

196. Поливанюк В.Д. Особа злочинця як елемент криміналістичної характеристики злочинів, вчинених у банківській системі України з використанням інформаційних технологій // Криміналістичні та процесуальні проблеми, що виникають під час проведення слідчих дій: Матеріали міжнародної науково-практичної конференції. Донецьк, 24 листопада 2006 року. – Донецьк: ООО Норд Комп'ютер, 2006. – С. 523-527.

197. Поливанюк В.Д. Поняття криміналістичної характеристики комп'ютерного злочину // Збірник наукових праць Третьої Міжнародної конференції «Інформаційні технології та безпека» 23-27 червня 2003 р. м. Партеніт. – Київ: Інститут проблем реєстрації інформації НАН України, 2003. – Випуск 3. – С. 141-150.

198. Поливанюк В.Д. Проведення слідчих дій щодо огляду та вилучення комп'ютерної інформації та комп'ютерної техніки // Вісник Академії праці та соціальних відносин ФПУ. – Київ, 2002. – № 2. – С. 196-199.

199. Поливанюк В.Д. Розвиток способів вчинення злочинів у банківській системі України з використанням інформаційних технологій // Проблеми державотворення і захисту прав людини в Україні: Матеріали X регіональної науково-практичної конференції. 5-6 лютого 2004 р. – Львів: Юридичний факультет Львівського національного університету імені Івана Франка, 2004. – С. 426.

200. Поливанюк В.Д. Тактичні особливості проведення допиту при розслідуванні злочинів, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж // Матеріали Всеукраїнської науково-практичної конференції «Теоретичні та практичні проблеми організації досудового слідства». 20-21 травня 2005 року м. Запоріжжя: У 2 ч. – Запоріжжя: Юридичний інститут МВС України, 2005. – Ч.1. – С. 79-81.

201. Поливанюк В.Д., Ращенко Є.М. Криміналістичні особливості комп'ютерних злочинів // Вісник Запорізького юридичного інституту МВС України. – Запоріжжя, 2004. – № 2. – С. 267–272.

202. Положення Правління Національного Банку України «Про впровадження пластикових карток міжнародних платіжних систем у розрахунках за товари, надані послуги та при видачі готівки».

203. Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 1994 р. № 632 // Збірка нормативних документів системи технічного захисту інформації. – Державний комітет України з питань державних секретів та технічного захисту інформації, 1997. – № 4. – С. 15-41.

204. Попович В.М. Правові основи банківської справи та її захист від злочинних посягань: Настільна книга з питань банківської та підприємницької економічної безпеки. – К., 1995. – 325 с.

технических экспертиз: Методические рекомендации / В.С. Зубаха и др. – М: ГУ ЭКЦ МВД России, 2001. – 72 с.

181. Орлов С.А. Международно-правовые аспекты борьбы с преступлениями в сфере компьютерных технологий // Матеріали міжвузівської науково-практичної конференції. – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 37.

182. Осмотр компьютерных средств на месте происшествия: Методические рекомендации. / Салтевский М.В. – К., 1999. – 11 с.

183. Основы борьбы с организованной преступностью / Под ред. В.С. Овчинского, В.Е. Эминова, Н.П. Яблокова. – М.: ИНФРА-М, 1996. – 400 с.

184. Особенности расследования тяжких преступлений (руководство для следователей) / Отв. ред. Б.П. Смагоринский, А.А. Закатов. – Волгоград, 1995. – 200 с.

185. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: Дис... канд. юрид. наук: 12.00.09. – К., 2004. – 214 с.

186. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: Автореф. дис. ... канд. юр. наук: 12.00.09. – К., 2005. – 18 с.

187. Панов Н.И. Уголовно-правовое значение способа совершения преступления. – Х., 1984. – 111 с.

188. Пастухов И., Яни П. Невозвращение валюты из-за границы: проблемы квалификации. // Законность. – 1999. – № 5.

189. Першиков В.И., Савинков В.М. Толковый словарь по информатике. – М.: Фин. и стат., 1991. – 536 с.

190. Поливанюк В.Д. Банківська безпека: правові, організаційні та методичні засади // Актуальні проблеми сучасної науки і правоохоронної діяльності / Матеріали IX науково-практичної конференції курсантів та слухачів. – Національний ун-т внутр.справ: Харків, 2002. – С. 262-263.

191. Поливанюк В.Д. Криміналістична характеристика злочинів, скоєних у банківській системі України з використанням сучасних інформаційних технологій // Вісник Запорізького юридичного інституту МВС України. – Запоріжжя, 2002. – № 2. – С. 233-241.

192. Поливанюк В.Д. Криміналістична характеристика злочинів, скоєних у кредитно-фінансовій системі України з використанням сучасних інформаційних технологій // Актуальні проблеми боротьби зі злочинністю на етапі реформування кримінального судочинства: Матеріали Всеукраїнської науково-практичної конференції 14-15 травня 2002 р. м. Запоріжжя: У 2 ч. – Запоріжжя: Юридичний інститут МВС України, 2002. – ч.2. – С. 75-78.

193. Поливанюк В.Д. Криміналістичне дослідження пластикових карток // Криміналістика: Підручник. / За ред. П.Д. Біленчука. – 2-ге вид., випр. і доп. – К: Атіка, 2001. – С. 211-227.

194. Поливанюк В.Д. Нові способи розрахунків – нові способи шахрайств

– ведення електронного документообігу;

– виявлення фактів порушення встановлених для конкретної організації (підприємства, установи) правил ведення електронного документообігу, технології виробництва, експлуатації ЗЕОТ, захисту ЗЕОТ та комп'ютерної інформації;

– визначення причин та умов, що сприяли вчиненню комп'ютерного злочину в банківській сфері.

Необхідно підкреслити, що перелік розглянутих вище слідчих дій та експертних досліджень не є вичерпним. Результати проведеного аналізу даної проблеми показують, що саме вони є найбільш специфічними й значимими для розслідування комп'ютерних злочинів у кредитно-фінансовій системі, особливо на початковому етапі досудового розслідування.

У підрозділі 1.3. «Сутність та межі спеціальних знань, які використовуються при дослідженні електронних документів на досудовому слідстві» обґрунтована думка про те, що поява в переліку доказів по кримінальних справах документів на машинних магнітних носіях інформації потребує по-новому розглянути проблему використання спеціальних знань при розслідуванні «комп'ютерних» злочинів, вчинених в кредитно-фінансовій системі України.

Слідча практика засвідчує, що на початковому етапі розслідування повинні використовуватися такі спеціальні знання спеціаліста:

– при підготовці до проведення окремих слідчих дій: для наукового консультування слідчого з питань визначення «комп'ютерної» специфіки слідчої дії, визначення її конкретної мети, способів і прийомів їх досягнення; для надання допомоги слідчому при підборі понятих, що мають відповідну підготовку в галузі комп'ютерних технологій, для адекватного сприйняття ними проведених слідчим і спеціалістом окремих дій;

– при огляді місця події, обшуку і виїмці: для виявлення засобів комп'ютерної техніки, які використовувались зі злочинною метою, її окремих компонентів, документації, інших об'єктів, які можуть містити сліди неправомірних дій; для коректного завершення роботи програм або контролю за ними; для наступного коректного відключення засобів комп'ютерної техніки від енергопостачання; для надання допомоги слідчому в описі специфічних ознак засобів комп'ютерної техніки, що вилучають, її окремих компонентів і документації; для надання допомоги слідчому при вирішенні питання визначення конкретного комплекту комп'ютерної техніки або окремих її компонентів, що підлягають вилученню або ізолюванню від вільного доступу; для надання допомоги слідчому в підготовці засобів комп'ютерної техніки до транспортування (їх упаковки, опечатуванні);

– при допиті, очній ставці, відтворенні обстановки і обставин події: для надання допомоги слідчому при його спілкуванні з особою, що використовує професійну «комп'ютерну» термінологію тощо [1-16].

Другий розділ роботи присвячений правовому регулюванню діяльності кредитно-фінансових установ України.

Таким чином, читачам пропонується оригінальне дослідження, присвячене новітнім проблемам, які вивчає сьогодні сучасна криміналістика.

РОЗДІЛ 1
ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ОСНОВИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1. Особливості порушення кримінальної справи та проведення першочергових слідчих дій при розслідуванні фінансових злочинів, вчинених з використанням сучасних інформаційних технологій

Вєхов В.Б. та Скромніков К.С. [38; 229] справедливо вважають, успіх розслідування злочинів у банківській системі, що вчинюються з використанням комп'ютерної техніки, прямо залежить від того, як швидко після вчинення суспільно небезпечного діяння почате досудове розслідування. Р.С. Бєлкін зазначає, що успішність розслідування злочинів залежить не тільки від методично правильного підходу до процесу розслідування, але й від оперативності дій, уміння організувати сили й засоби, які є у розпорядженні органів, що ведуть боротьбу зі злочинністю. Саме тому при розробці криміналістичної методики повинні враховуватися можливості оперативних апаратів органів внутрішніх справ, експертних установ і громадських організацій, які можуть бути використані з метою розслідування злочинів [21, с. 307]. На нашу думку, особливу актуальність і значимість отримує початкова стадія кримінального процесу, під якою розуміється порушення кримінальної справи. Специфіка даного етапу багато в чому обумовлена кримінально-правовою природою злочинів, що розглядаються, і тим, що всі дії, що складають цю стадію, проводяться до порушення кримінальної справи.

Виділяючи необхідність обов'язкової участі спеціаліста в галузі обчислювальної техніки й програмування, відзначимо, що проведене нами опитування слідчих і зазначених спеціалістів показало: тільки 14% слідчих працюють на ЕОМ на рівні користувача й 56% не знають нічого про принципи роботи ЕОМ. З іншого боку, 92% із числа програмістів вважають, що на сучасному рівні розвитку обчислювальної техніки без участі професіонала знайти в комп'ютері «захована» інформацію без побоювання знищити необхідні дані вкрай складно [106, с. 15-18]. Участь відповідного спеціаліста необхідна також і при проведенні допитів та інших слідчих дій, на яких з'ясовуються технічні аспекти вчиненого злочину.

На підставі викладеного, можна зробити висновок про те, що ефективність роботи слідчого щодо розкриття й розслідування комп'ютерних злочинів у банківській системі, у першу чергу, залежить від оперативності реагування на заяви й повідомлення про факти їх вчинення, своєчасного й обгрунтованого порушення за такими фактами кримінальних справ.

Затягнення з початком проведення першочергових слідчих дій може привести до втрати важливих доказів, безкарності злочинців, збільшенню строків досудового розслідування й інших негативних наслідків. Неухильне виконання приписів закону в стадії порушення кримінальної справи

пособие. – К., 1988. – 88 с.

164. Матусовский Г.А. Проблемы совершенствования методики расследования преступлений // Актуальные проблемы формирования правового государства: Краткие тезисы докл. и науч. сообщ. респ. науч. конф. 24-26 окт. 1990. – Х., 1990 – С. 280-282.

165. Матусовский Г.А. Экономические преступления: криминалистический анализ. – Х.: Консум, 1999. – 478 с.

166. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 364 с.

167. Методика расследования хищений социалистического имущества / отв. ред В.Г. Танасевич. – Вып 1. Общие вопросы расследования хищений: Метод. рекомендации / Всесоюзный институт по изучению причин и разработке мер предупреждения преступности. – М., 1976. – 189 с.

168. Методическое пособие по расследованию преступлений в сфере информации и осуществления прокурорского надзора за исполнением закона при их расследовании // Генпрокуратура РФ НИИ проблем укрепления законности и правопорядка. – М.: Б. и., 2001. – 50 с.

169. Методы и средства защиты информации: Методические указания. – К: КМУГА, 1997. – 38 с.

170. Модогоев А.А., Цветков С.И. Организация и криминалистическая методика расследования экономических преступлений: Учебное пособие / Академия МВД СССР. – М., 1990. – 87 с.

171. Моісеєв Є.М. Залучення спеціаліста до розслідування комп'ютерних злочинів // Матеріали міжвузівської науково-практичної конференції. – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 81.

172. Моторыгин Ю.Д. Исследование информации на гибких магнитных дисках // Компьютерная преступность: состояние, тенденции и превентивные меры ее профилактики. Ч. 3. – СПб.: Изд-во СПб ун-та МВД России, 1999. – С. 106-107.

173. Надгорный Г.М. Гносеологические аспекты понятия «специальные знания» // Криминалистика и судебная экспертиза. – 1980. – Вып. 21. – С. 37-42.

174. Настільна книга слідчого / Колектив авторів. Керівник Панов М.І. – К.: Видавничий Дім «Ін Юре», 2003. – 715 с.

175. Науково-практичний коментар до Кримінального кодексу України / За заг. ред. М.О. Потебенька, В.Г. Гончаренка. – К.: Форум, 2001. – 942 с.

176. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року / За ред. М.І. Мельника, М.І. Хавронюка. – К.: Канон, 2001. – 1104 с.

177. Науково-практичний коментар Кримінально-процесуального кодексу України. – К., 1997. – 624 с.

178. Никульшина О.Г. Исследование банковских документов-доказательств путем производства судебно-бухгалтерской, финансово-экономической, налоговедческои, компьютерно-технической экспертизы // Следователь. – 2002. – №7. – С. 30-32.

179. Образцов В.А. Криминалистика: Курс лекций. – М., 1996. – 448 с.

180. Общие положения по назначению и производству компьютерно-

147. Крылов В.В. Информационные компьютерные преступления. М.: Издательская группа ИНФРА М – НОРМА, 1997. – 285 с.

148. Крылов В.В. Основы криминалистической теории расследования преступлений в сфере информации: Автореф. дис. ... д-ра юрид. Наук. – М.: Изд-во Моск. ун-та, 1998. – 50 с.

149. Крылов В.В. Расследование преступлений в сфере информации. – М.: Городец, 1998. – 264 с.

150. Кузнецов В. Комп'ютерна інформація як предмет крадіжки // Право України. – 1999. – №7. – С. 85-88.

151. Кулагин Н.И. Организация и тактика следственного осмотра. – Волгоград, 1983. – 57 с.

152. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М.: ИНФРА М-НОРМА, 1998. – 153 с.

153. Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях. – СПб.: Право, 1998. − 90 с.

154. Ларичев В.Д. Преступления в кредитно-денежной сфере и противодействие им: Учебно-практическое пособие. – М., 1996. – 234 с.

155. Лащук Є.В. До питання про «безпредметні» злочини // Держава і Право. – 2000. – Випуск 8. – С. 375.

156. Лисиченко В.К., Циркаль В.В. Формы использования специальных познаний и виды участия специалистов на предварительном следствии. // Применение специальных познаний в борьбе с преступностью. – Свердловск, 1983. – С. 10-18.

157. Лисиченко В.К. Классификация документов как объектов следственно-судебного и экспертного исследования // Материалы теоретической конференции по итогам научно-исследовательской работы профессорско-преподавательского состава. – К., 1973. – С. 103-107.

158. Литвинчук Г.К., Морокко Д.Ф. Особливості розслідування злочинів про підробку банківських платіжних карток // Теорія та практика кримі-налістичного забезпечення розкриття та розслідування злочинів у сучасних умовах: Тези доп. міжнарод. наук.- практ. конференції. – К.: НАВСУ, 2001. – Ч. 11. – 288 с. – С. 199-214.

159. Лісовий В. Комп'ютерні злочини: питання кваліфікації // Право України. – 2002. – № 2. – С. 87-88.

160. Лісовий В. Огляд місця події при розслідуванні «комп'ютерних» злочинів. // http://www.crime-research.iatp.org.ua/library/Lisoviy.htm

161. Лузгин И.М. Некоторые аспекты криминалистической характеристики и место в ней данных о сокрытии преступлений // Криминалистическая характеристика преступлений: Сб.научных трудов / Всесоюзный институт по изучению причин и разработке мер предупреждения преступности. – М., 1984. – С. 25-30.

162. Луценко О.А. Расследование хищений в сфере банковской деятельности: Науч.-практ. пособие. – Ростов н/Д.: Изд-во Рост, ун-та, 1998. – 140 с.

163. Матусовский Г.А. Методика расследования хищений: Учебное

належною мірою забезпечує повноту, всебічність й об'єктивність досудового розслідування, вирішення завдань кримінального процесу й досягнення цілей правосуддя, а також дотримання прав громадян на судовий захист від злочинних зазіхань.

Результати проведеного нами дослідження свідчать про те, що ознаки вчиненого комп'ютерного злочину в банківській системі можуть бути виявлені одним із таких трьох шляхів. По-перше, їх виявляють шляхом проведення оперативно-розшукових заходів, що передують порушенню кримінальної справи. По-друге, їх виявляють громадяни й представники різних установ й організацій при проведенні перевірочних і контрольних заходів. По-третє, вони виявляються безпосередньо слідчим, прокурором або судом. Як було відзначено, у більшості випадків дані про ознаки злочину входять до складу тієї вихідної криміналістично значимої інформації, яку має слідчий або орган дізнання до моменту порушення кримінальної справи й початку розслідування. У зв'язку з чим їх діяльність на початковій стадії розслідування злочину розглянутої категорії містить у собі: 1) оцінку інформації про злочин, що надійшла; 2) перевірку заяви й повідомлення (якщо даних, що вказують на ознаки злочину, недостатньо); 3) прийняття й процесуальне оформлення рішення про порушення кримінальної справи.

З наукового погляду безсумнівний інтерес представляє той факт, що вперше ця проблема була піднята вченими П.Д. Біленчуком, В.Б. Вєховим, В.О. Голубєвим, В.В. Криловим, М.В. Салтевським, В.С. Цимбалюком лише в середині 90-х рр., а з 1995 р. стали з'являтися перші монографічні роботи, які частково торкались проблеми виявлення комп'ютерних злочинів у банківській системі [27; 37; 38; 62; 75; 148; 214; 220; 251].

Особливістю порушення й розслідування даної категорії кримінальних справ є те, що злочинців затримують, як правило, у момент проведення платежу по пластиковій картці. Таке затримання може бути як випадковим, так і результатом проведення оперативної розробки. У кожному разі слідчому необхідно вилучити: картку, по якій провадився платіж; сліпи з вказівкою оплаченої суми й підписом особи, що проводила платіж; сліпи, що свідчать про використання картки раніше; документи, що засвідчують особу.

Після порушення кримінальної справи затриманого необхідно допитати і отримати відповіді на такі питання: які його справжні анкетні дані; як, коли, де, у кого й з якою метою він придбав дану картку; як часто він її використовував, де саме, на які суми здійснював платежі; якщо купував товари, то які саме, як ними розпорядився, де вони в цей момент перебувають; чи отримував готівку за допомогою картки, якщо так, то де, як і хто йому в цьому допомагав; хто ще входить до складу групи, що вчинює розкрадання, хто був ініціатором її створення, як розподілялися ролі, як розподіляли прибутки; у кого, коли, де, за яких обставин придбав підроблені документи, що засвідчують особу; з якою метою відкрив поточний рахунок у банку й придбав картку за підробленими документами; як і де була виготовлена підроблена картка, де знаходиться обладнання для її виготовлення; як були отримані ідентифікаційні дані для виготовлення підробленої карти.

Після проведення допитів всіх осіб, підозрюваних у вчинені даного злочину, необхідно негайно провести обшуки за місцем їх проживання. У результаті обшуку можуть бути вилучені: викрадене майно; сліпи, що свідчать про раніше вчинені розкрадання; інші підроблені картки; підроблені документи; зразки підписів з наслідуванням підпису власника картки; обладнання для виготовлення підроблених карток; записні книжки, чорнові записи, що свідчать про коло знайомств затриманого.

Для закріплення всіх обставин затримання особи на місці злочину необхідно допитати: співробітників торговельного або сервісного підприємства (як правило, це касир або продавець), що виявили неплатоспроможність карти. Даним особам повинні бути задані такі питання: що послужило причиною відмови пред'явникові картки для здійснення платежу (не пройшла авторизацію, зовнішній вигляд картки викликав підозри, підпис пред'явника картки не відповідав підпису на картці, у пред'явника картки не виявилося документів, що засвідчують особу), яка сума підлягала оплаті, чи вилучалася картка, де вона в цей час знаходиться; прізвища співробітників міліції або служби безпеки підприємства, що здійснили безпосереднє затримання особи: за конкретними обставинами затримання. Крім того, варто з'ясувати, чи не було в затриманого спільників.

Завдання та хід подальшого розслідування визначаються колом обставин, які підлягають доказуванню (ст. 64, 65 КПК України). У відношенні до злочинів, які ми розглядаємо, дані обставини можуть бути конкретизовані та доповнені.

Одним з найважливіших завдань подальшого розслідування, характерним для розслідування всіх кримінальних справ даної категорії, є встановлення всіх епізодів злочинної діяльності обвинувачуваних.

Маючи інформацію, які саме НІТ (науково-інформаційні технології) і пластикові картки використовувалися для вчинення розкрадань, варто направити запит у розрахунковий центр, що обслуговує дану платіжну систему.

Після цього в зазначених підприємствах необхідно вилучити оригінали сліпів, на яких зазначена дата платежу, сплачена сума, реквізити картки, підпис платника. Всі сліпи повинні бути направлені на почеркознавчу експертизу для встановлення особи, що виконала підпис за клієнта.

Крім того, за допомогою зазначених сліпів можна встановити касира, що прийняв платіж, якого необхідно допитати для з'ясування можливості впізнання ним злочинця. Надалі необхідно провести впізнання касирами злочинців, які вчинили даний злочин.

Важливим питанням, що вимагає спеціального з'ясування при розслідуванні даного виду злочину, є встановлення потерпілого в справі. Відповідно до ЦК України банк, що отримує грошові кошти клієнта, стає їх власником, а у вкладника з'являється на ці кошти право вимоги, отже, збиток заподіюється банку.

Нижче розглянемо основні способи і алгоритми слідчих дій на досудовому слідстві.

