**ЕКОНОМІКА,
ФІНАНСИ,
ПРАВО**

- ***П. Біленчук, А. Кофанов, О. Кобилянський***
  КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ
- 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
  КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНІВ, ВЧИНЕНИХ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ
- П. Біленчук, А. Кофанов, О. Кобилянський
  ПРАВОВІ ОСНОВИ ДІЯЛЬНОСТІ ОРГАНІВ ПРАВОПОРЯДКУ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ

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

КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ

«НАУКОВА БІБЛІОТЕКА КРИМІНАЛІСТА» презентує підручники, монографії, навчальні посібники у 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»

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

КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ

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
НАЦІОНАЛЬНА АКАДЕМІЯ 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

КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ

Навчальний посібник

Київ 2011

ББК 67.52я73
Б 61

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

Рецензенти:
А.М. Гайдай – генеральний директор правничо-інформаційної компанії «Інтелект», заслужений працівник освіти України
Салтинський В.М. – віце-президент Поліцейської фінансово-правової академії, Заслужений юрист України

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л.
61 Комп'ютерна злочинність у кредитно-фінансовій індустрії: криміналістичний аналіз. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2011. – 52 с. – (Серія „Економіка, фінанси, право").

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

Для студентів і викладачів юридичних навчальних закладів.

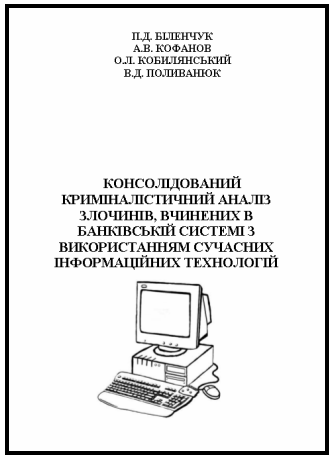
ББК 67.52я73

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Педик Я.Л. Автоматизовані інформаційно-комп'ютерні системи органів правопорядку України (характеристика, системна класифікація, ресурсне забезпечення). – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2009. – 68 с. – (Серія «Автоматизація, комп'ютеризація, інформатизація»).

У навчальному посібнику системно висвітлено українські, європейські і світові трансформаційні ідеї, інновації, тенденції, доктрини та концепції розвитку інформаційно-комп'ютерного забезпечення органів правопорядку.

В книзі детально викладено основні інформаційні системи і підсистеми органів внутрішніх справ України.

Для студентів, курсантів, аспірантів, викладачів та науковців, працівників-практиків органів правопорядку і спецслужб.

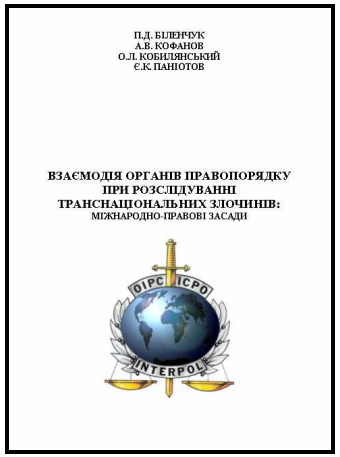


Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Поливанюк В.Д. Консолідований криміналістичний аналіз злочинів, вчинених в банківській системі з використанням сучасних інформаційних технологій. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2010. – 88 с. – (Серія „Економіка, фінанси, право").

У навчальному посібнику висвітлюються правові і технологічні засади електронних розрахунків у банківській системі України.

Дається системно-інформаційний криміналістичний аналіз існуючих загроз банківської системи, а також узагальнена криміналістична характеристика злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій.

Для студентів і викладачів юридичних навчальних закладів.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Паніотов Є.К. Взаємодія органів правопорядку при розслідуванні транснаціональних злочинів: міжнародно-правові засади. – Монографія / За ред. П.Д. Біленчука. – Київ: ННІПСК КНУВС, 2009. – 84 с. – (Серія «Національна і міжнародна безпека»).