Одержання в кредитній установі пластикової картки за підробленими

124. Конституція України. – К.: Офіційне видання Верховної Ради України, 1996. – 119 с.
125. Корж В.П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности: Монография. – Харьков, 2002. – 412 с.
126. Корухов ЮГ. Криминалистическая диагностика при расследовании преступлений. М: Норма-Инфра. – М, 1998. – 288 с.
127. Костюченко О.А. Банківське право. – К.: А.С.К., 2001. – 569 с.
128. Кривенко Т., Куранова Э. Расследование преступлений в кредитно-финансовой сфере. // Законность. – 1996. – № 1.
129. Криминалистика / Под общей ред. Образцова В.А. – М., 1995. – 592 с.
130. Криминалистика. / Под ред. Пантелеева И.Ф., Селиванова Н.А. – М., 1993. – 592 с.
131. Криминалистика: Учеб. / Под ред. А.Г. Филиппова (отв. ред.), А.Ф. Волынского. – М.: Спарк, 1998. – 200 с.
132. Криминалистика: Учебник для вузов. / Отв. ред. Яблоков Н.П. – М., 1995. – 708 с.
133. Криминалистическая характеристика в методике расследования преступлений. / Межвуз. сб. науч. трудов. Вып.69. – Свердловск, 1978. – 155 с.
134. Криміналістика: Енциклопедичний словник (україно-російський, російсько-український) / За ред. В.А. Тація. – Х.: Право, 2001. – 553 с.
135. Криміналістика: Підручник для слухачів, ад'юнктів, викладачів системи МВС України. /Біленчук П.Д., Дубовий О.П. – К., 1998. – 416 с.
136. Криміналістика: Підручник для студентів юрид. спец. вищих закладів освіти. / За ред. В.Ю. Шепітька. – К.: Видавничий Дім «Ін Юре», 2001. – 684 с.
137. Криміналістика: Підручник. / За ред. П.Д. Біленчука. – Атіка, 2001. – 544 с.
138. Кримінальна справа № 10-4043, порушена 09.08.95 СВ Печерського РУВС ГУМВС України в м. Києві.
139. Кримінальна справа № 1-137 за 2004 р. / Архів Київського районного суду м. Донецька.
140. Кримінальна справа № 1-172 за 1996 р. / Архів Апеляційного суду Черкаської області.
141. Кримінальна справа № 1-55 за 2002 р. / Архів Красноармійського міськ-суду Донецької області.
142. Кримінальна справа № 98271190 / Архів Дарницького районного суду м. Києва.
143. Кримінальна справа № 70001130 СУ УМВС України в Дніпропетровській області.
144. Кримінальна справа № 70001151 СУ УМВС України в Дніпропетровській області.
145. Кримінальна справа №1-19 за 2001 р. / Архів Кіровського районного суду Автономної Республіки Крим.
146. Кримінальний кодекс України. К: Атіка, 2001. – 160 с.

інформації від несанкціонованого доступу: Методичні рекомендації. – К.: НАВСУ, 1999. – 160 с.

105. Карманов Є.В. Банківське право України: навчальний посібник для студентів юридичних спеціальностей вищих закладів освіти. – Х.: Консум, 2000. – 464 с.

106. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: Автореф. дис. ... канд. юрид. наук. – М.: Академия МВД России, 1997. – 24 с.

107. Катков С.А., Собецкий И.В., Фёдоров А.Л. Подготовка и назначение программно-технической экспертизы // Информ. бюллет. СК МВД России. – 1995. – № 4 (85). – С. 93-94.

108. Качан О.О. Банківське право: Навчальний посібник / НАВСУ. – К.: Юрінком Інтер, 2000. – 288 с.

109. Клименко Н.И. Криминалистические знания в структуре профессиональной подготовки следователя: учебное пособие. – К.: Выща школа, 1990. – 103 с.

110. Клименко Н.І. Судова експертиза в розслідуванні комп'ютерних злочинів як форма використання спеціальних знань // Теорія та практика судової експертизи і криміналістики. – Харків: Право, 2002. – № 2. – С. 59-63.

111. Клименко Н.І., Кириченко О.А. Криміналістика як наука та навчальна дисципліна: Монографія. – Дніпропетровськ: ДДУ, 1994. – 200 с.

112. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М., 2002.

113. Колдин В.Я. Идентификация и ее роль в установлении истины по уголовным делам. – М.: МГУ, 1975.

114. Колдин В.Я. Идентификация при расследовании преступлений. М.: Юрид. лит-ра, 1978.

115. Колесник В.А. Розслідування комп'ютерних злочинів: Науково-методичний посібник. − К.: НАСБУ, 2003. − 124 с.

116. Колесниченко А.Н. Общие положения методики расследования отдельных видов преступлений: Текст лекции. – Харьков, 1976. – С.21.

117. Колесниченко А.Н., Коновалова В.Е. Криминалистическая характеристика преступлений: Учебное пособие. – Х., 1985. – 93 с.

118. Комиссаров А.Ю., Подлесный А.В. Идентификация пользователя ЭВМ и автора программного продукта: метод. рек. – М.: ЭКЦ МВД России, 1996. – 40 с.

119. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации. // Законность. – 1999. – № 3. – С. 12-15.

120. Компьютерная преступность и информационная безопасность / Под общ. ред. А.П. Леонова. – Минск: АРИЛ, 2000. – 120 с.

121. Компьютерная преступность// Служба безопасности. – 1997. – № 1. – С. 19.

122. Коновалова В.Е., Шепитько В.Ю. Криминалистическая тактика: теории и тенденции: Учебное пособие. – Х.: Гриф, 1997. – 255 с.

123. Коновалова В.Е. Допрос: тактика и психология: Учеб. пособие. – Х.: Консум, 1999. – 156 с.

документами з подальшим неповерненням перевитрачених коштів.

У цих випадках злочинці використовують зазвичай загублені або викрадені паспорти, у яких переклеюють фотографію.

У зв'язку із цим необхідно призначити техніко-криміналістичну експертизу паспорта, використаного для відкриття рахунку з метою встановлення внесених у нього відповідних змін.

Вилучити в кредитній установі, що видала картку, заяву про відкриття особового рахунку, поточного валютного внеску, документа про одержання особистої картки.

Встановити й допитати справжнього власника паспорта з таких питань: при яких обставинах і коли був втрачений паспорт; чи звертався в міліцію із цього приводу; чи знайомі йому особи, що проходять у справі; чи ним особисто виконані підписи в заяві про відкриття особового рахунку, поточного валютного внеску, документі про одержання особистої картки. Необхідно також допитати співробітників банку (операціоніста), що відкривали рахунок і видавали особисту картку, про обставини, що виникли, чи можуть вони впізнати й за якими ознаками особу, що відкрила рахунок.

Провести впізнання співробітниками кредитної установи винної особи.

Використання знайденої або вкраденої картки для оплати товарів чи послуг або для одержання готівки в банкоматах.

Цей спосіб є найбільш примітивним і його успіх багато в чому залежить від того, наскільки швидко винна особа здійснить задумане, оскільки у випадку своєчасного звернення власника картки в банк на неї виставляється стоп-аркуш.

У цьому випадку необхідно: допитати справжнього власника картки за обставинами її втрати, чи заявляв він про це в кредитну установу і як швидко. Допитати співробітників банку й розрахункового центру з питань: чи звертався до них із заявою про втрату картки її справжній власник, чи виставлявся стоп-аркуш і якщо ні, то чому; вилучити відеозаписи у випадку розкрадання коштів безпосередньо з банкомату (місцезнаходження банкомату в обов'язковому порядку контролюється відеоапаратурою) і призначити за ними портретну та, по можливості, дактилоскопічну експертизу.

Розкрадання з використанням підроблених кредитних або розрахункових карток.

У випадку вилучення підробленої картки необхідно призначити техніко-криміналістичну експертизу, на вирішення якої поставити такі питання: чи виготовлена надана на дослідження картка (вказати її ідентифікаційні дані) підприємствами даної платіжної системи (вказати якою саме); якщо ні, то яким способом і з застосуванням яких матеріалів вона виконана; чи виготовлена дана пластикова картка на обладнанні, вилученому у підозрюваного. Одночасно експертові повинні бути надані зразки справжніх карток, які можна вилучити у підприємства-виробника.

Далі варто встановити й допитати справжнього власника картки: якою карткою він користується і як давно; хто ще міг користуватися даною карткою; чи не помічав, що хтось користується його рахунком і чи зберігала картка авторизацію, чи звертався він з цього питанню в банк-емітент; чи

користувався він послугами торговельних і сервісних підприємств, через які здійснювалися платежі по його картці; чи його підпис стоїть в сліпах, вилучених у даних підприємствах.

Оскільки злочинці намагаються використовувати ідентифікаційні дані карток іноземних власників, проведення даної слідчої дії може бути ускладнене. У цьому випадку є сенс скористатися каналами Інтерполу, Європолу або використовувати можливості служби безпеки самих банків, куди варто направити запит із проханням встановити справжніх власників карток і одержати відповіді на питання, що цікавлять. Залучена до матеріалів справи відповідь банку буде відповідати ознакам іншого документа в значенні ст. 65 КПК України і може використовуватися як доказ.

Важливою обставиною, що підлягає доказуванню при використанні злочинцями підроблених карток, є спосіб заволодіння ідентифікаційними даними картки. У цьому випадку робота повинна вестися у двох напрямах.

По-перше, необхідно вжити заходів для встановлення кола знайомих обвинувачуваного. Така інформація може міститися в його записних книжках, чорнових записах тощо. З даного питання варто допитати його родичів (якщо вони погодяться давати показання), сусідів, знайомих, дати окреме доручення органу дізнання. Особливу увагу варто звертати на зв'язки в банках, торговельних і сервісних підприємствах.

По-друге, необхідно вжити заходів для встановлення, у яких саме підприємствах справжні власники карт використовували їх. Це допоможе виявити одне-два підприємства, послугами яких користувалися всі карткоутримувачі й на відпрацьовуванні саме їх співробітників зосередити основну увагу.

Використання підроблених карток нерозривно пов'язане з їх виготовленням, тому в процесі розслідування повинні бути вжиті заходи, спрямовані на виявлення відповідного обладнання. У випадку виявлення, обладнання для виготовлення пластикових карток, воно повинно бути вилучене, оглянуте й приєднане до справи як речовий доказ. В подальшому треба провести слідчий експеримент для встановлення можливості виготовлення на даному обладнанні підробленої пластикової картки.

Створення за підробленими документами фіктивного підприємства й укладання з банком договору на обслуговування пластикових карток.

Даний спосіб є різновидом вчинення розкрадань за допомогою підроблених карток.

У цьому випадку необхідно: вилучити установчі документи підприємства в реєстраційній палаті або банку; вилучити в банку договір на відкриття банківського рахунку, договір про обслуговування власників пластикових карток й угоди до нього, картки зі зразками підписів керівників підприємства, зведені чеки й сліпи, які надані підприємством у банк; за всіма зазначеними документами призначити почеркознавчу експертизу для встановлення, ким виконані в них підписи (у графах «клієнт», «касир» тощо); допитати за обставинами укладання договору на обслуговування пластикових карток спеціаліста управління пластикових карт банку; допитати співробітників банку, відповідальних за аналіз платіжних систем, про обставини

Терміни та визначення (від 01.01.1998).

85. Дулов А.В., Нестеренко Н.Д. Тактика следственных действий. – Минск, 1971. – 120 с.

86. Дутов М. Ответственность за компьютерные преступления, педусмотренная новой редакцией УК Украины. http://www.crime-research.org/library/dutov.htm

87. Єрьоміна Н.В. Банківські інформаційні системи: Навч. посібник. — К: КНЕУ, 2000. — 220 с.

88. Жбанков В.А. Тактика следственного осмотра. – М, 1992. – 131 с.

89. Жирний Г.Ю. Про формування окремих криміналістичних методик розслідування злочинів у сфері використання автоматизованих електронно-обчислювальних систем // Матеріали міжвузівської науково-практичної конференції. – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 70.

90. Закон України «Про банки і банківську діяльність» // Відомості Верховної Ради України. – 2001. – № 5-6. – ст. 30.

91. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

92. Закон України «Про інформацію» // Відомості Верховної Ради України. – 1992. – № 48. – ст. 650.

93. Закон України «Про міліцію» // Відомості Верховної Ради УРСР. – 1991. – №4. – ст. 20.

94. Закон України «Про Національний банк України» // Відомості Верховної Ради України. – 1999. – № 29. – ст. 238.

95. Закон України «Про оперативно-розшукову діяльність» // Відомості Верховної Ради України. – 1992. – № 22. – ст. 303.

96. Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» // Відомості Верховної Ради України. – 1993. – № 35. – ст. 358.

97. Закон України «Про платіжні системи та перекази грошей в Україні» // Відомості Верховної Ради України. – 2001. – № 29. – ст. 137.

98. Закон України «Про службу безпеки» // Відомості Верховної Ради України. – 1992. – № 27. – ст. 382.

99. Закон України «Про судову експертизу» // Відомості Верховної Ради України. – 1994. – № 28. – ст. 232.

100. Збірка нормативних документів системи технічного захисту інформації. – 1997. – № 4. – 91 с.

101. Збірник методичних рекомендацій з питань розкриття та розслідування злочинів слідчими та оперативними працівниками органів внутрішніх справ. / За ред. П.В. Коляди. – К.: ГСУ МВС, 2001. – 240 с.

102. Зубок М.І., Ніколаєва Л.В. Організаційно-правові основи безпеки банківської діяльності в Україні: Навчальний посібник для студентів вищих навчальних закладів. – К.: Істина, 2000. – 88 с.

103. Ищенко П.П. Специалист в следственных действиях: уголовно-процессуальные и криминалистические аспекты: Практическое пособие. – М., 1990. – 158 с.

104. Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л. Основи захисту

68. Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів / Під ред. О.П. Снігерьова. – Запоріжжя, 1998. – 144 с.

69. Гончаренко В.И., Кушнир Г.А., Подпалый В.Л. Понятие криминалистической характеристики преступлений // Криминалистика и судебная экспертиза. – К., 1986. – Вып. 33. – С. 15-19.

70. Гончаров Д. Квалификация хищений, совершенных с использованием компьютерных технологий // Законность. – 2001. – № 11. – С. 31-33.

71. Городиський О.М. Криміналістична характеристика та основні положення розслідування злочинів, пов'язаних з приховуванням валютних цінностей: Автореф. дис. ... канд.юр.наук: 12.00.09. – Х., 1998. – 18 с.

72. ГОСТ 6.10.4-84 «УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения».

73. Грамович Г.И. Тактика использования специальных знаний в раскрытии и расследовании преступлений: Учебное пособие. – Минск, 1987. – 65 с.

74. Гриненко А.В., Каткова Т.В., Кожевников Г.К., Коновалова В.Е., Шепитько В.Ю. Руководство по расследованию преступлений. Уголовная процедура. Криминалистическая техника. Тактика производства следственных действий. Экспертиза: Науч.-практ. пособие. – Х.: СПКПФ «Консум», 2001. – 608 с.

75. Гудков Г.П. Компьютерные преступления в сфере экономики // Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. – М.: МИ МВД России, 1995. – С. 142-144.

76. Гуняев В.А. Содержание и значение криминалистической характеристики преступлений // Криминалистическая характеристика преступлений: Сб.науч.трудов/ Всесоюзный институт по изучению причин и разработке мер предупреждения преступности. – М., 1984. – С. 58-61.

77. Гуцалюк М. Протидія комп'ютерній злочинності // Право України. – 2003. – № 6. – С. 114-117.

78. Гуцалюк М.С. Координація боротьби з комп'ютерною злочинністю // Право України. – 2002. – №5. – С. 21-26.

79. Дзюблюк О.В. Організація грошово-кредитних відносин суспільства в умовах ринкового реформування економіки. – К.: Поліграфкнига, 2000. – 512 с.

80. Дидковская С.П., Клименко Н.И., Лисиченко В.К. Подготовка и проведение отдельных видов судебной экспертизы: Учебное пособие. – К., 1977. – 79 с.

81. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – 480 с.

82. ДСТУ 2226–93. Автоматизовані системи. Терміни та визначення (від 01.07.94).

83. ДСТУ 2938–94 Системи оброблення інформації. Основні положення. Терміни та визначення (від 01.01.96).

84. ДСТУ 3396.2–97 Захист інформації. Технічний захист інформації.

співробітництва з фіктивним підприємством.

Оскільки в розглянутому випадку підроблені кредитні картки можуть бути й не виявлені, необхідно вилучити в розрахунковому центрі всі сліпи по пластикових картках, що цікавлять. Після цього необхідно призначити техніко-криміналістичну експертизу для визначення відповідності відбитків із кредитних карток у цих сліпах і відбитків з аналогічних картках у сліпах, наданих у банк обвинувачуваним.

Розслідування розкрадань у кредитно-фінансовій сфері, вчинених з використанням комп'ютерної техніки.

Основними проблемами, що виникають при розслідуванні таких справ про розкрадання є: складності у встановленні (у випадку вчинення злочину з використанням комп'ютерної техніки) самої події злочину й правильна його кваліфікація; значні ускладнення у слідчого при проведенні слідчих дій щодо виявлення, вилучення, фіксації й дослідження комп'ютерної інформації; відсутність у слідчих як практики розслідування злочинів, вчинених з використанням НІТ, комп'ютерної техніки, так і знань самої техніки.

Аналіз виявлених злочинів, вчинених з використанням електронних засобів доступу, показує, що найбільш часто злочинні зазіхання спрямовані на локальні комп'ютерні мережі й бази даних банківських установ.

Розслідування розкрадань, вчинених з використанням комп'ютерної техніки, здійснюється за такими основними напрямами: збір фактів, що свідчать про вчинення незаконних операцій з використанням комп'ютерної техніки; проведення заходів, спрямованих на встановлення причинного зв'язку між діями, що утворюють спосіб проведення незаконної операції, і наслідками, що настали, шляхом деталізації характеру вчинених винним дій; визначення розміру збитку, заподіяного протиправними діями; збір і фіксація фактів про причетність винної особи до вчинених дій і наслідків, що настали.

Кожний з цих напрямів припускає вирішення своїх специфічних завдань. Однак основною специфікою розслідування даної категорії злочинів є необхідність приділяти пріоритетну увагу збору й фіксації комп'ютерної інформації. Саме комп'ютерна інформація в багатьох випадках дозволяє встановити фактичні обставини справи, виявити коло осіб, причетних до вчинення злочину, а також виявити сліди злочину.

З огляду на особливості комп'ютерної інформації, а саме: бездокументальна форма зберігання, швидкість і легкість знищення, її знеособленість (при введенні інформації через комп'ютер), при розслідуванні перед слідчим виникає ряд завдань, без вирішення яких успішне розкриття злочину буде неможливе.

Насамперед, до роботи з розслідування даного злочину необхідно залучити грамотного спеціаліста з комп'ютерних систем і мереж.

Участь відповідного спеціаліста необхідна також і при проведенні допитів, на яких з'ясовуються технічні аспекти вчиненого злочину.

Виходячи з проаналізованої криміналістичної літератури та вивченої судової й слідчої практики можна виділити три типові ситуації, що складаються при вчиненні розкрадань із використанням НІТ і комп'ютерної техніки:

1. Власник або користувач комп'ютерної мережі (бази даних) власними силами виявив факт незаконного проникнення й інших протиправних дій, встановив винну особу й заявив про це в правоохоронні органи.

2. Власник або користувач комп'ютерної мережі (бази даних), інформаційної системи виявив факт незаконного проникнення в комп'ютерну мережу й інших протиправних дій, але не зміг встановити винну особу й заявив про це в правоохоронні органи.

3. Інформація про незаконне проникнення в комп'ютерну мережу та інших вчинених протиправних діях стала загальновідома або була встановлена в ході проведення оперативно-розшукових заходів.

Таким чином, першочерговим завданням слідчого й оперативного працівника є збір і фіксація за допомогою власника системи факту незаконного проникнення в комп'ютерну мережу та вчинення інших протиправних дій.

У комп'ютерних мережах, як правило, програмне забезпечення настроюється так, щоб максимально повно протоколювати всі події, що відбуваються в системі. Протоколюється, з якого комп'ютера відбулося з'єднання, а якщо на комп'ютері встановлена програма ідентифікації, то й ім'я користувача, що запросив з'єднання.

Забезпечення збереження електронних протоколів, що вказують на проникнення в мережу, є одним із завдань слідчого, оскільки така інформація, вилучена в ході розслідування кримінальної справи з дотриманням кримінально-процесуальних вимог, може бути доказом у справі. З подібних міркувань необхідно забезпечити збереження жорсткого диску зламаного комп'ютера. Якщо кримінальну справу порушено, то слідчий може дозволити власникові після відповідних досліджень з допомогою спеціаліста зняти копію з жорсткого диску, а сам диск направляється на експертизу. Подальший аналіз диску може дозволити визначити, що встиг зробити зловмисник, як він проник у систему й де перебуває комп'ютер, що використовувався для проникнення в мережу.

Особливу увагу необхідно звертати на спосіб незаконного проникнення в локальну обчислювальну мережу: підбір або знання паролів, відключення засобів захисту (у тому числі ззовні), використання недосконалості засобів захисту, використання спеціальних програмних засобів, а також на зміст й призначення інформації, на яку був здійснений вплив. В окремих випадках зазначена інформація дозволяє досить чітко визначити коло підозрюваних осіб.

З огляду на конкретні обставини й з урахуванням запропонованих слідчих ситуацій, слідчим можуть бути висунуті такі загальні версії:

– розкрадання вчинене співробітником даної кредитно-фінансової установи, або особою, що входить у коло родичів, друзів, знайомих співробітників установи, іншою особою, що має доступ до комп'ютерної техніки в даній установі;

– злочин вчинений групою осіб за участю співробітника даної установи;

– розкрадання вчинене особою або групою осіб, не пов'язаних з діяльністю даної кредитно-фінансової установи.

52. Воры проникли в компьютерную сеть Национального банка // Голос Украины. – 1998. – № 217 (1963). – С. 2.

53. Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій // Уряду України. Президенту, законодавчій, виконавчій владі «Боротьба з контрабандою: проблеми та шляхи їх вирішення». Аналітичні розробки, пропозиції наукових і практичних працівників / Керівники авторського колективу А.І. Комарова, О.О. Крикун. – К., 1999. – С. 148-154.

54. Гаврилов М., Иванов А. Следственный осмотр при расследовании преступлений в сфере компьютерной информации // Законность. – 2001. – № 9. – С. 11-16.

55. Герасимов И.Ф. Криминалистические характеристики преступлений в структуре частных методик // Криминалистические характеристики в методике расследования преступлений / Межвузовский сб. науч. трудов. – Свердловск, 1978. – Вып.69. – С. 5-10.