В монографічному дослідженні аналізуються міжнародно-правові засади взаємодії органів правопорядку України та зарубіжних країн при розслідуванні злочинів.

Структурно монографія складається з передмови, двох розділів, семи параграфів, тринадцяти підпараграфів, висновків, пропозицій і рекомендацій, списку використаної і рекомендованої літератури.

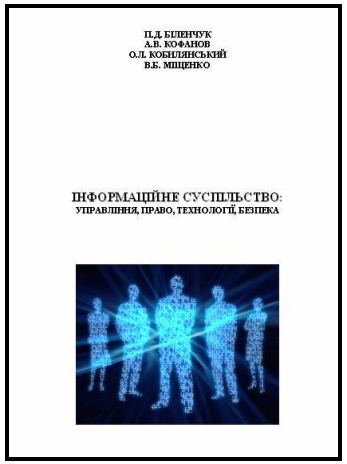
Для студентів і викладачів вищих закладів освіти, науковців, працівників вітчизняних органів правопорядку та зарубіжних правозахисних організацій.

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л.
Міжнародний тероризм: консолідований аналіз забезпечення безпеки. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 72с. – (Серія „Безпека людини, суспільства, держави").

В навчальному посібнику наведені узагальнені результати аналізу сучасного міжнародного тероризму. Висвітлюються поняття, сутність, види терористичних актів.

Дослідження виконано дослідниками Навчально-наукового інституту підготовки слідчих і криміналістів Київського національного університету внутрішніх справ.

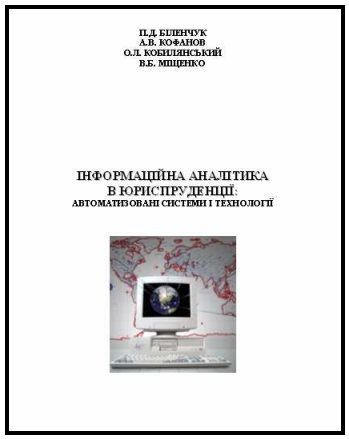
Для працівників органів державної влади, місцевого самоврядування, співробітників органів правопорядку та спецслужб (МВС, СБУ, МЧС, МО України), науковців, викладачів, аспірантів, слухачів та студентів навчальних закладів.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Міщенко В.Б. Інформаційне суспільство: управління, право, технології, безпека. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 60 с. – (Серія „Безпека людини, суспільства, держави").

У навчальному посібнику подається сучасний стан доктринальних основ формування інформаційного суспільства (історія, теорія, практика), дається аналіз розвитку мережі Інтернет в інформаційному просторі України, висвітлюються віртуальні системи управління знаннями і характеризуються всесвітні телекомунікаційні мережі, розкривається сутність інформаційної безпеки в телекомунікаційному просторі світу.

Навчальний посібник призначений для студентів вищих навчальних закладів, викладачів, аспірантів, фахівців-практиків.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Міщенко В.Б. Інформаційна аналітика в юриспруденції: автоматизовані системи і технології. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 47 с. – (Серія „Безпека людини, суспільства, держави").

У навчальному посібнику розглянуті та класифіковані основні джерела загроз для основних властивостей інформації у традиційній і електронній формах. Розглянуті основні заходи та засоби, які вживаються для збереження інформації. Продемонстровано необхідність якісного вирішення на практиці таких завдань: оцінка обстановки; аналіз ризиків; формування комплексу захисних систем; оцінки ефективності комплексу.

Навчальний посібник призначений для студентів вищих навчальних закладів, викладачів, аспірантів, фахівців-практиків.

ЗМІСТ

РОЗДІЛ 1
ПОНЯТТЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

В сучасних умовах соціально-економічного розвитку України комп'ютерна злочинність стала реальністю суспільного життя.

Розуміння причин її виникнення та розвитку потребує аналізу кризових ситуацій, що склалися і стали впливати на соціальний, економічний та правовий розвиток суспільства.

Як свідчить аналіз дискусійних матеріалів у літературі та періодичних виданнях, негативні тенденції в значній мірі обумовлені бурхливим процесом розвитку науково-технічної революції. Ця революція, як і попередня їй в історії суспільства революція (аграрна та промислова), викликала за собою важливі соціальні зміни, найбільш важливими з яких є виникнення нового виду суспільних відносин та суспільних ресурсів – інформаційних. Останні відрізняються від відомих раніше енергетичних ресурсів цілим рядом особливостей.

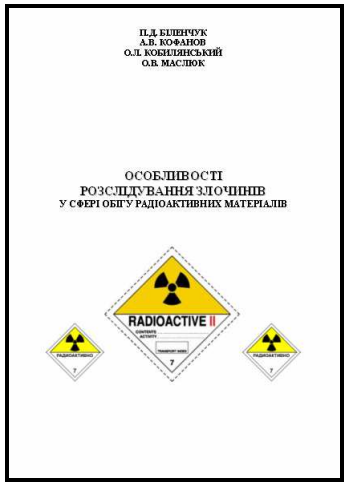
Інформація стала першоосновою життя сучасного суспільства, предметом та продуктом його діяльності, а процес її створення, нагромадження, збереження, передачі та обробки, в свою чергу, стимулює процес в галузі знаряддя її виробництва: електронно-обчислювальної техніки (ЕОТ), засобів телекомунікацій та систем зв'язку. Усе згадане в цілому входить в поняття нової інформаційної технології, яка є сукупністю методів та засобів реалізації інформаційних процесів у різних галузях людської діяльності, тобто способами реалізації інформаційної діяльності людини, яку також можна розглядати як інформаційну систему.

Іншими словами, інформація стає продуктом суспільних (інформаційних) відносин, пов'язаних з виготовленням, передачею, накопиченням та використанням інформації у різних її формах: науково-технічної документації, програмного забезпечення ЕОТ, баз даних, системи управління базами даних (СУБД) та інші.

У зв'язку з цим нові інформаційні технології дали поштовх не тільки прогресу суспільства, але й стимулювали виникнення та розвиток невідомих раніше негативних процесів. Одним з них є виникнення нових форм злочинності. Так, наприклад, революція в галузі електроніки надала злочинцям, їх угрупованням та об'єднанням широкі можливості доступу до нових технологічних засобів, які дозволяють їм незаконно привласнювати великі суми коштів, відмивати величезні доходи, отримані злочинним шляхом, уникати оподаткування та проводити комплексні заходи, спрямовані на підготовку, вчинення і маскування різних видів злочинів.

Крім негативних факторів історичного розвитку суспільства в період науково-технічної революції існує й ряд інших, не менш важливих форм, що впливають на розвиток нових форм злочинності в Україні. До них можна віднести:

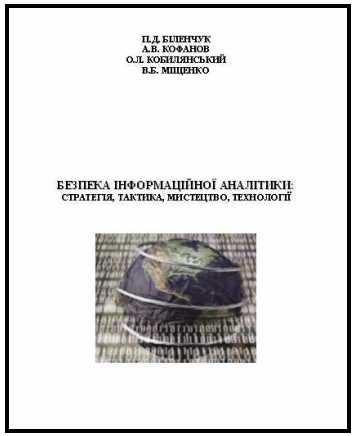
– часткову втрату державним апаратом функцій повноцінного управління суспільством та державою;



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Маслюк О.В. Особливості розслідування злочинів у сфері обігу радіоактивних матеріалів. – Монографія / За ред. П.Д. Біленчука. – Київ: ННІПСК КНУВС, 2009. – 88 с.