56. Герасимов И.Ф. Общие вопросы криминалистической тактики // Криминалистика. – М, 1994. – С. 221-229.

57. Глазырин Ф.В. Изучение личности обвиняемого и тактика следственных действий. – Свердловск, 1975. – 184 с.

58. Голубев В.А., Головин А.Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий // http://www.crime-research.org/library/New_g.htm

59. Голубєв В.О. Аналіз і класифікація загроз безпеки автоматизованих банківських систем // Вісник Запорізького юридичного інституту МВС України. – Запоріжжя, 1998. – Вип.1(4). – С. 103-110.

60. Голубєв В.О. Деякі особливості тактики окремих слідчих дій при розслідуванні комп'ютерних злочинів // Підприємництво, господарство і право. – 2003. – №8. – С. 107-110.

61. Голубєв В.О. Комп'ютерна злочинність // Юридичний вісник України. – № 6, 7. – 2002. – С. 5-7.

62. Голубєв В.О. Комп'ютерні злочини в банківській діяльності. – Запоріжжя: ВЦ «Павел», 1997. – 118 с.

63. Голубєв В.О. Правові проблеми захисту інформаційних технологій // Вісник Запорізького юридичного інституту. – 1997. – №2. – С. 35-40.

64. Голубєв В.О. Теоретично-правові проблеми боротьби з комп'ютерною злочинністю // Вісник Запорізького юридичного інституту. – 1999. – №3. – С. 52-60.

65. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навчальний посібник. / За заг. ред. д.ю.н., професора Р.А. Калюжного. – Запоріжжя: ГУ «ЗІДМУ», 2002. – 292 с.

66. Голубєв В.О., Юрченко О.М. Злочини в сфері комп'ютерної інформації: способи скоєння, засоби захисту. / НАВСУ, ЗЮІ МВС. – Запоріжжя, 1998. – 156 с.

67. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочиннністю. – Запоріжжя: ЗІДМУ, 2003. – 250 с.

35. Васильев А.Н., Яблоков Н.П. Предмет, система и теоретические основы криминалистики. – М., 1984. – 143 с.

36. Ведерников Н.Т. Личность преступника как элемент криминалистической характеристики преступления // Криминалистическая характеристика преступления: Сб. научных трудов / Всесоюзный институт по изучению причин и разработке мер предупреждения преступности. – М., 1984. – С. 74-77.

37. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. – М.: Право и Закон, 1996. – 181 с.

38. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: Учеб.-метод. пособие. – Волгоград: Перемена, 1998. – 72 с.

39. Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ / Под ред. Б.П. Смагоринского. – Волгоград: ВА МВД России, 2004. – 304 с.

40. Вехов В.Б., Попова В.В., Илюшин Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: Науч.-практ. пособие. – М.: ЛексЭст, 2004. – 160 с.

41. Вехов В.Б. Документы на машинном носителе // Законность. – 2004. – №2. – С. 18-20.

42. Вєртузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України. – 1998. – №1. – С. 101.

43. Вєртузаєв М.С. Проблеми взаємодії оперативних підрозділів органів внутрішніх справ зі службами безпеки банків в попередженні злочинних посягань з використанням пластикових платіжних засобів // Бизнес и безопасность. – 2002. – №5. – С. 2-3.

44. Вєртузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник / За ред. С.Г. Лаптєва. – К.: Європ. ун-т, 2001. – 321 с.

45. Возгрин И.А. Научные основы криминалистической методики расследования преступлений. СПб.: СПб ЮИ МВД России, 1993. – Ч. 4.

46. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002. – 496 с.

47. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. – 2002. – №1. – С. 4-12.

48. Волобуєв А.Ф Предмет розкрадання майна у сфері підприємництва як елемент криміналістичної характеристики злочинів даного виду // Вісник Одеського інституту внутрішніх справ. - 1998. – Вип.3. – С.39-43.

49. Волобуєв А.Ф. Загальні положення криміналістичної методики: Лекція. – Х., 1996. – 36 с.

50. Волобуєв А.Ф. Комплексна методика розслідування економічних злочинів // Вісник прокуратури. – 2003. – № 6 (24). – С. 53-56.

51. Волобуєв А.Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки // Вісник Луганського інституту внутрішніх справ. – 1998. – №2. – С. 179-185.

На думку вітчизняних і закордонних фахівців, на долю розкрадань, вчинених співробітниками установи, що має локальну обчислювальну мережу, або за змовою з ними, припадає близько 70-80% всіх розкрадань із незаконним використанням комп'ютерної інформації. Як правило, подібні розкрадання вчинюються групою, причому один з її членів є або співробітником даної установи, або має вільний доступ до комп'ютерів (представник служби технічного забезпечення, постійний контрагент тощо), вміє працювати з обчислювальною технікою, має уяву, яка інформація й де розташована в комп'ютері.

У цьому випадку злочинця характеризують дві ознаки, які істотно звужують коло підозрюваних: знання функцій, паролів різних операцій, виконуваних тим чи іншим комп'ютером в організації, і наявність доступу до комп'ютера або їх мережі.

Необхідно у зв'язку з цим, особливу увагу звернути на те, що часто розкрадання вчинюють не тільки кваліфіковані фахівці, знання яких дозволяють їм зламати захист багатьох комп'ютерних систем, але й некваліфіковані службовці, що мають можливість доступу до засобів комп'ютерної техніки.

У зв'язку з цим великого значення набувають допити потерпілих і свідків, а також одержання документів, що характеризують роботу як установи в цілому, так і окремих його співробітників.

Крім відомостей про осіб, що мають доступ до даного комп'ютера, по можливості варто встановити, яка комп'ютерна техніка використовується, чи підключена вона до джерела автономного або безперебійного живлення, де розташований щиток відключення електроенергії в даному приміщенні, чи є у користувача спільники, чи виставляється контрнагляд під час роботи комп'ютера тощо. Через вузол зв'язку, на якому зареєстрований даний абонентський номер телефону, необхідно встановити час, коли здійснюється модемний зв'язок.

Зазначена інформація необхідна для забезпечення успішного проведення одної з початкових слідчих дій по кримінальних справах даної категорії – обшуку.

З урахуванням проведеного аналізу варто виділити деякі типові слідчі ситуації, версії та алгоритми проведення відповідних слідчих дій.

Ситуація 1. Власник або користувач комп'ютерної мережі (бази даних) або кредитної картки власними силами виявив факт незаконного проникнення й інших протиправних дій, виявив винну особу й заявив про це в правоохоронні органи.

Ситуація 2. Власник або користувач комп'ютерної мережі (бази даних) інформаційної системи або кредитних карток виявив факт незаконного проникнення й інших протиправних дій, але не зміг встановити винну особу й заявив про це в правоохоронні органи.

Ситуація 3. Інформація про незаконне проникнення в комп'ютерну мережу та інші вчинені протиправні дії стали загальновідомі або були встановлені в ході проведення оперативно-розшукових заходів.

Виходячи з позначених типових слідчих ситуацій можливо висунути такі

окремі слідчі версії.

Версія 1. Злочин вчинений співробітником даної установи або особою, що входить у коло родичів, друзів, знайомих співробітників установи, іншою особою, що має доступ до комп'ютерної техніки в даній установі.

Версія 2. Злочин вчинений за попередньою змовою групою осіб або злочинним співтовариством за участю співробітника даної установи.

Версія 3. Злочин вчинений особою або групою осіб, не пов'язаних з діяльністю даної установи.

З урахуванням викладеного й вивчених матеріалів кримінальних справ, ми прийшли до висновку, що на початковому етапі розслідування необхідно проводити такі першочергові слідчі дії: обшук, огляд програмного продукту й комп'ютерної техніки (працюючої і непрацюючої), огляд і аналіз наявної інформації в програмних продуктах і машинних носіях й кредитних картках; допити свідків, потерпілих, підозрюваних (обвинувачуваних); призначення експертизи.

Безумовно, що запропоновані вище слідчі ситуації, типові версії і конкретні слідчі дії далеко не вичерпують усіх питань, пов'язаних із розслідуванням злочинів даної категорії.

1.2. Тактичні особливості проведення окремих слідчих дій при розслідуванні фінансових злочинів, вчинених з використанням сучасних інформаційних технологій

При розслідуванні злочинів, вчинених з використанням НІТ і комп'ютерної техніки чи технології або пластикових карт, сьогодні ще на достатньому рівні не розроблені, не відпрацьовані та не впроваджені в практику чіткі тактичні й методичні аспекти їх розкриття й розслідування, особливо в сфері економіки. Розкриття й розслідування зазначених злочинів мають особливості в проведенні слідчих дій, у ході яких необхідно мати спеціальні знання й уміло їх використовувати як спеціалісту, слідчому, прокурору, судді, так і працівникові органу дізнання.

Аналіз криміналістичної літератури показує, що загальним питанням тактики проведення окремих слідчих дій була приділена достатня увага в наукових працях О.Я. Баєва, В.П. Бахіна, Р.С. Бєлкіна, В.К. Весельського, А.Ф. Волобуєва, В.Г. Гончаренка, Н.І. Клименко, В.О. Коновалової, М.В. Костицького, В.С. Кузьмічова, В.К. Лисиченка, В.Г. Лукашевича, Г.А. Матусовського, О.Р. Михайленка, М.В. Салтевського, М.Я. Сегая, В.В. Тищенка, В.Ю. Шепітька та інших [7; 8; 16; 17; 24; 122; 123; 255; 256].

Деякі особливості тактики проведення слідчих дій при розслідуванні різних видів розкрадань, вчинених з використанням ЗЕОТ і комп'ютерної інформації, досліджувалися П.Д. Біленчуком, В.Б. Вєховим, В.О. Голубєвим, Л.П. Паламарчук, М.В. Салтевським, М.Г. Шурухновим [29; 38; 60; 185; 220; 221; 223; 261; 262]. А.В. Касаткін, В.В. Крилов, В.Ю. Рогозін й інші вчені у своїх роботах описали тактичні особливості й рекомендації з проведення окремих слідчих дій при розслідуванні злочинів у сфері НІТ і комп'ютерної інформації [106; 148; 214].

Разом з тим варто визнати, що особливості тактики проведення окремих

18. Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації та її попередження. / ЗЮІ МВС, НАВСУ – Запоріжжя, 1998. – 315 с.

19. Белецкий В.И. К методике расследования хищений денежных средств // Криминалистика и судебная экспертиза: Республиканский междуведомственный научно-методический сборник. – К., 1982, – Вып. 24.

20. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. – М., 1987. – 270 с.

21. Белкин Р.С. Курс криминалистики: В 3 т. – Т. 1: Общая теория криминалистики. М: Юристъ, 1997. – 408 с.

22. Белкин Р.С. Курс криминалистики: В 3 т. – Т. 2: Частные криминалистические теории. – М.: Юристъ, 1997. – 464 с.

23. Белкин Р.С. Курс криміналістики: В 3 т. – Т. 3: Криминалистические средства, приемы и рекомендации. – М.: Юристь, 1997. – 480 с.

24. Белкин Р.С. Очерки криминалистической тактики. Волгоград, 1993. – 200 с.

25. Біленчук П.Д., Борисова Л.В., Паніотов Є.К. Взаємодія правоохоронних органів України та країн світу при розслідуванні електронних високотехнологічних транснаціональних злочинів // Право і безпека. – 2003. – №1. – С. 54-59.

26. Біленчук П.Д. Криміналістичне дослідження обвинуваченого. – К: УАВС, 1995. – 128 с.

27. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: Навч. посіб. – К.: Українська академія внутрішніх справ, 1994. – 71 с.

28. Біленчук П.Д., Котляревський О.І. Портрет комп'ютерного злочинця: Навч. посібник. – К: В & В, 1997. – 48 с.

29. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність. Навчальний посібник. – Київ: Атіка, 2002. – 240 с.

30. Борисова Л.В. Використання спеціальних знань при проведенні розслідування злочинів у сфері комп'ютерної інформації: стан проблеми та перспективи дослідження / Сучасні судово-експертні технології в кримінальному і цивільному судочинстві: Матеріали міжнар. науково-практич. конф. (м. Харків, 14-15 березня 2003 р.). – Х.: Нац. ун-т внутр. справ, 2003. – С. 48-55.

31. Борисова Л.В. Транснаціональні комп`ютерні злочини як об'єкт криміналістичного дослідження: Автореф. дис. ... канд.юр.наук: 12.00.09. – К., 2007. – 16 с.

32. Бущан О.П. Криминалистическая характеристика и основные положения расследования преступлений, совершаемых посредством кредитных банковских преступлений: Дис. ... канд. юр. наук: 12.00.09. – Х., 1995. – 210 с.

33. Быховский И.Е., Глазырин Ф.В., Питерцев С.К. Допустимость тактических приемов при допросе. Волгоград, 1989. – 95 с.

34. Васильев А.Н. Тактика отдельных следственных действий. – М., 1981. – 112 с.

ВИКОРИСТАНА І РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика / Под ред. Р.С. Белкина. – М.: НОРМА-ИНФРА-М, 1999. – 990 с.
2. Аверьянова Т.В. Содержание и характеристика методов судебно-экспертных исследований. Алма-Ата, 1991. – С. 216.
3. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: Юрлитинформ, 2001. – 170 с.
4. Андреев И.С. Грамович Г.И. Криминалистика: учебное пособие. – Минск, 1997. – 344 с.
5. Андрушко П.П. Проблеми кримінальної відповідальності за втручання в роботу автоматизованих систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в автоматизованих системах України. – К., 2000. – С. 50-53.
6. Афанасьев А.Ю. Проблемы предупреждения хищений денежных средств, совершаемых с использованием пластиковых карт и других средств электронного доступа // Российский следователь. – 2003. – №4. – С. 31-35.
7. Бабий А. С., Бахин В. П., Весельский В. К., Гончаренко В. И., Дидковская С. П. Осмотр места происшествия при расследовании отдельных видов преступлений: Учеб. пособие / Н.И. Клименко (ред.). – К.: НВТ Правник, 2001. – 172 с.
8. Баев О.Я. Тактика следственных действий. Воронеж, 1992. – 208 с.
9. Бажанов М.И. Уголовное право Украины. Общая часть. – Днепропетровск, 1992. – 166 с.
10. Банківське право України / А.О. Селіванов, В.Л.Кротюк, Л.Н.Заруденко. – К.: Видавничий дім «Ін Юре», 2000. – 368 с.
11. Банківське право: навчальний посібник / Упорядник М.П. Кучерявенко. – Х.: Торсінг, 1999. – 784 с.
12. Банківське право: українське та європейське: навчальний посібник / П.Д.Біленчук, О.Г.Диннік, І.О.Лютий, О.В.Скороход. – К.: Атіка, 1999. – 398 с.
13. Банковское дело / Под ред. О.И. Лаврушина. – М.: ТОО «ЭКОС», 1992. – 428 с.
14. Баранов О.А. Кримінологічні проблеми комп'ютерної злочинності http://geocities.com/beta_fly/texts/s1.htm
15. Бахін В.П., Біленчук П.Д., Зубань М.А. Алгоритми вирішення слідчих дій. Навчальний посібник. – К.: Українська академія внутрішніх справ, 1995. – 93 с.
16. Бахін В.П., Весельський В.К. Тактика допиту. Навчальний посібник. (Серія «Навчально-практичне видання.») – Київ: НВТ «Правник», 1997. – 64 с.
17. Бахін В.П., Весельський В.К., Клименко Н.І., Котюк І.І., Лисиченко В.К. Огляд місця події при розслідуванні окремих видів злочинів: Науково-практичний посібник / П.В. Коляда (ред.). – К.: Юрінком Інтер, 2005. – 216 с.

слідчих дій і використання спеціальних знань у справах про комп'ютерні злочини в банківській сфері комплексно ще не досліджувалися. У той же час наявні методичні рекомендації вимагають систематизації, потребують подальшої розробки з метою максимально повного задоволення потреб сучасної оперативно-слідчої практики. Це підтверджують і отримані результати опитування слідчих і оперативних працівників, які серед факторів, що найбільш ускладнюють роботу з розкриття й розслідування злочинів зазначеного виду, виділили: недостатнє знання правових актів, нормативних документів, що регламентують сферу інформаційних відносин – 93% респондентів; складності з підготовкою й призначенням експертиз – 84%; дефіцит професійного досвіду слідчих, співробітників підрозділів БЕЗ, КР – 81%; відсутність спеціальних знань у співробітників в галузі комп'ютерної інформації, знарядь і технологій її обробки, захисту, можливостей засобів комп'ютерної техніки – 59%; відсутність спеціальних знань у співробітників в галузі бухгалтерського електронного документообігу – 73 %; відсутність науково обґрунтованих методик, рекомендацій з розкриття й розслідування злочинів – 67%.

Вказані вище результати проведеного нами дослідження дозволяють виділити основну особливість тактики проведення окремих слідчих дії по справах про злочини виділеної групи – особиста участь слідчого в організації, плануванні, підготовці й проведенні невідкладних слідчих дій. Це диктується безпосередньою залежністю ходу подальшого розслідування злочинів даного виду від результатів реалізації оперативних матеріалів. Саме тому слідчий разом з оперативними працівниками повинен розробити варіанти проведення слідчих дій так, щоб виключити можливість знищення знарядь і предметів посягань, інших доказів і слідів злочину, а також інші можливі дії осіб, що ускладнюють розслідування. Необхідно звернути особливу увагу на такі типові недоліки, що мають місце в оперативно-слідчій практиці при проведенні початкових слідчих дій:

– затримання злочинця, його особистий обшук, обшук за місцем його роботи й(або) проживання, початковий огляд місця події, машинних носіїв інформації й самої комп'ютерної інформації (включаючи «електронні документи»), огляд знарядь підготовки, вчинення й приховання злочинів та інших невідкладних слідчих дій співробітниками оперативних служб правоохоронних органів без участі слідчого, а також без попереднього узгодження з ним всіх можливостей одержання доказів, що викривають злочинців;

– необґрунтоване підпорядкування початкових слідчих дій одній меті – вилученню викраденого, документів, знарядь злочину та інших предметів у підозрюваного або на місці виявлення злочину без вживання процесуальних заходів до доведення факту існування між ними причинно-наслідкових зв'язків, надання їм статусу речового доказу на шкоду можливості одержання доказової інформації з інших джерел;

– неякісне процесуальне закріплення криміналістично значимих даних, отриманих при затриманні підозрюваного або в результаті проведення інших слідчих дій.

По справах розглянутої категорії також існує нагальна потреба одночасного проведення, як правило, декількох слідчих дій у найбільш стислий термін. Це визначається тим, що злочинці можуть знищити прямі докази своєї злочинної діяльності буквально за лічені хвилини, найчастіше ті, що неможливо відновити – комп'ютерну інформацію, її фізичні носії, а також інші сліди.

Участь у багатьох початкових слідчих діях декількох спеціалістів одного профілю або різних спеціальностей, використання нових науково-технічних засобів вимагають від слідства вживання додаткових заходів до процесуального підтвердження вірогідності результатів і забезпеченню доказового значення.

На нашу думку, зазначені складності можна розв'язати тільки шляхом спільного планування кожної слідчої дії. Погоджене планування визначає взаємозумовленість і зв'язок між слідчими діями та оперативно-розшуковими заходами. У ході оперативно-розшукової діяльності може надходити інформація, що вказує слідчому на необхідність проведення тих чи інших слідчих дій. З іншого боку, нерідкі й такі випадки, коли факти, встановлені в процесі проведення слідчих дій, викликають необхідність проведення оперативно-розшукових заходів [45, с. 49-50]. Стосовно розглянутого виду злочинних деліктів, ми вважаємо за можливе, не вдаючись у полеміку, підтримати думку І.А. Возгрина, який вважає, що в методиках розслідування окремих видів злочинів рекомендації щодо поєднання слідчих дій і оперативно-розшукових заходів повинні ґрунтуватися на загальних організаційно-методичних принципах [45, с. 47].

Проведене дослідження показало, що в 78% випадків у процесі розслідування кримінальних справ про злочини виділеної категорії спостерігається позитивна тенденція спільного проведення слідчих дій і в 72% – спільне їх планування за участю слідчого й оперативного співробітника. Однак зміст плану конкретної слідчої дії залишає бажати кращого. Дотримуючись наявних розробок криміналістичної науки [131], у плані підготовки й проведення окремої слідчої дії по справах про комп'ютерні злочини в банківській сфері необхідно обов'язково вказувати таке: мету слідчої дії; питання, що підлягають з'ясуванню, або обставини, що підлягають встановленню; точний час проведення; місце проведення; коло осіб, які будуть надавати допомогу слідчому в його проведенні, розподіл обов'язків між ними; науково-технічні засоби, які будуть застосовуватися для фіксації її ходу й отриманих результатів (слідча валіза, фотоапарат, відеокамера, магнітофон, ЕОМ із програмним забезпеченням; або інші засоби електронно-обчислювальної техніки (ЗЕОТ), спеціальна пошукова й моніторингова апаратура тощо); тактика проведення слідчої дії; тактика її фіксації; несекретні оперативно-розшукові заходи супроводження, необхідні для її успішного проведення.

Вивчення криміналістичної літератури свідчить про те, що в цей час відсутні чіткі рекомендації щодо факультативного складу слідчо-оперативної групи (СОГ) у справах вказаної категорії. Акцентуючи уваги на цю обставину й беручи за основу методологічний підхід, запропонований В.Б. Вєховим

роботу ЕОМ банківської установи являє собою сукупність процесуальних і непроцесуальних дій особи, що проводить розслідування, спрямованих на встановлення відомих (слідчому) об'єктів, які мають значення для розслідування справи.

До числа основних об'єктів розшуку по справах про незаконне втручання в роботу ЕОМ банківської установи необхідно відносити: осіб, що вчинили незаконне втручання; знаряддя, які використовувались для вчинення незаконного втручання; комп'ютерну інформацію; спеціальну літературу, присвячену питанням вчинення незаконного втручання в роботу ЕОМ і проблемам комп'ютерної безпеки.

Серед основних пошукових ознак осіб, що вчинили незаконне втручання в роботу ЕОМ банківської установи, необхідно виділяти загальні ознаки (стать, вік, національність, прикмети, місце проживання, професія тощо) і спеціальні (володіння навичками в програмуванні, знання комп'ютерного устаткування, володіння певним комп'ютерним устаткуванням, дані залишені злочинцем про самого себе в різних комп'ютерних системах і мережах тощо).