В монографічному дослідженні розкрито особливості проведення окремих слідчих дій у справах ядерної злочинності, визначено роль спеціаліста. Звернуто увагу, що особливий характер ядерної злочинності потребує введення в практику криміналістичного дослідження нових ядерно-фізичних методик. Вивчено форми і механізм міжнародного співробітництва у справах ядерної злочинності, достатність національного ядерного права. Показано, що перспективи криміналістичних досліджень у справах ядерної злочинності пов'язані зі створенням мережі ядерних судових лабораторій та національної бази даних характеристик радіоактивних матеріалів та специфіки виробника чи експлуатаційника.

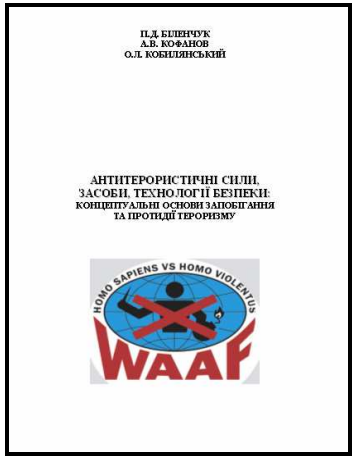
Для викладачів юридичних вузів, а також слідчих, які спеціалізуються на розслідуванні даних видів злочинів.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Міщенко В.Б. Безпека інформаційної аналітики: стратегія, тактика, мистецтво, технології. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 68 с. – (Серія „Безпека людини, суспільства, держави").

У навчальному посібнику висвітлюються питання програмного і технічного забезпечення телекомунікаційного середовища, аналізуються потенційні ризики, загрози і небезпеки в кіберпросторі, дається характеристика злочинності в інформаційно-телекомунікаційній сфері.

Для студентів, викладачів, фахівців-практиків.



Біленчук П.Д., Кофанов А.В., Кобилянський О.Л. Антитерористичні сили, засоби, технології безпеки: концептуальні основи запобігання та протидії тероризму. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 46 с. – (Серія „Безпека людини, суспільства, держави").

В навчальному посібнику дається характеристика антитерористичних сил, методів, засобів і технологій, які сприяють забезпеченню запобігання та протидії тероризму.

Для працівників органів державної влади, місцевого самоврядування, співробітників органів правопорядку та спецслужб (МВС, СБУ, МЧС, МО України), науковців, викладачів, аспірантів, слухачів та студентів навчальних закладів.

670 с.

269. Яблоков Н.П. Криминалистическая характеристика финансовых 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.

– суперечність та недосконалість законодавчої бази;

– нездатність державних інститутів задовольнити життєво необхідні потреби населення;

– безгосподарність та розбалансованість економіки країни, особливо у кредитно-фінансовій, валютно-грошовій та товарно-сировинній сфері;

– незацікавленість у збереженні матеріальних цінностей з боку посадових осіб державних та фінансово-комерційних структур.

Основною особливістю сучасної криміногенної ситуації є інтенсивне перетворення кількісних характеристик злочинності у негативні якісні. Набирають силу небезпечні процеси зростання організованої злочинності з так званої респектабельної («білих комірців»), до якої ми відносимо економічну та комп'ютерну злочинність: лідери злочинних угрупувань і об'єднань з корумпованими посадовими особами. Йде активний процес розмивання межі між різними видами злочинності. Наприклад, злочинці, організовані в групи та об'єднання, починають застосовувати методи, що традиційно використовуються в своїй злочинній діяльності злочинцями економічної сфери, нерідко використовують при цьому засоби комп'ютерної техніки, зв'язку та телекомунікації і вступають в змову з посадовими особами. Дані процеси призводять до того, що злочинні об'єднання починають направляти свою діяльність на отримання та використання незаконних засобів, добутих протиправними діями (наприклад, вимагання), на вчинення маніпуляцій з законними засобами у корисних цілях.

Іншими словами, перехід від обігу злочинних засобів до більш корисних законних засобів. Міжнародний досвід свідчить, що сучасна злочинність проникає в сферу законного підприємництва, підриває репутацію усіх, хто так чи інакше стикається з нею, і корумпує дії посадових осіб, послуги яких їй необхідні для відмивання незаконних прибутків.