Практика свідчить, що сьогодні існує принципова можливість розшуку комп'ютерного обладнання, використаного при вчиненні злочину. При цьому типовими пошуковими ознаками можуть бути: конфігурація комп'ютера, використаного для вчинення злочину; мобільність використаного комп'ютерного обладнання; наявність певного мережного або периферійного обладнання; установка на комп'ютері певного програмного забезпечення тощо.

маскуванні, фальсифікації, як традиційно досліджуваними криміналістикою способами (маскування зовнішності, дача неправдивих свідчень тощо), так і специфічними способами, пов'язаними з комп'ютерним обладнанням та інформацією (маскування й фальсифікація програмних продуктів, маскування місцезнаходження злочинця при віддаленому доступі до ЕОМ банківської установи, відновлення нормальної працездатності комп'ютера тощо). Протидія розслідуванню також може виражатися у впливі на його учасників або ухиленні від участі в розслідуванні.

Практика свідчить, що незаконне втручання в роботу ЕОМ в п'ять разів частіше здійснюється чоловіками. Причому, більшість суб'єктів даного злочину мають вищу або незакінчену вищу технічну освіту, а також іншу вищу або незакінчену вищу освіту. Серед них переважають особи у віці від 20 до 40 років.

Розробка класифікацій слідів-відображень, пов'язаних з інформаційними взаємодіями, і розгляд особливостей цих слідів дозволяє зробити такі висновки:

1) сліди, пов'язані з інформаційними взаємодіями, мають криміналістичну значимість і можуть використовуватися для з'ясування істини в кримінальній справі у випадку, якщо при вчиненні злочину використовувалася комп'ютерна техніка.

2) механізм утворення слідів, пов'язаних з інформаційними взаємодіями, ґрунтується на закономірностях функціонування конкретної файлової системи, програм і вимагає подальшого вивчення стосовно до файлових систем FAT 16 (операційні системи DOS, Windows), FAT 32 (операційні системи WINDOWS 95 і вище), NTFS (операційна система WINDOWS NT), іншим файловим системами, а також щодо системних і прикладних програм, що з'явилися.

3) документи на машинних магнітних носіях інформації є новим криміналістичним об'єктом, що має особливі властивості, і не дозволяють застосувати до даних об'єктів наявні визначення сліду й розроблені класифікації слідів.

4) розроблені класифікації слідів-відображень і виявлені особливості цих слідів можуть бути покладені в основу криміналістичних методик експертного дослідження документів та іншої інформації на магнітних носіях.

3. Результати проведеного нами аналізу слідчої практики показують, що такі слідчі дії, як огляд місця події, обшук та виїмка, допит, призначення експертиз є найбільш специфічними, типовими й значимими для розслідування комп'ютерних злочинів у банківській системі, особливо на початковому етапі досудового розслідування. Невідкладність проведення зазначених слідчих дій й організаційних заходів пояснюється тим, що саме вони спрямовані на встановлення події злочину, способу його вчинення, виявлення типових слідів, встановлення очевидців, встановлення злочинців та інших обставин, що, в кінцевому результаті, сприяють успішному розслідуванню досліджуваних нами злочинних зазіхань, справедливому покаранню винних і відшкодуванню збитку, заподіяного потерпілій стороні.

Пошукова діяльність слідчого по справах про незаконне втручання в

[38, с. 30-31], слід запропонувати такі методичні рекомендації щодо удосконалення діяльності СОГ.

Для проведення огляду місця події у справах про злочини в банківській сфері, які вчинені з використанням комп'ютерної інформації, залежно від конкретної слідчої ситуації до складу СОГ повинні входити такі особи:

– *обов'язкові учасники* – слідчий, що спеціалізується на розслідуванні кримінальних справ виділеної категорії (керівник СОГ); оперативні співробітники (КР, БЕЗ, податкової міліції, СБУ), працівники дізнання, що спеціалізуються на виявленні й розкритті злочинів розглянутої категорії; поняті (не менш двох чоловіків);

– *факультативні учасники* – спеціаліст-криміналіст, що знає особливості роботи зі слідами по злочинах даної категорії; спеціаліст із ЗЕОТ конкретного виду; спеціаліст із мережених технологій (у випадку наявності на місці події периферійного обладнання віддаленого доступу або локальної комп'ютерної мережі); спеціаліст із систем зв'язку (при використанні для дистанційної передачі даних каналів електрозв'язку); бухгалтер-ревізор конкретного профілю, що знає особливості електронного документообігу, або, як мінімум, користувач ЕОМ; спеціаліст ДНДЕКЦ або науково-дослідного інституту судових експертиз, співробітник оперативно-технічного підрозділу або приватної охоронної структури по профілю встановленого спеціального технічного пристрою; інспектор служби охорони або служби безпеки об'єкта, що оглядається, (у випадку, коли місце події або ЗЕОТ, що перебуває на ньому, одночасно є охоронюваним об'єктом).

При необхідності для участі в огляді місця події можуть бути запрошені й інші незацікавлені в справі спеціалісти, що знають специфіку роботи об'єкта, що оглядається, (предмета), а саме: інженери-електрики, спеціалісти супутникових систем зв'язку, оператори комп'ютерних систем і мереж (стільникових, пейджингових, Інтернет тощо).

Підбір понятих, що беруть участь у проведенні слідчого огляду місця події, ЗЕОТ, комп'ютерної інформації й «електронного» документу, а також при проведенні обшуку або виїмки з метою їх вилучення, доцільно здійснювати на підготовчому етапі до початку проведення слідчої дії з числа осіб, по-перше, не зацікавлених у справі, по-друге, що мають хоча б загальне уявлення про предмет, що вилучається або оглядається [226, с. 38].

Завершуючи першу стадію підготовчого етапу огляду місця події, слідчий повинен визначити, які техніко-криміналістичні засоби будуть використовуватися при огляді, і впевнитися в їх комплектності й справності. Аналіз практики показує, що найчастіше при огляді місця події у справах про комп'ютерні злочини в банківській сфері використовується фотографування, звукозапис і відеозапис. Викликає подив той факт, що як техніко-криміналістичні засоби у таких справах практично не використовуються паспортизовані: комп'ютерна техніка й спеціальне програмне забезпечення; пошукова апаратура для виявлення пристроїв негласного одержання інформації й впливи на неї; спеціальні свинцеві або алюмінієві контейнери, ZIP-Диски й інші технічні пристрої, призначені для вилучення (копіювання), безпечного зберігання й переміщення великих масивів комп'ютерної

інформації та їх носіїв. На думку багатьох фахівців, у справах розглянутої категорії слідча валіза (портфель) повинна бути додатково доукомплектована у такий спосіб. Крім стандартного набору приналежностей у ньому повинні перебувати: хімічні засоби виявлення й фіксації слідів пальців рук, що не мають у своєму складі магнітовмістких матеріалів (наприклад, сажа, прожарений порошок оксиду цинку тощо) – для роботи зі слідами, залишеними на магнітних носіях інформації й ЗЕОТ; спеціальні алюмінієві або свинцеві контейнери або побутова алюмінієва фольга (можливо, алюмінієва каструля з кришкою з того самого матеріалу) для грамотного вилучення магнітних носіїв машинної інформації, що виключають сторонній вплив електромагнітних і магнітних полів, здатних модифікувати й знищити вилучену комп'ютерну інформацію; паспортизовані машинні носії інформації, призначені для копіювання комп'ютерної інформації у випадку неможливості фізичного її вилучення разом з «рідним» носієм, упаковані в алюмінієву фольгу або контейнер; паспортизовані машинні носії інформації з відповідним ліцензованим програмним забезпеченням, необхідним для проведення огляду пам'яті ЗЕОТ і комп'ютерної інформації, що цікавлять слідство (системні завантажувальні програми, тестові, антивірусні детектори, здатні відновлювати стерті файли, визначати конфігурацію або внутрішню специфікацію ЗЕОТ, що оглядається, індивідуальні характеристики комп'ютерної інформації – розмір, дату створення, назву тощо).

Після прибуття СОГ на місце події починається друга стадія підготовчого етапу огляду. Особливу увагу необхідно приділити певним заходам безпеки, спрямованим на запобігання знищення речових доказів або їх втрати. З цією метою керівник СОГ повинен виходити з наявних методичних рекомендацій.

Після виконання цього слідчий повинен провести опитування осіб, які можуть дати яку-небудь нову інформацію про подію, що сталася. Особливу увагу необхідно звернути на категорію об'єкта огляду, на наявність ЗЕОТ і комп'ютерної інформації обмеженого доступу. У цьому випадку для проведення їх огляду й вилучення необхідний дозвіл судді, якою заздалегідь повинен заручитися слідчий. Зазначена обставина найбільш типова для юридичних осіб, що функціонують у таких сферах: відомствах і установах виконавчої влади, кредитно-банківської, послуг електрозв'язку, приватної охоронної діяльності.

Склавши для себе повне й чітке уявлення про подію, що сталася, слідчий повинен остаточно вирішити питання про коло учасників огляду (можливо, йому буде потрібно додатково викликати якихось додаткових фахівців, оперативних працівників або охорону), а також провести інструктаж учасників огляду, у якому визначити таке: роз'яснити кожному його функції і завдання, що конкретно він повинен робити, його права й обов'язки, запобіжні заходи при огляді ЗЕОТ, комп'ютерної інформації, роботі зі специфічними слідами тощо.

Після цього й повинен починатися безпосередній огляд місця події – його дослідницький етап, що, з урахуванням вимог наукової організації праці, в криміналістиці умовно поділяють на три стадії: загальний огляд (статична стадія), детальний (динамічна) і заключний (фіксація ходу й результатів

Організація інформаційно-технологічних систем на світовому рівні поряд з покращенням взаємодії ставить багато проблем. Організовані злочинні формування намагаються проникнути у виробництво програмного забезпечення і впливати на безпеку комп'ютерних мереж. Ці проблеми не можна не враховувати.

Просте управління комп'ютерами та водночас недостатня захищеність банківських комп'ютерних мереж від несанкціонованого доступу стає причиною розкрадання великої кількості коштів шляхом їх електронного переказу за вигадані послуги, з міжнародних банків усього світу на поточні рахунки до тих країн, де уряди не особливо турбують себе різними формами аудиторського контролю та іншими формами фінансової перевірки. Випадки крадіжок грошей за допомогою комп'ютерної техніки стають такими ж небезпечними злочинами, як викрадення дітей, вимагання, тероризм, торгівля наркотиками, зброєю, людьми тощо.

2. Злочини в сфері банківської комп'ютерної інформації відомі відносно недавно. Вітчизняна практика розслідування таких злочинів поки дуже невелика, оскільки лише в останні роки в результаті розвитку програмно-технічних засобів і підвищення «комп'ютерної освіченості», зовсім недавно інформаційні системи стали впроваджувати в такі галузі, як бухгалтерський облік, економічні розрахунки, банківська справа й ін. Суспільна небезпека злочинних дій у зазначеній сфері стає усе більш очевидною і досвід формалізації законодавцем головним чином закордонних криміналістичних знань про «комп'ютерні злочини» відбувається на наших очах.

Недоліки правової регламентації, законодавчого регулювання в даній галузі і дефіцит у слідчих, прокурорів, суддів, знань про сучасні інформаційні технології значною мірою сприяють збереженню високого рівня латентності протиправних дій в галузі інформаційних відносин та їх безкарності. Істотну допомогу у виявленні, розкритті і розслідуванні таких злочинів може зробити детальна розробка криміналістичної характеристики злочинів даного виду.

Криміналістична характеристика злочинів, вчинених у банківській системі України з використанням інформаційних технологій, відрізняється особливостями, специфікою й містить у собі: дані про предмет злочину; відомості про способи підготовки, вчинення й приховування злочину; дані про обстановку вчинення злочину; дані про особу злочинця, а так само відомості про «слідову картину».

Способи вчинення незаконного втручання в роботу ЕОМ банку доцільно поділяти на дві групи: 1) способи безпосереднього доступу і 2) способи віддаленого доступу до ЕОМ. Існування двох принципово різних за своїм характером способів незаконного втручання в роботу ЕОМ, кожний з яких має певну специфіку, обумовлює особливості пошукової діяльності по кожному з них.

Інформацію пошукового характеру можна одержати, вивчаючи типові способи протидії розслідуванню по розглянутій категорії кримінальних справ. Основне інформаційне навантаження несе спосіб приховання слідів злочину. Приховання по злочинах, пов'язаних із незаконним втручанням у роботу ЕОМ банківської установи, може виражатися в знищенні, утаюванні,

ВИСНОВКИ, ПРОПОЗИЦІЇ, РЕКОМЕНДАЦІЇ

Дослідження всього комплексу теоретичних і практичних проблем, пов'язаних із особливостями розслідування злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій, дозволяє сформулювати такі висновки, пропозиції та рекомендації:

1. Розвиток мережі комерційних банків з великими обсягами банківських фінансових операцій щодо переказів значних сум грошей між державними і комерційними структурами як в межах країни, так і за кордон, поставив питання про необхідність спрощення розрахунків шляхом впровадження в банківську систему електронної комп'ютерної мережі та інших сучасних технічних засобів комп'ютерної обробки інформації.

Введення мережі електронних розрахунків безумовно, певною мірою, призводить до зміни техніки вчинення злочинцями корисливих злочинів у сфері банківської діяльності, але в її основі є ті самі механізми паперового і електронного документообігу, що ґрунтуються на системі бухгалтерського обліку. Тому діюча сьогодні технологія вчинення злочинів у банківській системі може механічно перенестись також і в умови електронних розрахунків. Ця злочинність як для України, так і для світової спільноти набуває міжнародного характеру, а тому загрожує економічним основам, як нашої держави, так і світовій економічній системі. На погляд зарубіжних спеціалістів незаконне використання комп'ютерів дає більші прибутки з меншим ризиком, ніж звичайне пограбування банків, тому кількість таких злочинів з кожним роком у світі буде зростати.

Специфіка банківських автоматизованих систем, з точки зору їх вразливості, пов'язана в основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнорідними елементами. Вразливими є буквально всі основні структурно-функціональні елементи розподілених АБС: робочі станції, сервери, міжмережні мости, канали зв'язку.

Деякі банківські керівники пов'язують надійність електронних банківських систем із засобами їх зовнішнього захисту, тобто введенням системи шифрів (системи паролів) для входу не тільки в саму комп'ютерну мережу, а й до різних рівнів інформації банківської системи в залежності від допуску користувачів. Коло працівників, які за технологією виконання банківських операцій мають доступ до широкого діапазону цієї інформації, досить велике. Тому система захисту банківських електронних мереж, що ґрунтується тільки на кодуванні входів до різних видів інформації, малоефективна. Треба знайти принципово нові підходи для розробки відносно надійної системи захисту банківських комп'ютерних мереж. Така система повинна будуватися згідно з технологією банківського документообігу та особливостями форм розрахунково-кредитних операцій.

Протягом останнього десятиріччя в світі значно розширилися масштаби протизаконного використання ЕОМ саме при вчиненні економічних злочинів і особливо в банківському секторі.

огляду).

На стадії загального огляду вирішальне значення має складання плану розташування місця огляду щодо сусідніх з ним об'єктів і сторін світу; прив'язка місця події й основних предметів, що перебувають на ньому, до декількох постійних орієнтирів; попереднє визначення меж території, що підлягає огляду.

При розслідуванні справ про комп'ютерні злочини в банківській сфері дуже важливо правильно вирішити питання про вихідну точку огляду. У тактичному відношенні найбільш доцільною відправною точкою, на нашу думку, буде конкретний (встановлений оперативним або іншим шляхом) ЗЕОТ із комп'ютерною інформацією, що виступає як предмет або знаряддя вчинення злочину, що має максимально інформативні й численні сліди злочинної діяльності.

Аналіз емпіричних джерел слідчої практики показує, що в цьому випадку оптимально буде використовувати об'єктивний метод огляду, при якому відбувається суцільний огляд усього місця події. Найбільш доцільним є ексцентричний спосіб, коли огляд провадиться від центра до периферії, де центр – вихідна точка.

У процесі проведення огляду місця події бажано використовувати відео- або фотозйомку.

Після того як характер і розташування об'єктів будуть досліджені й зафіксовані, наприклад, складені схеми провідних з'єднань ЗЕОТ між собою, з засобами й каналами електрозв'язку, іншим периферійним обладнанням, починається друга стадія дослідницького етапу – детальний огляд кожного з виявлених предметів. При цьому допускається переміщення предмета, що оглядається, його розбирання й інші маніпуляції з ним, які продиктовані слідчою необхідністю [131, с. 249]. Таким чином, може бути розкритий корпус ЗЕОТ; відкритий захисний кожух друкуючого механізму принтера; знята передня панель банкомату, досліджена пам'ять ЗЕОТ і машинного носія інформації тощо. На цій стадії потрібно провести необхідні пошукові дії з метою виявлення на місці події й на окремих об'єктах, які оглядаються (документах, машинних носіях інформації, ЗЕОТ тощо) слідів злочину.

За наявності даних, що свідчать про вчинення злочину в банківській сфері з використанням комп'ютерної інформації, не зайвим буде проведення пошукових заходів з метою встановлення можливого технічного каналу витоку такої інформації й конкретного технічного пристрою. Для цього необхідно за участю спеціаліста з оперативно-технічного підрозділу з використанням спеціальної апаратури провести контроль радіоефіру, перевірити наявні на місці огляду засоби охоронно-пожежної сигналізації, телекомунікаційне обладнання тощо. Можливе проведення й інших пошукових заходів.

Як правило, на даному етапі проведення слідчої дії виникає нагальна потреба детального огляду й наступного вилучення ЗЕОТ, машинного носія інформації, комп'ютерної інформації (у тому числі машинного документа). Як показує аналіз проведеної нами методичної літератури, стосовно до предмета нашого дослідження оптимальними є рекомендації, які

запропоновані В.Б. Вєховим [38, с. 34-37], тому доцільно використовувати їх у повному обсязі.

На заключному етапі огляду місця події провадиться фіксація його ходу й отриманих результатів: повністю оформлюється протокол проведення слідчої дії; упаковуються виявлені й вилучені предмети й сліди; остаточно допрацьовуються плани, схеми й креслення; розглядаються зауваження, що надійшли від учасників огляду даної слідчої дії.

Правила, що регламентують діяльність слідчого на цій стадії огляду, докладно регламентовані чинним кримінально-процесуальним законодавством, досить широко висвітлені в криміналістичній літературі й не вимагають додаткових пояснень.

Відзначимо, що в протоколі слідчої дії необхідно вказати всі дії щодо виявлення й вилучення слідів і предметів огляду в тій послідовності, у якій він проводився, і в тому вигляді, у якому виявлене спостерігалося (наприклад, маніпуляції спеціаліста із ЗЕОТ, програмним забезпеченням і комп'ютерною інформацією; натискання клавіші керування ЗЕОТ та їх результат).

У протоколі обов'язково необхідно вказати всі застосовані для виявлення, фіксації, вилучення слідів та їх носіїв технічні засоби, включаючи програмне забезпечення: їх паспортні дані – тип, вид, марка або назва, заводський або реєстраційний (інвентарний) номер виробу, серію (модель), виробника тощо, умови й порядок їх використання (наприклад, при використанні ПЕОМ і програмного забезпечення зробити оцінку про те, що перед цим вони були протестовані спеціалістом на предмет відсутності в них шкідливих програмно-апаратних засобів – вказати паспортні дані засобу тестування), а також докладно описати сліди й об'єкти, на яких знаходяться ці сліди, в статиці щодо місць їх виявлення; умови й порядок їх вилучення й упакування.

Аналіз, проведений нами, спеціальної літератури, судової й слідчої практики показує, що дослідження різних видів документів, які виявлені в процесі огляду, мають важливе значення при розслідуванні досліджуваної категорії злочинів. Особливе доказове значення мають ті документи, які несуть у собі криміналістично значиму інформацію, необхідну для правильного розслідування кримінальної справи. Саме в конкретних документах банківської діяльності, як правило, виявляються криміналістичні ознаки комп'ютерних злочинів у банківський сфері, проявляються певні способи їх підготовки, вчинення й приховання, залишаються основні сліди злочинної діяльності, простежується шлях і хід її розвитку. Таким чином, ознайомлення із цими документами допомагає слідчому й оперативному працівникові висунути обгрунтовані версії про коло осіб, які брали участь або могли брати участь у підготовці, вчиненні і приховуванні злочину, намітити невідкладні слідчі дії й оперативно-розшукові заходи, скорегувати алгоритм розслідування.

При проведенні огляду документа важливо пам'ятати, що доказами по кримінальній справі можуть бути визнані тільки оригінали документів. Згідно з Державним стандартом (ДСТ) № 6.10.4-84 УСД «Придание юридической силы документам на машинном носителе и машинограмме, создаваемым

комп'ютерних системах і мережах тощо).

4. Слідча практика свідчить, що існує принципова можливість розшуку комп'ютерного обладнання, яке використовувалось при вчиненні злочину. При цьому основними пошуковими ознаками можуть бути: а) конфігурація комп'ютера, який використовувався для вчинення злочину; б) мобільність використаного комп'ютерного обладнання; в) наявність певного мережного або периферійного обладнання; г) установка на комп'ютері певного програмного забезпечення.

даних обчислювальних засобах, чи можлива робота користувача з документом при заданих умовах; встановлення ролі й робочого місця кожного з учасників події, наприклад, чи був документ підготовлений одним або декількома виконавцями (у робочій групі), які робочі місця й де обладнані програмами, необхідними для створення, обробки, накопичення, зберігання, поширення й надання споживачу документа, чи є непрямі ознаки, що свідчать про роботу з документом саме на даних робочих місцях; визначення умов, за яких відбувалася дія (подія), наприклад, які обставини сприяли знищенню документів на даному машинному носієві.

Встановлення причинного зв'язку подій, дій:

– встановлення причинного зв'язку між дією, що мала місце, (подією) і наслідками, що настали, наприклад, чи перебуває у причинному зв'язку модифікація документа й порушення працездатності обчислювальних засобів;

– визначення причини результатів, що настали, наприклад, яка причина порушення структури документа;

– визначення можливих наслідків щодо вчиненої дії, наприклад, які могли бути наслідки збереження документа одним із зазначених способів;

– визначення можливості вчинення дії або виникнення фактів (слідів) при певних умовах, наприклад, чи могли утворитися копії документа на машинному носієві без команди (без відома) користувача ЕОМ при роботі його з конкретною комп'ютерною програмою;

– встановлення відповідності (невідповідності) дій користувача спеціальним правилам, наприклад, чи правомірно конкретне використання документа на машинному носії, що містить персональні дані, чи суперечить порядку роботи з персональними даними.

Необхідно відмітити, що в межах розглянутих завдань може бути сформульована велика кількість окремих питань, які виносять на вирішення експертизи.

Результати проведеного дослідження дозволяють зробити такі висновки:

1. Пошукова діяльність слідчого при розслідуванні справ про незаконне втручання в роботу ЕОМ банківської установи являє собою сукупність процесуальних і непроцесуальних дій особи, що проводить досудове слідство, спрямованих на встановлення відомих слідчому об'єктів, що мають значення для розслідування справи.

2. До основних об'єктів розшуку по справах про незаконне втручання в роботу ЕОМ банківської установи варто відносити: а) осіб, що вчинили незаконне втручання; б) знаряддя, які використовувались для вчинення незаконного втручання; в) комп'ютерну інформацію; г) спеціальну літературу, присвячену питанням вчинення незаконного втручання в роботу ЕОМ і д) комплекс систем комп'ютерної безпеки.

3. Серед основних специфічних пошукових ознак осіб, що вчинили незаконне втручання в роботу ЕОМ банківської установи, можна виділяти: а) загальні ознаки (стать, вік, національність, прикмети, місце проживання, професія тощо) і б) спеціальні (володіння навичками в програмуванні, знання комп'ютерного устаткування, володіння певним комп'ютерним устаткуванням, дані залишені злочинцем про самого себе в різних

средствами вычислительной техники. Основные положения» оригіналом документу на довгому носії є перший за часом запис документу на машинному носії, а оригіналом машинограми – перший за часом надрукований ЗЕОТ екземпляр документу на паперовому носієві [72]. На практиці часто слідчим доводиться стикатися з небажанням керівників установ, організацій і підприємств, особливо кредитно-фінансових (банківських), надавати оригінали документів для огляду, а тим більше для їх вилучення, замість яких пропонуються їх ксерокопії або копії на машинних носіях. У цьому випадку необхідно проявити наполегливість і домогтися надання оригіналів, а юридичній особі залишити копії вилучених документів з копією протоколу слідчої дії. Необхідно також пам'ятати, що відповідно до чинного законодавства України, документи, що містять відомості конфіденційного характеру й мають відповідний гриф таємності («конфіденційно», «для службового користування» тощо), можуть бути оглянуті й вилучені слідчим тільки за згоди судді. Тому даний дозвіл необхідно одержати заздалегідь, особливо, якщо під час огляду передбачається досліджувати документи, що перебувають у банку або його структурному підрозділі, а також є поштово-телеграфною кореспонденцією (у тому числі «електронною» поштою).

На нашу думку, огляд документів по справах про комп'ютерні злочини в банківській сфері, виходячи із конкретних обставин, розслідування повинно передбачати такі основні цілі: перевірку дійсності документа; перевірку приналежності документа пред'явникові; виявлення ознак підробки документа; виявлення ознак інтелектуальної підробки; виявлення слідів, залишених на документі злочинцем і знаряддям злочину. Тактика проведення даної слідчої дії буде полягати в такому.

По-перше, оглядається загальний вид документа. З'ясовуються й описуються його найменування, призначення (наприклад, платіжне доручення, чек, облігація, кредитна картка, грошова купюра, паспорт тощо), форма (наприклад, у загальнодоступній формі або у формі машинного документа, у тому числі записаний у складних форматах), зовнішній вигляд (документ на паперовому носії або на машинному носії інформації), розмір та індивідуальні ознаки матеріального носія (або його реквізити), всі реквізити документа.

Нажаль, обсяг даної роботи не дозволяє нам докладно зупинитися на дослідженні всіх можливих груп документів, що підлягають огляду по справах про комп'ютерні злочини в банківській сфері, тому відзначимо лише найбільш специфічні з них. Умовно можна виділити такі загальні їх групи: первинні (вихідні) документи, що відображають ті виробничі операції, які привели або могли привести до утворення збитків або настання інших тяжких наслідків або в яких є сліди правопорушення; документи, що регламентують і визначають порядок виконання конкретної виробничої операції, повноваження й обов'язки конкретної особи при її виконанні, здійсненні контролю; документи, що регламентують і визначають порядок застосування ЗЕОТ і електронного документообігу та електронного цифрового підпису в конкретній виробничій операції (технологічному ланцюгу) і обов'язки

конкретної особи, відповідальної за конкретний ЗЕОТ, її програмне забезпечення й здійснення контролю за даним документообігом; документи, що регламентують категорію й тактико-технічні характеристики ЗЕОТ, комп'ютерної інформації й засобів їх захисту, використовуваних у конкретній виробничій операції; робоча документація конкретного ЗЕОТ і засобів його захисту (наприклад, журнал оператора, обліку роботи ЗЕОТ, його програмного забезпечення й засобів захисту, журнал обліку нестандартних аварійних ситуацій, технічний паспорт, журнал ремонту й технічного обслуговування, інструкція для експлуатації й проведенню окремих операцій, протоколи дій оператора, протоколи обліку роботи користувачів мережі тощо); документи, що фіксують питання дотримання технологічного процесу, що включає в себе конкретну виробничу операцію, належного виконання правил роботи й техніки безпеки на конкретному ЗЕОТ; документи по особовому складі, що фіксують прийом, звільнення, переведення, заохочення, стягнення, підвищення кваліфікації й навчання кадрів; особисті документи підозрюваного, у тому числі його професійні знання, що характеризують, уміння й навички, особистісні якості; цінні папери й гроші, у тому числі в безпаперовій формі (наприклад, електронні акції, кредитні й інші платіжні пластикові карти тощо).

Відомо, що реквізити документа умовно поділяються на дві категорії: постійні, що є складовою (а іноді, і єдиної) частиною бланка документа, і змінні (змінна частина реквізиту документа). До змінних реквізитів документа, як правило, відносять: рукописні (буквені, цифрові й змішані тексти, підписи та інші позначення); відбитки друкованих форм (печаток, штампів, телеграфних, телетайпних, факсимільних, контрольно-касових апаратів і пристроїв, машинописні тексти, у тому числі створені друкуючими ЗЕОТ); реквізити, що наклеюють (фотознімки, марки, захисні знаки й т.д.); ембосовані й перфоровані знаки (ті, що наносять, наприклад, компостером або ембосуючим пристроєм).

Особливістю огляду документа на машинному носії інформації (МНІ) і машинограми є таке: у відповідності з п. 1.6 ДСТ 6.10.4-84 запис документа на машинному носії й створення машинограми повинні провадитися на основі даних, зафіксованих у вихідних (первинних) документах, отриманих каналами електрозв'язку від автоматичних пристроїв, що реєструють, або в процесі автоматизованого вирішення завдань [72]. Це припускає спільний (або одночасний) огляд вихідних (первинних) документів, що перебувають в «електронній» формі в пам'яті ЗЕОТ і на МНІ, як правило, у складних форматах. Документ на машинному носії або машинограмі повинен містити такі обов'язкові реквізити, як найменування організації; місцезнаходження організації або поштова (мережева) адреса; найменування документа; дату його виготовлення; ідентифікаційний код особи, відповідальної за правильність виготовлення документа або особи, що затвердила документ. При повному автоматичному циклі створення документа допускається використання замість останнього із зазначених реквізитів ідентифікаційного коду прийомного або передавального автоматичного пристрою, що реєструє, при наявності технічних, програмних засобів і організаційних умов, що

1) при його безпосередньому дослідженні:

– встановлення змісту документа;

– дослідження властивостей документа та його ознак, у тому числі для встановлення їх відповідності певним характеристикам, заданим заздалегідь, наприклад, чи є документ вихідним кодом шкідливої програми для ЕОМ;

– коли були внесені останні зміни в документ і т.п.;

– визначення фактичного стану документа, наявність або відсутність у ньому відхилень від звичайного (нормального) стану подібних об'єктів. Наприклад, чи зберігає цілісність формат документа, чи має документ стороннє включення – тіло шкідливої програми для ЕОМ.;

– встановлення первісного стану документа, наприклад, де під яким ім'ям зберігався комп'ютерний файл перед його видаленням, які характеристики файлу;

– встановлення причин та умов зміни властивостей (стану) документа, наприклад, яким способом могли бути внесені зміни в документ;

2) за відображенням документа (дублікатом, копією, машинограмою або їх частиною (Термінологія наведена за ДСТ 6.10.4-84)):

– визначення ступеня інформативності відображення (дубліката, копії, машинограми або їх частини) документа, наприклад, чи зберігає дублікат, копія інформацію про формат, особливості документа;

– встановлення властивостей і стану відображення (дубліката, копії, машинограми) документа, наприклад, чи є машинограма, дублікат, копія повним або частковим відображенням документа;

– встановлення причини зміни зафіксованих властивостей відображення (дубліката, копії, машинограми) документа, наприклад, чи є особливість машинограми точним відтворенням особливості документа або слідством впливу деякої причини на роботу друкувального пристрою комп'ютера [72].

Інтегративне діагностування кримінальної ситуації на підставі дослідження результатів маніпулювання документом або його відображеннями: визначення механізму й обставин події, пов'язаної з наявним документом або його відображенням (дублікатом, копією, машинограмою, наприклад, чи можливо за виявленим документом, його відображенням (дублікатом, копією, машинограмою) встановити механізм впливу шкідливої комп'ютерної програми на обчислювальні засоби; визначення окремих етапів (стадій, фрагментів) події, наприклад, які дії виконує шкідлива комп'ютерна програма, що перебуває в тілі документа, з метою забезпечення подальшого «зараження» документів, а також приховання факту свого функціонування; виявлення механізму дії (події) у цілому, у тому числі й у його динаміці, наприклад, як впливає робота користувача із «зараженим» документом на документи, що перебувають на інших комп'ютерах локальної або глобальної мережі; визначення часу (періоду) виконання дії користувачем або хронологічної послідовності подій, наприклад, коли був створений оригінал документа, коли й у якій послідовності він піддавався незаконній модифікації, скільки часу потрібно для виконання конкретних дій з документом; визначення місця дії, локалізація його границь, наприклад, чи міг бути створений документ на

проведення слідчої дії, що супроводжується вилученням зазначених технічних пристроїв. Це пов'язане з тим, що у зв'язку з повсюдним використанням комп'ютерної техніки деякі знання втрачають значення спеціальних і стають загальнодоступними.

Деякі завдання, що входять до третьої групи, на нашу думку, не відносяться до завдань, що розв'язують шляхом експертизи, оскільки вивід комп'ютерної інформації на паперові носії є наслідком виконання вимог суду при використанні комп'ютерної інформації як доказу й обов'язковий етап проведення комп'ютерно-технічної експертизи (підготовка додатку до висновку експерта); вилучення програм і даних з оперативної пам'яті ЕОМ приведе до одержання неприпустимих доказів, оскільки можливе лише за умови навмисного знищення частини інформації, що міститься там (програма вилучення заміщає дані при розміщенні в оперативній пам'яті своєї копії).

Судова комп'ютерно-технічна експертиза документів на машинних носіях інформації у свою чергу може мати підвиди залежно від категорії досліджуваних об'єктів: наприклад, такий підвид, як судова комп'ютерно-технічна експертиза документів на машинних магнітних носіях інформації.

При формулюванні експертного завдання слідчий (суд) може вдатися до класифікації експертних завдань, запропонованої Ю.Г. Коруховим [126, с. 68]. Крім цього, він повинен взяти до уваги той факт, що документ на машинному магнітному носії інформації може мати копію на паперовому носії – машинограму, наявність якої полегшує вирішення експертного завдання.

З урахуванням даної класифікації варто сформулювати експертні завдання, розв'язувані за допомогою судової комп'ютерно-технічної експертизи документів на машинних магнітних носіях інформації.

До *ідентифікаційних завдань* віднесені:

– ототожнення оригіналу документа на машинному носії за наявності дубліката або копії документа на машинному носії (іноді, навіть при наявності тільки машинограми – паперової копії автентичного змісту);

– встановлення групової приналежності як у значенні встановлення загального джерела походження документів, так і з метою визначення класу програмного забезпечення або екземпляра комп'ютерної програми – представника даного класу програм, за допомогою якої створений документ.

До *класифікаційних завдань* віднесене встановлення формату документа (внутрішньої організації даних) за документом або його частиною. У силу кодованого характеру документа на машинному магнітному носії інформації класифікаційне завдання є визначальним, першорядним, оскільки без вирішення його не може бути встановлений навіть значеннєвий зміст документа. Внаслідок цього вирішення класифікаційного завдання відносно документа на машинному магнітному носії інформації дозволяє експертові або спеціалісту в першу чергу підібрати для прочитання вмісту документа комп'ютерну програму (спосіб), що використовує шуканий формат даних.

Діагностичні завдання систематизовані в такий спосіб.

Діагностичне вивчення властивостей і стану документа на машинному магнітному носії інформації.

виключають можливість несанкціонованого використання даного коду й повністю гарантуюча дійсність документа на машинному носії й машинограмі. Юридична чинність документа, збереженого, оброблюваного й переданого за допомогою ЗЕОТ, може підтверджуватися електронним цифровим підписом (ЕЦП). Юридична чинність ЕЦП визнається за наявності в автоматизованій інформаційній системі програмно-технічних засобів, що забезпечують ідентифікацію підпису, дотримання встановленого режиму їх використання й за наявності відповідної ліцензії.

По-друге, встановлюється юридична чинність документа, що оглядається: чи відповідає бланк документа сучасним діючим формам; ким і коли він виданий; як і ким складений; чи уповноваженою на це особою підписаний; які є відбитки печатки (штампа тощо) і що в них значиться; який термін дії документа.

По-третє, індивідуальні дані про предмет, фізичну (юридичну) особу, наявні в документі, що оглядається, порівнюються з аналогічними в документах або предметами, дійсність яких не викликає сумніву (наприклад, зображення особи на фотознімку кредитної карти з фотознімком паспорта конкретної особи й(або) з його зовнішністю; реквізити вихідної форми платіжного доручення – з аналогічними в «електронній» формі або навпаки тощо).

По-четверте, докладно досліджується зміст документа з метою виявлення ознак підробки: виправлення, підчищення, дописки, травлення, підробки відбитків печатки, неточність зображення водяних знаків, невідповідність барвників, паперу, захисної сітки, емблем та інших знаків (у тому числі захисних), установленим тим або іншим стандартом, розбіжність ембосованих знаків знакам, виконаним барвником, заміни фотографій, ламінованого шару та інші ознаки підробки й виготовлення документів з використанням знакосинтезуючих друкувальних пристроїв ЗЕОТ. Виявлені ознаки повної або часткової підробки документів далі перевіряються експертним шляхом.

У ході проведення слідчої дії обов'язково повинні використовуватися необхідні науково-технічні засоби й допомога спеціалістів. Документ, що оглядається, у кожному разі завжди фотографується. Документи-речові докази – необхідно приєднувати до справи використовувати відповідні прийоми і методи їх упаковки. При цьому їх не можна підшивати, робити на них які-небудь позначки, додаткові перегини, скріплювати клеєм, нитками, стиплером або іншим способом.

Процесуальні, тактичні, психолого-етичні аспекти проведення обшуку. Основна проблема, що виникає в ході обшуку полягає в тому, що суб'єкт, що проводить обшук, не може безпосередньо оглянути вміст машинного носія, оскільки останній являє собою, як правило, окрему намагнічену ділянку магнітного носія. Для вирішення даного завдання потрібно використовувати певну проміжну ланку, що дозволяє суб'єктові, який проводить обшук, всебічно й об'єктивно оцінити інформацію, що міститься на машинному носієві, тому питання про використання в ході проведення слідчих дій програмних засобів є важливими.

Необхідно підкреслити, що зазначені питання вже неодноразово висвітлювалися в криміналістичній літературі [119; 149, с.245-246, 250].

Так, В.В. Крилов вказує, що корисно для слідчого мати із собою при проведенні огляду місця події, обшуку й інших слідчих дій дискету (CD-диск, Flash-пам'ять) з набором сервісних програм, що забезпечують визначення властивостей і якостей комп'ютера; перевірку справності окремих пристроїв і зовнішньої пам'яті; роботу з файлами; інструмент для пошуку прихованої або вилученої інформації. Підбір таких програм проводиться на основі наукових рекомендацій і особистого досвіду слідчого [149, с. 250].

У цей час у зв'язку з величезними обсягами різноманітної інформації й значних розмірів самих програмних засобів помістити на дискети всі необхідні програми, навіть у тому обсязі, про яке говорить В.В. Крилов, буде практично неможливо.

Крім того, підбір програмних засобів здійснюється в процесі підготовки до проведення слідчих дій. Слідчий, як би добре він не знав ті засоби комп'ютерної техніки, які йому необхідно буде оглядати або вилучати, не може бути до кінця впевнений у тому, з якими саме технічними труднощами він може зіткнутися. Програмні технічні засоби розвиваються настільки швидко і стрімко, що може привести до досить важких наслідків у формі знищення значних обсягів інформації або втрати нею доказового значення. Тому в ході підготовки й проведення цих слідчих дій повинна активно використовуватися обов'язкова допомога спеціаліста в сфері сучасних комп'ютерних технологій.

Програмне забезпечення залежно від напрямів використання в ході огляду машинного носія інформації й ЕОМ варто поділяти на кілька груп:

– для одержання інформації про пристрої, що входять до складу ЕОМ і підключених до неї, у тому числі їх технічний стан;

– для одержання інформації про файлову структуру машинних носіїв інформації;

– для виявлення інформації, що перебуває на машинних носіях, шкідливих програм, як уже відомих та їх модифікацій, так і програм, які імовірно можуть бути шкідливими;

– для одержання інформації про програми, що функціонують на момент огляду та перебувають в оперативній пам'яті ЕОМ, про вміст буфера пам'яті ЕОМ;

– для перегляду й виводу на друк вмісту файлу.

Все наявне в цей час програмне забезпечення можна поділити на дві великі групи: спеціального та загального призначення. До останньої групи відносяться всі програмні засоби, що не мають прямого цільового призначення використання в забезпеченні діяльності правоохоронних органів.

На наш погляд, весь досвід роботи співробітників правоохоронних органів свідчить про необхідність створення спеціального програмного забезпечення для розслідування даних видів злочинів, заздалегідь закладаючи в нього функції, що необхідні для проведення огляду. Це дозволить слідчому уникнути вивчення значного масиву інших програм, спростить процес

комп'ютера й розміщених зловмисниками в ЕОМ з метою збору конфіденційної інформації [106].

Питання використання спеціальних знань при розслідуванні злочинів у сфері інформації розглядались й у працях В.В. Крилова, що вказувало на особливу роль спеціаліста та експерта в розслідуванні злочинів, який сформулював окремі питання, що підлягають вирішенню експертом, та підтримав О.Р. Росинську, інших вчених у питанні про необхідність існування комп'ютерно-технічної експертизи [147, с. 82]. В.В. Криловим виділено три групи слідчих та експертних завдань [149, с. 221-223]:

– діагностичного характеру, що ставляться, як правило, до машинних носіїв інформації;

– діагностичного та ідентифікаційного характеру, що ставляться, як правило, до комп'ютерної й задокументованої інформації;

– допоміжного (у тому числі лабораторного) характеру, щодо виявлення, закріплення й вилучення доказів.

У першу групу завдань входять:

– визначення найбільш важливих властивостей та ознак об'єкта, у тому числі функціональних, з метою встановлення, чи є він машинним носієм інформації, і якщо так, то в чому саме полягає його функція або їх сукупність – введення, зберігання, передача, обробка інформації й т.п.;

– оцінка властивостей й ознак машинного носія для встановлення якісних характеристик важливих для розслідуваної події – стану (наприклад, справний-несправний), призначення (наприклад, чи є це ЕОМ, мережею або системою ЕОМ) і особливостей (наприклад, чи призначений пристрій для роботи в мережі ЕОМ), відповідності нормативним вимогам (наприклад, чи збігається конфігурація пристрою запропонованій до нього документації).

У другу групу входять такі завдання:

– виявлення, оцінка й визначення властивостей та ознак стану й статусу комп'ютерної й задокументованої інформації (наприклад, чи є інформація програмою, чи не є програма шкідливою й т.п.), а також встановлення індивідуальних ознак інформації, що дозволяють визначити її автора;

– пошук конкретної комп'ютерної й задокументованої інформації, визначення слідів й ознак неправомірного впливу на неї й визначення ознак способу й механізму такого впливу.

До третьої групи входять такі завдання:

– вивід комп'ютерної інформації з машинних носіїв на паперові;

– вилучення програм і даних з оперативних запам'ятовувальних пристроїв ЕОМ, засобів зв'язку та інших машинних носіїв (пейджерів, телефонів, магнітних пластикових карт й ін.);

– дешифрування даних, зняття паролів захисту й ін.

При всій новизні представлена В.В. Криловим класифікація завдань має істотні недоліки і певною мірою ускладнює розглянуту проблему. По-перше, викликає заперечення формулювання деяких завдань першої групи: у сучасних умовах зовсім непотрібне призначення експертизи для встановлення, чи є об'єкт ЕОМ, мережею ЕОМ, машинним носієм інформації. Даний висновок робить сам слідчий або спеціаліст у ході

коригування з урахуванням сучасних особливостей виробництва комп'ютерів. Наприклад, міжнародний поділ праці, якість монтажу елементів електронних схем, існуюча практика нанесення позначень на друковані плати комп'ютера не дозволяють сподіватися на успішне вирішення завдання визначення місця й часу виготовлення комплектуючих або комп'ютера в цілому. Розповсюджена практика індивідуальної комплектації комп'ютера при його продажі (перепродажу) також не дозволяє сподіватися на успішне встановлення експертом факту внесення в конструкцію комп'ютера змін. Частина питань набуває значення при уточненні, з яким значенням необхідно порівнювати вимірюваний параметр технічного пристрою.

Доцільно уточнити формулювання експертного завдання на проведення технічної експертизи комп'ютерів та їх комплектуючих (згідно класифікації О.Р. Росинської):

1. Яка технічна назва (можливо, модель, серійний номер і т.п.) і призначення пристрою (комплекту апаратури), вилученого у гр. А.?