Швидке кількісне та якісне зростання злочинності обумовлені збільшенням протиріч у різних сферах суспільного життя, частою зміною системи правоохоронних органів, недосконалістю законодавства, помилками у правозастосовчій практиці та сприяють розвитку комп'ютерної злочинності як соціального явища.

Відсутність чіткого визначення комп'ютерної злочинності, єдиного розуміння сутності цього явища у значній мірі перешкоджають формулюванню завдань правозастосовчих органів у вироблені єдиної стратегії боротьби з нею.

До недавнього часу вважалось, що комп'ютерна злочинність – явище, властиве тільки капіталістичним країнам через недостатню комп'ютеризацію нашого суспільства. Ця обставина й призвела до відсутності яких-небудь наукових досліджень цієї проблеми. Тільки в останні роки з'явились праці з проблем боротьби з комп'ютерною злочинністю, в яких розглядаються кримінально-правові та кримінологічні аспекти цього явища. Сама поява комп'ютерної злочинності в нашій країні призводить до висновку про те, що це явище властиве всім державам, які в силу свого наукового прогресу вступають в період широкої комп'ютеризації своєї діяльності.

Таким чином, протягом останніх 15-20 років, з розвитком

комп'ютеризації господарсько-управлінської та фінансово-комерційної діяльності з'явились нові види злочинів, які стали називати комп'ютерними, виходячи з аналогів та термінів зарубіжної юридичної практики.

Дані злочинні діяння отримали найбільше розповсюдження у різних галузях господарства та управління, у тому числі у виробництві, банківській справі та у сфері обслуговування населення. Так, проведені дослідження свідчать про те, що за останні роки серед виявлених корисних злочинів домінують розтрата грошових коштів у великих та особливо великих розмірах на промислових підприємствах, організаціях та установах, котрі застосовують автоматизовані системи на основі ЕОМ для обробки первинних бухгалтерських документів, що відображають касові операції, рух матеріальних цінностей та інші види обліку. Перший подібний злочин у колишньому СРСР був зареєстрований в 1979 року у місті Вільнюсі. Шкода державі від розтрати склала 78584 крб. Цей факт був записаний у міжнародний реєстр правопорушень і є своєрідною відправною точкою у розвитку нового виду злочинів у нашій країні.

Між тим у кримінально-правовій та криміналістичній науці усе ще немає визначення поняття комп'ютерного злочину, дискутуються різні точки зору їх класифікації. Складність у визначенні цих понять існує як з причин неможливості виділення єдиного об'єкту злочинного посягання, так і множини предметів злочинних посягань з точки зору їх кримінально-правової охорони.

Наприклад, Ю.М. Батурін вважає, що комп'ютерна злочинність як особлива група злочинів у юридичному значенні не існує, відзначає при цьому той факт, що традиційні види злочинів модифікувались через використання при їх вчиненні обчислювальної техніки і тому вірно було казати лише про комп'ютерні аспекти злочинів, не виділяючи їх в окрему групу злочинів.

А.М. Карах'ян під комп'ютерними злочинами розуміє протизаконні дії, об'єктом яких є електронно-обчислювальні машини. Існують й інші точки зору з цього питання.

Виходячи з аналізу наукових робіт та публікацій вітчизняних та зарубіжних досліджень можна зробити висновок про те, що існує два основні напрями наукової думки. Одні дослідники відносять до комп'ютерної злочинності дії, в яких комп'ютер є об'єктом або знаряддям посягання. При цьому крадіжка самих комп'ютерів буде розглядатися як один із способів вчинення комп'ютерних злочинів.