2. Чи є серед наданої документації документи на комп'ютер (обчислювальну мережу, периферійний пристрій, блок комп'ютера)?

3. Чи відповідає комплектність (технічні характеристики, окремі параметри, сервісні функції) наданого на експертизу комп'ютера (обчислювальної мережі, периферійного пристрою, блоку комп'ютера) стандарту або тій комплектності, що зазначено в документації або позначена в питанні слідчим)?

4. У чому полягають розходження між наявною комплектацією (технічними характеристиками, окремими параметрами, сервісними функціями) комп'ютера (обчислювальної мережі, периферійного пристрою, блоку комп'ютера) і комплектацією, зазначеної в документах (або позначеної в питанні слідчим)?

5. Чи працездатний комп'ютер (обчислювальна мережа, периферійний пристрій, блок комп'ютера, інший об'єкт)? Якщо ні, який характер несправності та її причини?

6. Чи є ознаки зносу комп'ютера (периферійного пристрою, блоку комп'ютера, іншого об'єкта)? Яка ступінь зносу?

О.Р. Росинською також були узагальнені питання, що вирішуються експертизою даних і програмного забезпечення [216, с. 174-175], обгрунтованість і коректність яких підтверджена експертною практикою.

У результаті розпочатих вченими зусиль були підняті й інші актуальні питання. Так, А.В. Касаткін у кандидатській дисертації розглянув проблему попереднього й експертного дослідження комп'ютерної інформації. Погодившись із назрілою необхідністю появи комп'ютерно-технічної експертизи, він відзначив загальні напрями криміналістичного дослідження технічних і програмних засобів комп'ютера: експертиза друкувальних пристроїв ЕОМ (принтерів); експертиза магнітних носіїв інформації; експертиза пристроїв, що забезпечують ввід й вивід інформації з магнітних дисків; експертиза спеціальних електронних пристроїв типу електронного ключа, службовців для ідентифікації користувача; експертиза апаратних заставних електронних пристроїв, що є позаштатною електронною начинкою

взаємодії слідчого з ЕОМ, скоротить час на проведення огляду й позбавить від значної частини рутинної технічної роботи, прямо не пов'язаної із процесом проведення слідчої дії. У цьому полягають основні переваги такого програмного забезпечення. Однак варто констатувати, що сьогодні програм, що мають цільове призначення для забезпечення діяльності правоохоронних органів, створюється вкрай мало, і на практиці в основному застосовуються стандартні програмні засоби.

Підготовка обшуку містить у собі попереднє одержання інформації про фактори, що здатні вплинути на результативність обшуку, зокрема:

– про особу що обшукується (соціальний статус, професія, зайняття, знання, уміння, навики, схильності, родинні зв'язки і коло знайомих, осіб, що з ним співпрацюють, проживають, наявність і місцезнаходження дачі, гаража, автомашини);

– про місце обшуку (планування квартири, будівлі, підсобних приміщень, ділянки місцевості, їх розміри, стан, наявність тварин тощо);

– про предмети, документи, цінності, знаряддя злочинів, що розшукуються (кількість, цінність, характерні ознаки, особливі характеристики і властивості, що обумовлюють зберігання), а також про живі особи, трупи;

– про передбачувані умови обшуку (приблизна тривалість, можливість запросити понятих, участь спеціаліста й застосування технічних засобів, використання спецодягу, необхідність забезпечити охорону об'єкта, безпеку учасників, транспорт, засоби зв'язку тощо).

Наявність упевненості слідчого в успішному проведенні обшуку визначається такими факторами:

– знання, що обшук добре підготовлений, призначений вчасно, для його проведення залучена достатня кількість учасників і є всі необхідні технічні засоби та методи;

– відмінна професійна підготовка слідчого, а при відсутності навичок у проведенні такого обшуку – знання, що в ньому будуть приймати участь досвідчені помічники й в обшуку беруть участь всі необхідні спеціалісти;

– уміння не реагувати на ознаки, що свідчать про можливу невдачу обшуку (убога обстановка, відсутність предметів розкоші, абсолютний спокій особи, що обшукується тощо);

– знання, що нерідко позитивні результати обшуку стають очевидними тільки в самому його кінці;

– не боятися майбутнього великого обсягу роботи й психологічно налаштуватися на проведення його в складних умовах.

Слідчий не повинен проявляти непевності, тому що це несприятливо може вплинути на діяльність інших учасників обшуку. З цією метою рекомендується:

– намагатися бути врівноваженим і не проявляти зовні свої емоції з приводу тривалої відсутності яких-небудь результатів обшуку;

– уникати яких-небудь висловлювань з приводу його результатів;

– намагатися своїм поводженням вселити особі, що обшукується, незважаючи ні на які труднощі, що предмет, який розшукується, буде

знайдено (подібним чином діють і методичність проведення обшуку, і наявність у розпорядженні слідчого розшукуваних засобів, значення яких роз'ясняється особі, що обшукується тощо);

– не зупинятися перед проведенням обшуку у складних умовах (забруднення приміщення, великий обсяг території, необхідність пошуку в антисанітарних умовах: туалетних кімнатах, сміттєвих і вигрібних ямах тощо), маючи для цієї мети спецодяг, потрібні технічні засоби і користуючись допомогою своїх помічників.

Необхідно зазначити, що проведення обшуку при розслідуванні даної категорії справ вимагає особливої концентрації уваги й спостережливості, а тому слідчий повинен:

– не приступати до обшуку у втомленому або збудженому стані, переборюючи хворобу або почуття голоду;

– уникати відволікаючих подразників (сторонні розмови, репліки, непотрібне ходіння учасників обшуку тощо);

– зосередитися на дослідженні об'єкта, що він у цей момент оглядає, не відволікатися, не думати про те, що потрібно буде зробити надалі, не приступати до огляду наступного предмета, не закінчивши дослідження попередніх;

– не поспішати й діяти у певній послідовності, оскільки квапливість і сумбурність обшуку викликають у його учасників роздратування, і, як наслідок цього, зниження уважності й зосередженості.

Психологія особи, що обшукується. На вибір місця для зберігання предметів злочинного посягання впливають риси характеру особи, що обшукується. З огляду на дану обставину, слідчому необхідно пам'ятати, що, як правило: завбачлива, акуратна людина ховає предмети злочину подалі й ретельніше; самовпевнений, легковажний суб'єкт не буде витрачати багато сил на приготування складних схованок; неуважна, ледача людина навіть при готуванні спеціального сховища допустить помилки, що сприяють найшвидшому виявленню розшукуваного; жадібний і недовірливий ховає близько, щоб можна було легко перевірити, чи на місці приховувані речі; недовірливий, навпаки, ховає предмети злочину подалі.

На вибір місця схову, а також й прийомів, які при цьому використовуються, впливають професійні й інші навички особи, що обшукується, її фізичний стан тощо. Це проявляється, зокрема, в такому: при виборі або спеціальному обладнанні сховища використовує свої професійні знання й інші навички, у тому числі ті, що є результатом власного захоплення (хобі), а також наявні в його розпорядженні інструменти й матеріали (так, більш імовірно, що особа, що вміє столярувати, влаштує схованку в дерев'яних предметах, а муляр – у цегельній стіні, сантехнік – в окремих місцях схову санвузла, бджоляр – у вуликах, садівник – у землі на присадибній ділянці тощо); фізично сильні, умілі люди можуть обладнати схованку у важкодоступних місцях, на більшу глибину закопати шукане в землю тощо.

Все перераховане стосується й родичів особи, в якої проводиться обшук, а також інших осіб, що проживають разом з ним.

мереж, а також причин виникнення збоїв у роботі вищевказаного обладнання; експертиза даних і програмного забезпечення, здійснювана з метою вивчення інформації, що зберігається в комп'ютері й на магнітних носіях [216, с. 173].

Були узагальнені питання, що вирішуються кожним видом комп'ютерно-технічної експертизи. Так, питання, що вирішуються технічною експертизою комп'ютерів та їх комплектуючих, мають діагностичний характер і такий зміст:

Комп'ютер якої моделі наданий на дослідження? Які технічні характеристики його системного блоку та периферійних пристроїв? Які технічні характеристики даної обчислювальної мережі?

Де й коли виготовлений і зібраний даний комп'ютер та його комплектуючі? Чи здійснювалася зборка комп'ютера у заводських умовах або кустарно?

Чи відповідає внутрішній пристрій комп'ютера й периферії технічній документації? Чи не внесені в конструкцію комп'ютера зміни (наприклад, установка додаткових вбудованих пристроїв: жорстких дисків, пристроїв для розширення оперативної пам'яті, зчитування оптичних дисків та ін., інші зміни конфігурації)?

Чи справний комп'ютер або його комплектуючі? Який їх знос? Які причини несправності комп'ютера й периферійних пристроїв? Чи не містять фізичних дефектів магнітні носії інформації?

Чи не проводилася адаптація комп'ютера для роботи з ним специфічних користувачів (лівша й ін.)?

Які технічні характеристики інших електронних засобів прийому, накопичення й видачі інформації (електронна записна книжка, телефонний сервер)? Чи справні ці засоби? Які причини несправностей? [216, с. 174].

Вилучена слідчим комп'ютерна техніка, як правило, повинна розглядатися в комплексі, як єдиний, складний, багатокомпонентний об'єкт дослідження. При проведенні експертного дослідження кожен компонент комплекту комп'ютерної техніки повинен бути перерахований у вступній й описаний у дослідницькій частині висновку експерта, подібно одиничному традиційному об'єкту судової експертизи. У цьому випадку модель пристрою, серійні та інші номери, марка процесора обсяг оперативної пам'яті й інша інформація, що індивідуалізує технічний пристрій, буде в обов'язковому порядку зазначена у висновку експерта, внаслідок чого відпадає необхідність додаткової постановки перед експертом подібних питань (тобто про комплектність складеного об'єкта судової експертизи).

Крім того, доцільно замість терміна «справність» (пристрою) використовувати більш влучний – «працездатність». Поняття справності передбачає багато критеріїв, причому не тільки відповідність технічних характеристик пристрою деяким заданим (паспортним чи іншим) параметрам, але й оцінку споживчих якостей пристрою. Наприклад, деякі нестандартні шуми можуть бути визнані, але можуть і не визнаватися ознакою несправності пристрою. Внаслідок різного трактування поняття справності експертом, слідчим, адвокатом, судом, у цій ситуації воно не може бути оцінене як вдале. Деякі питання, що ставляться перед експертом потребують

у справі, в галузі програмування як користувач [107, с. 93-94; 37, с. 151-152].

Виходячи із зазначених завдань, авторами наведені формулювання питань, які слідчий може поставити на вирішення експерта, при цьому підкреслювалося, що список питань не є вичерпним.

Звернемо увагу на те, що наведений вище перелік завдань, розв'язуваних програмно-технічною експертизою, є неповним і носить різнорідний, безсистемний характер (аж до інтерпретації завдань товарознавчої експертизи – п. 7), визначений невеликим масивом експертних висновків, а також складними окремими цілями, поставленими в ході розслідування конкретних кримінальних справ. На формування типових експертних завдань великий вплив зробили принципово нові можливості, що відкрилися перед експертами, дослідження раніше не досліджуваних властивостей нових об'єктів – засобів комп'ютерної техніки, комп'ютерних програм, машинних носіїв інформації й т.п. Важливо відзначити й те, що дослідженнями С.А. Каткова, І.В. Собецького, А.Л. Федорова та інших вчених на початку 90-х рр. було позначене початок етапу формування нового класу судової експертизи, до числа закономірностей якого відносяться:

– усвідомлення потреб слідчої та судової практики у проведенні судових експертиз, раніше невідомих суб'єктам судочинства й відсутніх у науковій класифікації;

– епізодичне проведення нової категорії експертних досліджень поза експертними установами спеціалістами-одинаками;

– початкове нагромадження емпіричного матеріалу й перші спроби його наукового аналізу й узагальнення;

– створення переліку експертних завдань, розв'язуваних новою судовою експертизою;

– формування переліку типових питань, що формулюють експертне завдання слідчого, суду, особи, що проводить дізнання. До 1996 р., завдяки науковому внеску, що внесла в становлення нового роду судової експертизи О.Р. Росинська, це завдання було в основному вирішене.

З урахуванням специфіки об'єктів дослідження О.Р. Росинська відійшла від назви «програмно-технічна експертиза», що звужує перелік об'єктів експертизи, і обґрунтувала іншу назву нової експертизи – «судова комп'ютерно-технічна експертиза» [216, с. 173]. Поняттям об'єкта комп'ютерно-технічної експертизи охоплюються комп'ютери в зборці, їх системні блоки, периферійні пристрої, комунікаційні пристрої комп'ютерів й обчислювальних мереж, магнітні носії інформації, роздруківки програмних і текстових файлів, словники пошукових ознак систем (тезауруси), класифікатори та інша технічна інформація, електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них [216, с. 176]. У загальноприйнятій класифікації експертиз комп'ютерно-технічна експертиза віднесена до класу інженерно-технічних експертиз.

У межах комп'ютерно-технічної експертизи О.Р. Росинською виявлені два види експертиз: технічна експертиза комп'ютерів та їх комплектуючих, що проводиться з метою вивчення конструктивних особливостей і стану комп'ютера, його периферійних пристроїв, магнітних носіїв, комп'ютерних

З урахуванням зібраної інформації визначається тактика проведення зазначеної слідчої дії:

1. Визначається час початку обшуку, а також заходи, що забезпечують його раптовість і конфіденційність. У випадку наявності інформації про знаходження на комп'ютері даних, що свідчать про причетність його власника до вчинення злочину, починати обшук краще в той час, коли можливість роботи на ньому зведена до мінімуму.

2. Проконсультувавшись із спеціалістами, визначити, яка інформація може перебувати на комп'ютері, і підготувати відповідну техніку для її копіювання. Визначити можливі заходи безпеки, що використовуються злочинцями з метою знищення доказів у справі.

3. Підібрати понятих, які розбираються в комп'ютерній техніці (основних операціях, назвах комп'ютерних програм тощо), щоб виключити можливість заперечування в суді правильності проведеної слідчої дії і його результатів.

Специфічність і складність маніпуляцій з комп'ютерною технікою для непосвяченої людини можуть нівелювати зусилля слідчого щодо закріплення виявленої доказової інформації. Нерозуміння значення всіх дій понятими може переконати суд у визнанні неприпустимими зібрані докази.

4. Виходячи із кваліфікації й професійних навичок власника комп'ютера, доцільно залучити відповідного спеціаліста з комп'ютерної техніки, що візьме участь у слідчій дії.

З урахуванням специфіки досліджуваного злочину після прибуття на місце обшуку або огляду необхідно:

– швидко й зненацька увійти в приміщення, щоб звести до мінімуму можливість знищення інформації, що перебуває на комп'ютері. У деяких випадках, коли це можливо й доцільно, безпосередньо перед входом до приміщення, в якому необхідно провести обшук, варто знеструмити його;

– не дозволяти, кому б то ні було з осіб, що працюють на об'єкті обшуку, або іншим особам, доторкатися до працюючих комп'ютерів, магнітним носіям, включати й виключати комп'ютери, за необхідності перевести персонал в інше приміщення;

– не дозволяти кому б то ні було з персоналу виключати або включати електропостачання об'єкта; якщо перед початком обшуку електропостачання було виключено, то до його підключення варто відключити від електромережі всі комп'ютери й периферійні пристрої;

– не провадити ніяких маніпуляцій з комп'ютерною технікою, якщо їх результат заздалегідь невідомий.

Після виконання перерахованих заходів необхідно зробити попередній огляд комп'ютерної техніки з метою визначення, які програми працюють у цей момент. У випадку виявлення працюючої програми по знищенню інформації, вона зупиняється, і огляд починається саме із цього комп'ютера.

Якщо комп'ютери, що перебувають у приміщенні, з'єднані в локальну мережу, їх огляд доцільно почати із сервера, потім оглядають працюючі комп'ютери, а потім іншу комп'ютерну техніку й джерела живлення. (У цьому випадку й далі під оглядом розуміється огляд комп'ютерної техніки й визначення пристроїв, які підлягають вилученню.)

При огляді працюючого комп'ютера необхідно:

– визначити, яка програма виконується в цей момент. Для цього вивчається зображення на екрані дисплея й детально описується в протоколі. За необхідності може проводитися фотографування або відеозапис зображення на екрані дисплея;

– зупинити виконання програми й зафіксувати в протоколі результати своїх дій, відобразити зміни, що відбулися на комп'ютері;

– визначити наявність у комп'ютера зовнішніх пристроїв-накопичувачів інформації на твердих магнітних дисках (вінчестері), на дискетах і пристроях типу ZIP, наявність віртуального диска (тимчасовий диск, що створюється при запуску комп'ютера для прискорення його роботи), відобразити отримані дані в протоколі;

– визначити наявність у комп'ютера зовнішніх пристроїв віддаленого доступу до системи й визначити їх стан (підключення до локальної мережі, наявність модему), після чого відключити комп'ютер з мережі й виключити модем, відобразити в протоколі результати своїх дій;

– скопіювати програми й файли даних, створені на віртуальному диску (якщо він є), на магнітний носій або на жорсткий диск комп'ютера в окрему директорію;

– виключити комп'ютер і далі діяти відповідно до положень, які розглянуті нами щодо огляду непрацюючого комп'ютера.

При огляді непрацюючого комп'ютера необхідно:

– відобразити в протоколі й на схемі, яка до нього додається, місцезнаходження комп'ютера і його периферійних пристроїв (принтера, модему, клавіатури, монітора тощо);

– відобразити в протоколі призначення кожного пристрою, назву, серійний номер, комплектацію (наявність і тип дисководів, мережних карт й ін.), наявність з'єднання з локальною обчислювальною мережею й (або) мережами телекомунікації, стан пристроїв (ціле або зі слідами зламу);

– точно описати порядок з'єднання між собою зазначених пристроїв, за необхідності, відмітити сполучні кабелі й порти їх підключення, після чого роз'єднати пристрої від комп'ютера;

– у ході огляду комп'ютера необхідно за допомогою спеціаліста встановити наявність всередині комп'ютера вмонтованої позаштатної апаратури, вилучення мікросхем, відключення внутрішнього джерела живлення (акумулятора);

– упакувати (із вказівкою в протоколі місця їх виявлення) магнітні носії на дискетах і стрічках. Для пакування можуть використовуватися як спеціальні футляри для дискет, так і звичайні паперові й целофанові пакети, що виключають вплив бруду й т.п. на робочу поверхню дискети або магнітної стрічки;

– упакувати кожний пристрій комп'ютера й сполучні кабелі. Попередньо, для виключення доступу сторонніх осіб, необхідно опечатати системний блок – заклеїти стрічкою кнопку включення комп'ютера й гніздо для підключення електрокабеля, а також місця з'єднання бічних поверхонь із передньою й задньою панелями.

інформація, адресні дані); проблема інформування слідчих підрозділів про наявність таких спеціалістів.

Проведені нами узагальнення свідчать про те, що сьогодні дослідження в цьому напряму в Україні не проводяться, а практика змушена самостійно розв'язувати виникаючі питання.

Безумовно, досягнення поставленої мети – формування професійних кадрів спеціалістів в галузі комп'ютерних технологій – вимагає часу, аналізу актуальних проблем і розробки шляхів їх вирішення. Однак процеси, що відбуваються в даний час у сфері використання нової галузі спеціальних знань, у найближчому майбутньому дозволять ефективно поєднати професіоналізм штатних співробітників державних судово-експертних установ і високий правовий рівень їх діяльності як спеціалістів на етапі досудового розслідування злочинів.

Розглядаючи участь спеціаліста в розслідуванні злочинів, вчинених з використанням комп'ютерної техніки, у цілому, і використанням документів на машинних магнітних носіях інформації, зокрема, ми жорстко обмежили його функції виявленням, фіксацією, вилученням доказів. Тим самим ми позначили свою позицію, відповідно до якої при розслідуванні цієї категорії злочинів одним з основних процесуальних способів одержання доказів вважаємо комплекс судових експертиз, які забезпечать дослідження комп'ютерної техніки, документів й іншої інформації на машинних магнітних носіях.

Практику підготовки й призначення «програмно-технічних експертиз» в 1995 р. узагальнили С.А. Катков, І.В. Собецький, А.Л. Федоров. Вивчення ними експертної практики показало, що за допомогою програмно-технічної експертизи найчастіше вирішувалися такі типові експертні завдання:

– встановлення факту відтворення й роздруківки всієї або частини (по певних темах, ключовим словам і т.п.) інформації, що міститься на фізичних носіях засобів комп'ютерної техніки, у тому числі, яка знаходиться в нетекстовій формі (у складних форматах мов програмування), наприклад, у формі електронних таблиць, баз даних, Windows тощо;

– відновлення інформації, що раніше містилася на фізичних носіях засобів комп'ютерної техніки й згодом стертої (знищеної) або зміненої (модифікованої) з різних причин;

– встановлення часу введення, зміни, знищення або копіювання тієї чи іншої інформації (документів, файлів, програм і т.д.);

– розшифровка закодованої інформації, підбір паролів і розкриття системи захисту засобів комп'ютерної техніки;

– встановлення виду й конкретних технічних засобів, на яких велася підготовка й виготовлення документів (файлів, програм і т.д.);

– встановлення можливих каналів витоку інформації з комп'ютерних мереж;

– визначення технічного стану, справності засобів комп'ютерної техніки, відсотка їх зношування, оцінки їх вартості, а також адаптації засобів комп'ютерної техніки під конкретного користувача;

– встановлення рівня професійної підготовки окремих осіб, що проходять

у проведенні необхідних на початковому етапі розслідування слідчих дій.

Слідча практика засвідчує, що на початковому етапі розслідування повинні використовуватися такі спеціальні знання спеціаліста:

– при підготовці до проведення окремих слідчих дій: для наукового консультування слідчого з питань визначення «комп'ютерної» специфіки слідчої дії, визначення його конкретної мети, способів й прийомів їх досягнення; для надання допомоги слідчому при підборі понятих, що мають відповідну підготовку в галузі комп'ютерних технологій, для адекватного сприйняття ними проведених слідчим і спеціалістом окремих дій;

– при огляді місця події, обшуку й виїмці: для виявлення засобів комп'ютерної техніки, які використовувались зі злочинною метою, її окремих компонентів, документації, інших об'єктів, які можуть містити сліди неправомірних дій; для коректного завершення роботи програм або контролю за ними; для наступного коректного відключення засобів комп'ютерної техніки від енергопостачання; для надання допомоги слідчому в описі специфічних ознак засобів комп'ютерної техніки, що вилучають, її окремих компонентів і документації; для надання допомоги слідчому при вирішенні питання визначення конкретного комплекту комп'ютерної техніки або окремих її компонентів, що підлягають вилученню або ізолюванню від вільного доступу; для надання допомоги слідчому в підготовці засобів комп'ютерної техніки до транспортування (їх упаковки, опечатуванні);

– при допиті, очній ставці, відтворенні обстановки і обставин події: для надання допомоги слідчому при його спілкуванні з особою, що використовує професійну «комп'ютерну» термінологію тощо.

Вказані вище вимоги, які запропоновані до професійних знань спеціаліста, потребують відзначити таке. Накопичення, узагальнення й активне застосування спеціальних знань при розслідуванні злочинів з використанням комп'ютерної техніки можливе тільки в тому випадку, якщо буде залучений до розслідування постійний контингент спеціалістів, які мають знання в галузі комп'ютерних технологій. Дані фахівці повинні відповідати таким професійним критеріям: мати необхідний обсяг програмно-технічних знань, необхідних для пошуку, фіксації й вилучення «комп'ютерних» слідів злочину; мати належні документи, що підтверджують їх кваліфікацію; вони повинні проходити періодичну професійну перепідготовку й підвищення кваліфікації; перебувати в штатах відповідного підрозділу правоохоронного органу й на постійній основі брати участь у слідчих діях як спеціаліст в галузі комп'ютерних технологій.

У цей час багато проблем, пов'язаних з формуванням зазначених підрозділів, залишаються невирішеними. Частина з них носить невідкладний характер: проблема визначення переліку кваліфікаційних вимог, пропонованих до спеціалістів цієї категорії; проблема створення кваліфікаційних комісій для атестації спеціалістів; проблема проведення атестацій даних спеціалістів; проблема постійної поглибленої спеціалізації фахівців (комп'ютерні мережі, периферійні пристрої, комп'ютерна поліграфія, інше); проблема створення регіональних і загальнодержавних баз даних осіб, які мають знання, навики і уміння в цій галузі (кваліфікаційна

Якщо в ході огляду й вилучення комп'ютерної техніки виникає необхідність включення комп'ютера, його запуск необхідно здійснювати із заздалегідь підготовленої завантажувальної дискети, виключивши тим самим запуск програм користувача.

Проведене нами узагальнення слідчої практики показує, що найбільш типовою слідчою дією по справах про комп'ютерні злочини в банківській сфері є *допит свідків*. Основна особливість проведення зазначеної слідчої дії щодо злочинів, які ми досліджуємо, полягає в тому, що суб'єктом допиту, як правило, є представник потерпілої сторони або інша особа тим або іншим способом пов'язана з цією діяльністю. Адже потерпілою стороною від розглянутих злочинів здебільшого є юридична особа, тому така слідча дія, як допит потерпілого, нами окремо не виділяється й розглядається в контексті допиту свідків.

Відомо, що сутність допиту як слідчої дії полягає у вивченні показань про обставини, що мають відношення до розслідуваної події, і їх фіксації у встановленому законом порядку. Чинний кримінально-процесуальний закон досить докладно регламентує порядок підготовки й проведення допиту, права й обов'язки особи, що провадить допит, і допитуваних ним осіб. Основні процесуальні, криміналістичні, психологічні й етичні аспекти допиту досить повно досліджувалися.

На перший погляд, проведення допиту не представляє особливих труднощів. Однак варто погодитися з положенням про те, що ця легкість лише оманлива, оскільки допитувані далеко не завжди дають правдиві, повні й об'єктивні показання, тому дуже часто одержати об'єктивні відомості вдається лише після тривалих, наполегливих зусиль слідчого, у результаті вмілого застосування цілого ряду тактичних прийомів. При розслідуванні комп'ютерних злочинів у банківській сфері слідчі нерідко зіштовхуються зі значними труднощами об'єктивного й суб'єктивного характеру, що відображається на змісті тактики проведення багатьох слідчих дій, включаючи допит свідків. Ускладнюють ситуацію недосконалість і відносна новизна кримінального законодавства, а також суперечливість чинного законодавства, що регулює правовідносин як у банківській сфері, так і в сфері комп'ютерної інформації. Таким чином, тактика проведення допиту свідків по справах про комп'ютерні злочини в банківській сфері буде мати певні особливості.

Підготовчий етап допиту свідків по справах про комп'ютерні злочини в банківській сфері має дуже велике значення й багато в чому визначає результативність даної слідчої дії. Відзначимо найбільш значимі, на наш погляд, його компоненти.

При визначенні кола обставин, що підлягають з'ясуванню в ході допиту свідка, слідчому необхідно докладно проаналізувати наявні в справі матеріали, продумати план проведення слідчої дії й конкретизувати версії, які необхідно відпрацювати.

З огляду на відсутність у цей час у переважної більшості слідчих необхідних спеціальних знань по справах даної категорії, при підготовці до допиту свідків їм треба значну увагу приділяти вивченню спеціальних

питань, які можуть виникнути в ході його проведення. З цією метою перед початком допиту слідчий повинен вивчити спеціальну літературу; проконсультуватися з відповідним спеціалістом; ще раз ознайомитися з результатами огляду місця події, документів та інших предметів, освіжити в пам'яті їх зовнішній вигляд, конструктивні, функціональні, технологічні й інші особливості; ознайомитися з особливостями виробничого процесу й технологічним режимом конкретної установи, підприємства або організації. Особлива увага з боку слідчого повинна бути приділена спеціальним знанням в галузі електронного документообігу, режиму конфіденційності комп'ютерної інформації, засобів і методів її захисту й безпечної обробки.

При визначенні кола учасників допиту необхідно враховувати таку обставину.

Оскільки кількість осіб, яких можливо використовувати як свідків по таких кримінальних справах, як правило, досить велика, при визначенні кола й черговості їх допитів варто виходити з обсягу даних, які вони можуть мати, і сформованої на даний момент слідчої ситуації. Так, при встановленні суб'єкта, що вчинив або можливо вчинив злочин, необхідно в першу чергу допитати: осіб, що брали участь у викритті злочинця (оперативних працівників, посадових осіб, співробітників служби безпеки, ревізорів, контролерів, операторів, касирів, інспекторів, адміністраторів мережі й баз даних тощо); знайомих і родичів підозрюваного; осіб, знайомих зі службовою діяльністю підозрюваних, які навіть, можливо, виконували певні дії в їх інтересах, але не стали співучасниками злочину; безпосередніх начальників підозрюваного (на місці вчинення злочину, місці події).

Допитати якомога швидше вищевказаних осіб необхідно з таких причин. По-перше, тому, що підозрювані завжди знають таких осіб і, як правило, мають можливість особисто або через посередників (у тому числі невідомих слідству співучасників злочину) спілкуватися з ними. Користуючись цим, вони можуть намагатися залякати, розжалобити або підкупити свідків і таким чином схилити їх до дачі неправдивих свідчень, відмовитись від дачі показів або дачі неповної і неточної інформації при допиті. По-друге, їх покази при вмілому використанні можуть зробити сильний психологічний вплив на підозрюваного. За допомогою такого роду показів свідків слідчому нерідко вже на самому початку розслідування вдається переконати підозрюваного в тому, що єдиний вихід для нього – зізнатися у вчиненому; повністю або частково уникнути конфліктну ситуацію.

В інших випадках, коли особа, що вчинила злочин, не встановлена, у першу чергу необхідно допитати як свідка таких осіб:

– заявника (потерпілого або представника потерпілої сторони);

– особи, яка виявила ознаки складу злочинів (оперативних працівників, посадових осіб, співробітників служби безпеки, ревізорів, контролерів, операторів, касирів, інспекторів, адміністраторів мережі й баз даних й ін.);

– осіб, безпосередньо відповідальних за конкретну ділянку роботи (конкретну операцію, технологічний цикл або процес), на якому були виявлені сліди злочину; осіб, безпосередньо не відповідальних за дану ділянку роботи, але в силу своїх службових обов'язків мають владно-

додаткового пристрою.

На жаль, перелік подібних прикладів досить об'ємний, оскільки включає рекомендації багатьох авторів [38, с. 159, 160; 65; 147, с. 75, 78, 80; 149, с. 249], при цьому кількість спірних моментів у них зростає в геометричній прогресії.

Вважаємо, що, оскільки є багато різнобічних, а деколи взаємовиключаючих позицій, то необхідно висловити свою оцінку даної проблеми.

По-перше, стрімке ускладнення технічних і програмних компонентів комп'ютерної техніки, комп'ютерних технологій у цілому унеможливлює одноособове використання слідчим найефективніших рекомендацій технічного характеру. Крім того, всі рекомендації фактично є спробою вирішення завдання прогнозування слідчої ситуації в умовах невизначеності (тип комп'ютера, характер розв'язуваних з його допомогою завдань, склад технічного й програмного забезпечення, наявність або відсутність мережі комп'ютерів, програмних або технічних засобів захисту інформації, багато чого іншого до проведення початкових слідчих дій невідомо й одночасно повинне бути враховане слідчим або спеціалістом саме як комплекс факторів, що визначають послідовність і зміст дій зазначених осіб).

По-друге, більша частина рекомендацій потребує від слідчого знань, навичок і умінь, формування яких не передбачене програмами підготовки й перепідготовки слідчих у навчальних закладах, а тому самостійне одержання їх шляхом самопідготовки, самоосвіти це не реально.

По-третє, експериментальні дослідження, які проведені нами, свідчать про недоцільність, а часом і про шкідливість окремих таких рекомендацій: багато розповсюджених програм, що працюють під керуванням операційної системи MS DOS, мають здатність схованих взаємодій з файловою системою комп'ютера, в результаті чого утворюються криміналістично значимі сліди. Будь-який запуск такої програми слідчим або спеціалістом на місці події спричинить безумовну й приховану зміну (перекручування) слідової картини; операційні системи Windows 95 і вище, а також більшість програм, що працюють під їх управлінням, крім здатності схованих взаємодій з файловою системою комп'ютера містять різні механізми відстеження станів програм і документів. Запуск комп'ютера з таким програмним забезпеченням сам по собі тягне безумовну й приховану зміну (перекручування) слідової картини.

Таким чином, властивості найпоширенішого програмного забезпечення комп'ютерів дозволяють зробити висновок про заборону в категоричній формі будь-яких маніпуляцій з комп'ютерною технікою на місці події, за винятком коректного її вимикання. Фіксація «комп'ютерних» слідів злочину можлива тільки за допомогою коректного завершення працюючих програм, вимикання комп'ютера й кваліфікованого вирішення завдання з визначення комплекту комп'ютерної техніки або окремих її компонентів, що підлягають обов'язковому вилученню слідчим.

Сформульовані пропозиції, на наш погляд, дозволять слідчому уникнути невизначеності і багатозначності початкової слідчої ситуації, допоможе йому точніше визначити конкретні функції спеціаліста, який залучається до участі

накопичення знань про закономірності функціонування комп'ютерних систем і про процедури роботи з комп'ютерною інформацією. Розуміючи це, В.Б. Вєхов ще раніше звертав увагу на необхідність постійного підвищення спеціальної кваліфікації співробітників правоохоронних органів, а також необхідність створення спеціальних підрозділів з боротьби з комп'ютерною злочинністю та використання штатних спеціалістів в цій галузі в кожному підрозділі правоохоронних органів [37, с. 147, 155].

Пізніше свій вклад в розробку рекомендацій слідчим щодо проведення окремих слідчих дій при розслідуванні «комп'ютерних» злочинів внесли П.Д. Біленчук, М.В. Гаврилов, В.О. Голубєв, В.І. Комісаров, В.В. Крилов, В.А. Мінаєв, Л.П. Паламарчук, В.Ю. Рогозін, О.Р. Росинська, М.В. Салтевський, О.П. Снігерьов, В.С. Цимбалюк та інші вчені [29; 54; 60; 119; 149; 185; 216; 223].

Оскільки ці конкретні рекомендації всебічно висвітлені в літературі, відзначимо тільки їх специфічні особливості.

1. Багато авторів цілком обґрунтовано адресують свої рекомендації спеціалістам, що залучаються до участі у проведенні слідчих дій. Причину такого підходу коротко й точно визначили В.Д. Курушин і В.А. Мінаєв, які вказують, що комп'ютер, будучи складною електронною системою, може сам виступати в ролі речового доказу, тому огляд й поводження з ним вимагають спеціальних знань. При втручанні некваліфікованого співробітника можуть виникнути серйозні й значні проблеми, що мають дуже негативні наслідки для слідства. Безумовно, що розслідування даних видів злочинів із самого початку вимагає негайного залучення кваліфікованого спеціаліста з комп'ютерних систем [152]. Однак деякі автори адресують свої рекомендації в основному слідчим [38, с. 156-161; 106; 147, с. 72-81; 223].

2. Окремі рекомендації орієнтовані на особливості функціонування конкретних технічних засобів, програмних засобів і технологій у цілому, мають аргументи як «за», так і «проти», але не мають необхідного ступеню універсальності, оскільки суперечать один одному. Прикладом подібних рекомендацій є такі: визначення останньої програми, що виконувалася, по розташуванню курсору в менеджері файлів (Norton Commander) при огляді включеної комп'ютерної техніки на місці події; дозвіл обмежених маніпуляцій із клавіатурою включеного комп'ютера (крім вирішення завдання коректної зупинки програм) з фіксацією дій та їх результатів у протоколі огляду; вилучати всі засоби комп'ютерної техніки, що перебувають у приміщенні об'єкта, незалежно від їх юридичної приналежності; передбачати можливість зростання в ході обшуку напруги статичної електрики; копіювати програми й файли даних, збережених на віртуальному диску, на магнітний носій; роздруківка на папір інформації, що з'являється на екрані дисплея, як спосіб фіксації даних з оперативної пам'яті; роздрукування даних, виявлених на машинних носіях, безпосередньо в ході огляду; зазначення в протоколі огляду місця події при зупиненні програм, що виконуються на комп'ютері, – яка програма виконувалася і яка інформація отримана після закінчення її роботи; перевірка наявності в системному блоці додаткових проводів як ознаки розкрадання інформації шляхом підключення

розпорядницькі функції стосовно конкретного працівника (наприклад, безпосередній начальник);

– осіб, що працюють на конкретній виробничій ділянці або забезпечують проведення операції (виробничого циклу або технологічного процесу) у силу своїх службових обов'язків або технології виробництва (включаючи співробітників суміжних організацій);

– осіб, що безпосередньо забезпечують технічно задане технологічне функціонування конкретного ЗЕОТ, його програмного забезпечення, засобів захисту й безпеки (які проводили пусконалагоджувальні роботи, розробку й супровід програмного забезпечення, засобів і систем електрозв'язку ЗЕОТ, ремонт і технічне обслуговування, регламентні роботи, перевірку безпеки комп'ютерної системи й відповідності її технічних параметрів вимогам діючих нормативних правил і керівних документів й ін.).

На підготовчому етапі допиту свідків певну увагу варто також приділити визначенню необхідних матеріалів, які будуть пред'являтися допитуваному в ході його проведення. Документи ЗЕОТ та інші предмети, у тому числі речові докази, які передбачається пред'явити в ході допиту, необхідно заздалегідь підготувати, наприклад, зробити закладки в об'ємних за змістом документах, а самі документи й інші предмети розташувати поблизу від себе за місцем проведення слідчої дії.

Хід і результати допиту важливих свідків доцільно фіксувати за допомогою технічних засобів, які необхідно заздалегідь підготувати. Для цього необхідно використовувати відеокамеру (аудіовізуальна фіксація) і персональний комп'ютер з відповідним програмним забезпеченням та друкувальним пристроєм (процесуальна фіксація – підготовка й оформлення протоколу слідчої дії; допомога в організації й тактиці проведення допиту – автоматизоване робоче місце слідчого).

Як показує аналіз криміналістичної літератури, матеріалів слідчої й судової практики, допит будь-якого свідка обов'язково повинен містити в собі такі умовні стадії:

– з'ясування необхідних даних про особу допитуваного (заповнення анкетної частини протоколу слідчої дії);

– вільна розповідь допитуваного;

– опитувально-відповідна стадія;

– фіксація ходу й результатів допиту.

У ході вільної розповіді слідчий уважно вислуховує допитуваного, по можливості не перебиваючи й не зупиняючи його, тільки якщо той явно відволікається від суті справи, то в тактовній формі повертає його до предмету допиту.

При цьому уточнюючі й конкретизуючи питання, які задає слідчий, як правило, не відображаються в протоколі. Варто пам'ятати про процесуальну «чистоту» слідчої дії й не задавати навідних запитань, що націлюють допитуваного на бажані для слідчого відповіді.

Зазвичай допит свідків відбувається в умовах безконфліктної ситуації. Однак це не означає, що вірогідність показань допитуваного буде при цьому гарантована. Аналіз матеріалів кримінальних справ показує, що комп'ютерні

злочини в банківській сфері в основному вчинюються протягом досить тривалого періоду, у зв'язку з чим свідкам у ході допитів доводиться згадувати про давно минулі події, тому важливим у тактичному відношенні є використання слідчим різних способів активізації асоціативних зв'язків у пам'яті допитуваного. Із цією метою доцільно перший допит (якщо дозволяє обстановка) провести вже на місці події після його огляду. Для відновлення в пам'яті свідка окремих обставин, що мають значення для слідства, під час допиту можна пред'явити деякі предмети обстановки події, що сталася, документи, ЗЕОТ й інше; оголосити показання свідків. Іноді потерпілі через власні психічні переживання і хвилювання забувають певні нюанси, а тому для відновлення забутого можна створити такі умови, коли спогад відбувається після впізнання тих чи інших об'єктів. Так, якщо допитуваний забув про якийсь факт, то йому можна нагадати про іншу відому обставину, що супроводжує за часом і місцем факт, що перевіряється. Можна використовувати й повторний допит, який варто провести через певний час, коли людина заспокоїться й емоції поступляться місцем об'єктивній оцінці своїх дій і дій інших осіб, які мають відношення до події, що сталася.

При повторних допитах сумбурність перших показів замінюється логічною послідовністю викладу обставин подій, його подробиць і деталей, що мають деколи важливе значення для розкриття й розслідування комп'ютерних злочинів у банківській сфері.

У деяких випадках позитивних результатів можна досягти шляхом участі в допиті відповідних спеціалістів і експертів. У ході його проведення вони можуть відігравати активну роль – давати кваліфіковані пояснення щодо спеціальних питань; задавати з дозволу слідчого відповідні питання допитуваному, не виходячи за межі своєї компетентності. Іншою важливою слідчою дією по справах даної категорії є призначення експертиз. Основною і найбільш значимою є програмно-технічна (комп'ютерно-технічна).

Особливості призначення деяких судових експертиз. Ефективність розкриття й розслідування злочинів у банківській сфері, вчинених з використанням комп'ютерних технологій, багато в чому залежить від умілого використання слідчим і оперативним співробітником різних форм допомоги спеціалістів на всіх стадіях кримінального процесу. З огляду на основні положення наукової організації праці, слідчому необхідно звернути увагу на розподіл своєї праці – важливо знати, виходячи з конкретної слідчої ситуації, якому спеціалісту й у якому обсязі можна доручити виконання тієї чи іншої невідкладної роботи в межах чинного кримінально-процесуального законодавства. Варто в такій ситуації погодитися з положенням про те, що тільки при такому підході спеціалісти здатні надійно й швидко впровадити в слідчо-оперативну практику останні досягнення науки й техніки, нові методи дослідження речових доказів, що, у свою чергу, обумовлює розробку нових тактичних прийомів використання допомоги спеціалістів. Відомо, що найпоширенішими формами такої допомоги є: попереднє дослідження документів, матеріалів, технічних пристроїв та інших предметів і об'єктів, що проводиться до порушення кримінальної справи, наприклад, при проведенні оперативно-розшукових заходів (ОРЗ) – отримані при цьому результати не

одержання достатніх даних, що вказують на ознаки вчиненого злочину.

Вище вказані пропозиції, потребують розробки проблем, які пов'язані з додатковими заходами щодо забезпечення своєчасного й законного порушення кримінальної справи, серед яких необхідно розглянути: регламентацію строків проведення експертиз у стадії порушення кримінальної справи, технологію проведення додаткових й повторних експертиз на даній стадії досудового слідства тощо.

Ця стадія досудового розслідування злочинів, які вчинені з використанням електронних документів потребує від слідчого оцінити елементи складу злочину, встановити наявність доказової бази за допомогою приєднання до справи предметів, документів та інших речових доказів, які мають значення для встановлення істини у справі. При цьому слідчий використовує не тільки свої професійні (юридичні) знання, а також і висновки спеціалістів різних галузей знань (кібернетики, інформатики, бухгалтерії, фінансів тощо). Відомо, що законодавчо ця проблема уже вирішена, що дозволяє залучати до справи двох особливих процесуальних суб'єктів: спеціаліста й експерта, які мають різний процесуальний статус на досудовому слідстві.

Рівень накопичення знань в процесі розслідування злочинів, які вчинені з використанням комп'ютерів в банківській сфері дозволив вченим розробляти проблему необхідності й форми використання спеціальних знань при розслідуванні таких злочинів. При цьому сформувалися такі наукові напрями, школи у даній галузі: 1) розробка тактичних рекомендацій з проведення окремих слідчих дій, пов'язаних з одержанням доказів з комп'ютерних систем, 2) залучення окремих категорій технічних спеціалістів для допомоги слідчому; 3) розробка проблем судової комп'ютерно-технічної експертизи.

В умовах відсутності в правоохоронних органах спеціалістів, які мають знаннями в галузі комп'ютерних технологій, В.Б. Вєхов ще в 1995 році зробив першу спробу розробити і сформулювати конкретні рекомендації для слідчих щодо тактики і методики проведення деяких слідчих дій при розслідуванні комп'ютерних злочинів. Зокрема, був запропонований перелік рекомендованих спеціалістів, яких необхідно залучати при розслідуванні даних справ, він запропонував представників таких технічних спеціальностей: програмісти, системні аналітики, особи, які знають інформатику, оператори ЕОМ, інженери по засобам зв'язку й телекомунікаційному обладнанню, обслуговуванню комп'ютерної техніки, забезпеченню безпеки комп'ютерних систем, веденню банківського обліку коштів з використанням комп'ютерної техніки, і вказав на те, що участь таких спеціалістів при розслідуванні злочинів, вчинених у банківській сфері, повинна бути обов'язковою [38, с. 30-31]. Очевидно, що даний перелік є відкритим й орієнтованим на окрему, певну категорію злочинів, а тому може бути за необхідності доповнений.

На наш погляд, такий підхід до добору спеціалістів був у той час єдино вірним, однак не мав реальної перспективи втілення у практику. Разове залучення правоохоронними органами сторонніх осіб як спеціалістів для розв'язування конкретних завдань не могло автоматично забезпечити

На нашу думку, вказані вище обставини істотно підвищують роль спеціальних знань як у стадії порушення кримінальної справи, так й у стадії досудового розслідування злочинів, вчинених з використанням документів, які зберігаються на машинних магнітних носіях. Для додаткового підтвердження цього судження розглянемо деякі важливі аспекти застосування спеціальних знань по справах даної категорії.

У стадії порушення кримінальної справи спеціальні знання в галузі комп'ютерних технологій можуть застосовуватися для одержання достатніх даних, що вказують на ознаки злочину, а також для закріплення слідів злочину. Нерідко тільки використання таких спеціальних знань дозволяє виявити самі ознаки злочину.

Таким чином, актуальність проблеми використання спеціальних знань у стадії порушення кримінальної справи зростає в умовах можливого застосування злочинцями комп'ютерної техніки. Дискусійним залишається питання про процесуальну форму використання таких знань.

У цей час слідчі й оперативні працівники стали використовувати попередні дослідження документів, а також іншу інформацію, яка знаходиться на машинних магнітних носіях, що являють собою одну з форм перевірки, яка проводиться в порядку ст. 97 КПК України. Результати таких досліджень мають характер орієнтовної інформації, і не є доказами по справі, однак такі відомості допомагають вирішенню завдань виявлення ознак злочину й закріплення його слідів. При цьому обсяг попередньо проведених досліджень, а також застосовувані методи для дослідження конкретних об'єктів, сутність експертного висновку фактично дублюють можливе наступне експертне дослідження й, як справедливо відзначає Т.В. Аверьянова, перетворює експертизу у формальність, спричиняє нераціональну витрату сил, засобів і часу самого експерта [2, с. 216].

Для підтвердження цього висновку наведемо єдиний аргумент: відомо, що повноцінне попереднє дослідження сучасного машинного носія інформації пов'язане з вивченням декількох сотень документів, що зберігаються на ньому, десятків працездатних комп'ютерних програм, включаючи програми невідомого призначення, вимагає спеціально обладнаного комп'ютеризованого робочого місця, особливих методик дослідження, а іноді використання всього обсягу професійних знань, навиків і умінь в галузі комп'ютерної техніки й інформаційних технологій.

Розглядаючи питання про можливості призначення експертизи до порушення кримінальної справи, яке пропонується в криміналістичній літературі, ми вважаємо, що це перспективна думка і вона заслуговує позитивного вирішення. Разом з тим є противники цієї новели В.Д. Арсеньєва, В.М. Савицький, І.М. Сорокотягін та інші, їхні позиції всебічно проаналізовані Р.С. Бєлкіним [23, с. 101-106]. Вважаємо, що специфіка аналізованих в цьому дослідженні злочинів потребує нових роздумів, підходів, які повинні бути кардинально іншими, ніж ті, які використовує сьогодні слідча практика. Погоджуючись з позицією Р.С. Бєлкіна, вважаємо, що проведення експертизи в стадії порушення кримінальної справи може стати важливим, а іноді і єдиним способом

мають доказового значення; консультації спеціалістів (одержання інформації довідкового характеру), якими може скористатися слідчий або оперативний працівник на будь-якому етапі провадження в справі; участь спеціаліста в проведенні слідчих дій, що й було розглянуто нами при дослідженні виділених слідчих дій; проведення судових експертиз.

Одним з перших – проведення інженерно-технічних (судово-інженерної комп'ютерної; комп'ютерно-технічної або просто комп'ютерної) експертиз запропонував Р.С. Бєлкін [1, с. 412-451]. Цю проблему досліджують сьогодні й інші автори Л.В. Борисова, Н.І. Клименко, М.В. Салтевський, М.Г. Щербаковський [30; 110; 220; 265]. Однак у криміналістичній науці сьогодні ще не сформувалося достатньо чітке наукове визначення подібних судових експертиз.

Основною формою використання спеціальних знань є судова експертиза, що призначається у випадках, коли при проведенні дізнання, досудового слідства й при судовому розгляді необхідні спеціальні знання в науці, техніці, мистецтві або ремеслі. На це прямо вказують і керівні документи МВС України – необхідно підвищити роль експертно-криміналістичної служби у виявленні й розслідуванні злочинів у банківській сфері, приділивши першочергову увагу освоєнню й проведенню нових видів бухгалтерських і комп'ютерних експертиз.

Стаття 1 Закону України «Про судову експертизу» дає таке визначення поняття судової експертизи: «Судова експертиза – це дослідження експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів дізнання, досудового слідства чи суду» [99].

Судова експертиза – це процесуальна дія, яка проводиться з метою отримання висновку з питань, що мають доказове значення у справі і полягає в дослідженні експертом речових доказів, явищ, процесів та інших об'єктів за завданням органів дізнання, слідчого або судді. Предмет експертизи визначений об'єктом дослідження й питаннями, сформульованими в постанові слідчого (суду). Таким чином, предметом даної слідчої дії є фактичні дані, які необхідно встановити при розслідуванні кримінальної справи. Типовими об'єктами експертного дослідження зі справ про комп'ютерні злочини в банківській сфері є: документи (у тому числі підготовлені за допомогою ЗЕОТ, машинограми, гроші, цінні папери й т.п.), ЗЕОТ (ПЕОМ, мережа ЕОМ, банкомати), різні типи друкувальних пристроїв – принтери, контрольно-касові машини, автоматизовані торговельні термінали, цифрові таксофони, електронні записні книжки й перекладачі, різноманітні машинні носії інформації (дискети, диски, пластикові карти, стрічки, інтегральні мікросхеми, стримери, ZIP-накопичувачі тощо), комп'ютерна інформація (програма для ЕОМ, файл, електронний цифровий підпис, «електронний» документ тощо), цифрові засоби електрозв'язку (стільникові апарати, пейджери, телефонні апарати із внутрішньою пам'яттю тощо), спеціальні технічні засоби для негласного одержання інформації; функціональний перелік; назви й принцип дії; рекомендації із призначення експертизи; сліди та їх копії, зразки, приєднані до кримінальної справи, інші

речові докази.

Основними завданнями, які вирішуються судовими експертизами, є: ідентифікація об'єктів; діагностика механізму події (часу, місця, способу й послідовності дій, подій, явищ і процесів, причинних зв'язків між ними, природи, якісних і кількісних характеристик об'єктів, їх властивостей і ознак, що не піддаються безпосередньому сприйняттю); експертна профілактика – діяльність щодо виявлення обставин, що сприяють вчиненню злочинів, і розробці заходів щодо їх усунення.

Як показує проведений нами аналіз кримінальних справ, при розслідуванні комп'ютерних злочинів у банківській сфері широко використовуються різноманітні види судових експертиз. Результати опитування слідчих свідчать про те, що по справах розглянутої категорії складності з підготовкою й призначенням експертиз зазнавали 83% із числа опитаних респондентів. Тому питання, що стосуються підготовки й призначення різних видів судових експертиз по справах про комп'ютерні злочини в банківській сфері, особливо найбільш специфічні, повинні більш глибоко вивчатися слідчими.

Можливість розглянути деякі особливості підготовки й призначення окремих видів судових експертиз у тому обсязі, у якому дозволяють це зробити обмежені рамки цієї роботи.

Техніко-криміналістична експертиза документів, виготовлених з використанням друкуючих ЗЕОТ і нових технологій, є новим видом експертних досліджень, які стали успішно використовуватися в слідчо-судовій практиці з середини 90-х р. минулого століття.

Розглянута експертиза комплексна, оскільки для вирішення деяких питань у процесі дослідження об'єктів необхідно застосовувати методики, що ґрунтуються на знаннях криміналістики, поліграфії, матеріалознавства, інформатики, кібернетики й нейробіоники.

Завдання, що становлять предмет експертизи, носять діагностичний та ідентифікаційний характер. До діагностичних завдань відносяться:

– встановлення способу виготовлення документа, факту й способу внесення в нього змін;

– визначення початкового змісту документа;

– виявлення невидимих і слабовидимих текстів (у тому числі за вдавленими штрихами), залитих, закреслених записів, текстів на спалених документах;

– визначення відносної давності виготовлення документа.

До ідентифікаційних відносяться:

– встановлення групової (родової, видової) приналежності порівнюваних об'єктів (засобів письма, знарядь письма, документів у цілому);

– встановлення спільності їх походження;

– встановлення індивідуальної тотожності певних об'єктів (засобів, що застосовувалися при виготовленні документів) за їх відображеннями у документі, а також встановлення документа за його частинами.

Зокрема, при призначенні технічної експертизи документів розглянутого виду потрібно провести діагностику або ідентифікацію друкувального

даного виду злочинів.

На завершення необхідно підкреслити, що перелік розглянутих вище слідчих дій та експертних досліджень не є вичерпним. Результати проведеного нами аналізу даної проблеми показують, що саме вони є найбільш специфічними й значимими для розслідування комп'ютерних злочинів у банківській системі, особливо на початковому етапі досудового розслідування. Невідкладність проведення зазначених слідчих дій й організаційних заходів пояснюється тим, що саме вони спрямовані на встановлення події злочину, способу його вчинення, виявлення типових слідів, встановлення очевидців, затримання злочинців, а також інших обставин, що сприяють успішному розслідуванню злочинних зазіхань, справедливому покаранню винних і відшкодуванню шкоди, заподіяної потерпілій стороні.

1.3. Сутність та характеристика спеціальних знань, які використовуються при дослідженні фінансових електронних документів на досудовому слідстві.

Поява в переліку доказів по кримінальних справах документів на машинних магнітних носіях інформації потребує по-новому розглянути проблему застосування спеціальних знань при розслідуванні «комп'ютерних» злочинів, вчинених у банківській системі України. Це обумовлено такими об'єктивними обставинами, що визначають специфіку застосування таких знань по даній категорії справ.

1. Припущення про наявність на жорсткому магнітному носієві (вінчестері) або дискеті документів, що мають відношення до вчиненого злочину, носить імовірний характер у тих випадках, коли комп'ютер фігурує як елемент об'єктивної сторони злочину. Слідчий має всі підстави припускати, що в якому-небудь комп'ютері такі документи знаходяться, однак доказової інформації (крім можливої оперативної інформації), як правило, не мають.

2. Виявлення документів з відповідною інформацією на машинних магнітних носіях можливо тільки за допомогою комп'ютерної техніки, оснащеної спеціальними прикладними програмами. Використання програмного забезпечення комп'ютера, що належить підозрюваній особі, з метою виявлення такого роду документів, несе загрозу знищення певної кількості криміналістично значимих слідів у файловій системі комп'ютера й настроюваннях програм, а тому можливе лише з дозволу спеціаліста після спеціальної перевірки.

3. Кількість виявлених слідів підготовки й вчинення злочинів такого роду та їх інформаційна значимість залежать від кваліфікації особи, що виявляє й фіксує ці сліди.

4. Документи та інші сліди злочину, якщо вони знаходяться на машинних магнітних носіях інформації, можуть бути ненавмисно й невідновно знищені при проведенні слідчих дій, якщо слідчий не дотримується особливого порядку поводження з носієм інформації, як з технічним пристроєм так і особливим порядком огляду інформації на ньому.

носіях? Яке їх призначення й можливість використання?

Чи зберігаються на пред'явлених системних блоках і магнітних носіях текстові файли? Якщо так, то який їх зміст і можливість використання?

Чи є знищена інформація на представлених магнітних носіях? Чи можливо її відновлення? Якщо так, який її зміст, можливості використання? Які програмні продукти зберігаються на пред'явлених магнітних носіях? Який їх зміст, призначення, можливість використання?

Чи є на представлених магнітних носіях спеціалізовані програми, які використовуються для підбору паролів або іншого незаконного проникнення в комп'ютерні мережі? Якщо так, то які їх назви, особливості роботи, можливості використання для проникнення в конкретну комп'ютерну мережу? Чи є ознаки, що свідчать про застосування конкретної програми для незаконного проникнення у вищевказану мережу? Якщо так, то які?

Яка хронологічна послідовність необхідних дій для запуску конкретної програми або здійснення певної операції?

Чи можливо, працюючи в даній комп'ютерній мережі, зробити в середовищі програмних продуктів які-небудь зміни програмних файлів? Якщо можливо, то які, як і з якого комп'ютера можуть бути зроблені подібні зміни?

Чи можливо одержати доступ до фінансової та іншої конфіденційної інформації, наявної в зазначеній мережі?

Як здійснюється такий доступ?

Як здійснене незаконне проникнення в зазначену локальну комп'ютерну мережу? Які є ознаки, що свідчать про таке проникнення?

Якщо незаконне проникнення відбулося ззовні, то які є можливості для ідентифікації комп'ютера, з якого відбулося проникнення?

Якщо відсутні ознаки входження в мережу стороннього користувача, указати, з яких комп'ютерів можна зробити подібні операції?

Можна також ставити питання про сумісність тих чи інших програм, можливості використання програми на конкретному комп'ютері тощо.

Крім того, перед експертами можуть ставитися питання про призначення того чи іншого предмета, пов'язаного з комп'ютерною технікою (комп'ютерно-технічна експертиза):

Яке призначення даного предмета, можливість його використання? Які конструктивні особливості він має? З яких частин складається? Промисловим або кустарним способом виготовлений?

Якщо предмет виготовлений кустарним способом, то пізнаннями в якій галузі науки, техніки й ремесла володіє особа, що виготовила зазначений предмет, який рівень професійної підготовки зазначеної особи?

У сукупності з якими предметами й приладами може бути використаний даний предмет?

Які технічні характеристики даного предмета?

Запропоновані вище методичні рекомендації далеко не вичерпують всіх питань, які можуть бути пов'язані з розслідуванням розкрадань у кредитно-фінансовій сфері, вчинених з використанням електронних коштів доступу, а лише відображають найбільш важливі специфічні особливості розслідування

пристрою, на якому виготовлені документи, що цікавлять слідство. Тому, як рекомендують спеціалісти, при проведенні огляду місця події, обшуку або виїмки особливу увагу варто приділяти первинним діагностичним ознакам принтерів ЗЕОТ. У випадку виявлення документів з такими ознаками при проведенні слідчих дій необхідно розширювати коло пошуку й огляду з метою встановлення даних друкувальних пристроїв, їхнього огляду й подальшого вилучення. Встановлення групи друкувальних пристроїв або конкретного пристрою дає можливість слідству визначити досить вузьке коло осіб, причетних до виготовлення документа, що цікавить слідство, або використанню його в злочинних цілях. Відомо, що виготовлення документа на принтері проводиться з використанням комп'ютера (ЕОМ) і його програмного забезпечення, тобто створюється електронний оригінал документа або його фрагменти, що згодом виводиться на друк на відповідний матеріальний носій (папір, пластик, плівку й т.п.), а також, як правило, зберігається в пам'яті ЗЕОТ (на машинному носії). Таким чином, визначаючи вид експертизи й формулюючи завдання експерту, слідчий заздалегідь турбується про належне оформлення й надання всіх необхідних (крім документа) технічних пристроїв (ЗЕОТ), комп'ютерної інформації (файлів), тобто електронному образі документа.

На думку спеціалістів, криміналістично значима інформація, отримана при експертному дослідженні документів на паперовому носії, може послужити каталізатором проведення досліджень програмно-технічною експертизою, оскільки за ними може бути визначений унікальний контекст (у загальному випадку сполучення кодів), що надалі послужить шаблоном для пошуку відповідної комп'ютерної інформації. За паперовим документом також може бути визначений і вид комп'ютерної інформації.

Відносно електронного документа класифікаційним завданням є встановлення електронного формату документа (програмної організації даних) або його частини. У силу кодованого характеру електронного документа класифікаційні завдання, розв'язувані комплексною експертизою, будуть, на нашу думку, першочерговими, оскільки, без їх вирішення не може бути встановлене навіть значеннєвий зміст конкретного документа. Іншими словами, електронний документ, створений певною комп'ютерною програмою, може містити інформацію в складних форматах, недоступних сприйняттю стандартних програм, що перебувають у розпорядженні експерта або спеціаліста (наприклад, документ, завірений електронним цифровим підписом), внаслідок чого вирішення класифікаційних завдань дозволяє експертові або спеціалісту спочатку підібрати відповідний спосіб (ключ) для прочитання вмісту електронного документа, а потім використовувати отриманий формат даних для дослідження втримування перетвореної форми документа.

Програмно-технічна експертиза як самостійний вид криміналістичного дослідження заявила про себе, на думку деяких дослідників, з початку 90-х рр. [1, с. 458] У цей час за допомогою зазначених експертиз можуть вирішуватися такі завдання:

– відтворення й роздрукування всієї або частини комп'ютерної інформації

(за певними темами, ключовими словами тощо), що міститься на машинних носіях, у тому числі та, яка знаходиться в нетекстовій формі (у складних форматах – у формі мов програмування, у формі електронних таблиць, баз даних тощо);

– відновлення комп'ютерної інформації, що раніше містилася на машинних носіях, але згодом стертої (знищеної) або зміненої (модифікованої) з різних причин;

– встановлення дати й часу створення, зміни (модифікації), стирання, пошкодження, знищення або копіювання тієї чи іншої інформації (файлів, програм і т.д.);

– розшифровка закодованої інформації, підбор паролів і розкриття системи захисту ЗЕОТ;

– дослідження ЗЕОТ на предмет наявності в них програмно-апаратних модулів і модифікацій, що призводять до несанкціонованого знищення, блокування, модифікації або копіюванню інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі (шкідливих засобів або вірусів);

– встановлення авторства, місця підготовки й способу виготовлення документів (файлів, програм), що перебувають на машинному носієві інформації;

– з'ясування можливих каналів витоку інформації з комп'ютерної мережі, конкретних ЗЕОТ і приміщень;

– встановлення можливих несанкціонованих способів доступу до охоронюваної законом комп'ютерної інформації та її носіїв;

– з'ясування технічного стану, справності ЗЕОТ, оцінки їх зношення, а також індивідуальних ознак адаптації ЗЕОТ під конкретного користувача;

– встановлення рівня професійної підготовки окремих осіб, що проходять у справі, в галузі програмування і як користувач;

– встановлення конкретних осіб, що порушили правила експлуатації ЕОМ, системи ЕОМ або їх мережі;

– встановлення причин і умов, що сприяють вчиненню злочину, пов'язаного з використанням ЗЕОТ.

Варто звернути увагу на ту обставину, що специфічними об'єктами дослідження даної експертизи є спеціальні технічні засоби, запрограмовані для негласного одержання інформації, а також цифрові засоби електрозв'язку.

Проведене нами дослідження показало, що в цей час у системі експертних установ МВС України відсутні спеціальні підрозділи, які повинні проводити програмно-технічні дослідження. На практиці, в інших країнах, найчастіше, проведення експертизи доручається спеціалістам відповідної кваліфікації.

Методика підготовки та призначення програмно-технічної експертизи досить повно і всебічно досліджена й описана в спеціальній літературі [38; 118; 172; 220], тому обмежимося вищевикладеним.

Комплексна судово-бухгалтерська й програмно-технічна експертиза є типовою слідчою дією по справах про комп'ютерні злочини в банківській сфері.

Проведене нами дослідження матеріалів кримінальних справ дозволяє сформулювати положення про те, що комплексна судово-бухгалтерська та програмно-технічна експертиза повинна призначатися в таких цілях:

– перевірка й процесуальна фіксація даних, викладених у матеріалах ревізій, інвентаризацій та інших контрольно-перевірочних актів;

– визначення розмірів нестачі або надлишків товарно-матеріальних цінностей, коштів та інших видів матеріальної шкоди;

– встановлення часу утворення (виникнення) шкоди;

– визначення конкретної особи, якій була заподіяна шкода;

– перевірка обґрунтованості автоматизації тих чи інших операцій, технологічних циклів або процесів; використання тих чи інших ЗЕОТ для цих цілей;

– перевірка правильності проведення бухгалтерсько-документальних операцій з використанням ЗЕОТ;

– ведення електронного документообігу;

– виявлення фактів порушення встановлених для конкретної організації (підприємства, установи) правил ведення електронного документообігу, технології виробництва, експлуатації ЗЕОТ, захисту ЗЕОТ і комп'ютерної інформації; звітності й обліку;

– встановлення причин та умов, що сприяли вчиненню комп'ютерного злочину в банківській сфері.

Проведення розглянутої експертизи доцільно доручити групі експертів різних спеціальностей, обумовлених специфікою досліджуваного об'єкта, обставинами розслідуваної події та змістом версій, що перевіряють.

Основні вимоги при підготовці слідчим зазначеної експертизи:

– до винесення постанови про призначення експертизи проконсультуватися з фахівцями з приводу її мети, формулювання питань, характеру й особливостей підготовки матеріалів, які будуть представлені експертам;

– вивчити відповідну спеціальну літературу щодо специфічних предметів і документів, які передбачається представити на експертизу;

– по можливості ознайомити експертів з усіма матеріалами справи, що стосуються предмету експертного дослідження (протоколами огляду місця події, документів і предметів, а також допитів відповідних осіб; матеріалами ревізій, інвентаризацій, документальних та інших перевірок; висновками інших фахівців, що мають до цього відношення, наприклад, результатами попереднього дослідження);

– постанова про призначення експертизи повинна містити максимально повну описову частину, а резолютивна частина – бути конкретною, короткою, але інформативною.

На вирішення *програмно-технічної експертизи* можуть бути поставлені такі питання:

Яку інформацію містять пред'явлені на експертизу системні блоки й дискети? Яка інформація є на системних блоках і магнітних носіях, її призначення та можливість використання?

Які програми знаходяться на пред'явлених системних блоках і магнітних