Дослідники другої групи відносять до комп'ютерних злочинів тільки протизаконні дії у сфері автоматизованої обробки інформації. Вони виділяють як головну класифікаційну ознаку, яка дозволяє віднести ці злочини до окремої групи єдині способи, знаряддя, що обробляються в комп'ютерній системі, а комп'ютер є знаряддям посягання.

Варто зазначити, що в системі кримінальної поліції ФРН за кілька останніх років було запропоновано кілька кримінально-правових визначень комп'ютерної злочинності. Наприклад, деякі вчені вважають, що комп'ютерні злочини – це всі злочинні дії при яких комп'ютер виступає як засіб, знаряддя

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

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

або метою його вчинення. Друге визначення об’єднує під цим терміном всі протизаконні дії, які завдають збитки майну і пов’язані з електронним обчислюванням даних. Третє визначення комп’ютерної злочинності окреслює три основні види протизаконної дії: комп’ютерні майнові (наприклад, комп’ютерне шахрайство, саботаж, промисловий шпіонаж), комп’ютерні злочини проти прав особи, правопорушення проти громадських і суспільних правових цінностей (наприклад, проти національної безпеки).

Починаючи з 1985 року кримінальна поліція ФРН взяла на озброєння нове визначення комп’ютерної злочинності, яке включає в себе «всі протизаконні дії, при яких електронне опрацьовування інформації було знаряддям їх вчинення або об’єктом».

В Швейцарії експерти під комп’ютерною злочинністю розуміють «всі продумані та протизаконні дії, які приводять до нанесення збитків майну і здійснення яких стало можливим в першу чергу завдяки електронній обробці інформації».

Розглянуті вище позиції відносно визначення поняття комп’ютерних злочинів дають основу для аналізу всієї палітри поглядів в цій галузі знань. На нашу думку, більш універсальним є визначення комп’ютерної злочинності, сформульоване дослідниками з ФРН. Вивчення цієї проблеми дає можливість і нам сформулювати свою позицію відносно поняття комп’ютерної злочинності. Під комп’ютерною злочинністю, на наш погляд, необхідно розуміти суспільно небезпечну дію чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп’ютерної техніки з метою спричинити збитки майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи.

Сформульоване визначення поняття комп’ютерної злочинності дозволяє зробити висновок, що це складне явище, яке потребує подальшого спеціального і системного вивчення.

В Україні комп’ютерна злочинність лише починає набирати силу і потребує наукового підходу.

Варто зазначити, що починаючи з 1990 року проблемами комп’ютерної злочинності в Україні займаються П.Д. Біленчук, В.Ф. Годованець, М.О. Зубань, М.В. Салтевський та інші. На сьогодні проблема комп’ютерної злочинності є однією з найпопулярніших дискусій XXI століття. Щодо окремих галузей юридичної науки, то тут приоритетними є такі напрями: для науки криміналістичного права – особливості кваліфікації даного виду злочинів; для криміналістики – засоби, методи і прийоми розкриття, розслідування і попередження злочинів; для судової психіатрії – діагностування комп’ютерних фобій та їх зв’язок з проблемами неосудності.

РОЗДІЛ 2
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНОЇ ЗЛОЧИННОСТІ У КРЕДИТНО-ФІНАНСОВІЙ СФЕРІ

На сучасному етапі у вітчизняній криміналістичній науці не існує скільки-небудь узагальнюючих даних для формування визначень основних елементів криміналістичної характеристики комп'ютерних злочинів.

Криміналістична характеристика комп'ютерних злочинів відрізняється від вже відомих криміналістичній науці злочинних посягань певною специфікою. На наш погляд, в першу чергу до неї повинні входити криміналістично значимі відомості про особу правопорушника, мотиви та мету його злочинної поведінки, типові засоби, предмети та місця посягань, а також про потерпілу особу та сліди злочину.

Як відомо, особа злочинця є об'єктом криміналістичного дослідження і багато типологічних даних про неї є елементом криміналістичної характеристики злочинів. Однак рамки криміналістичного вивчення особи злочинця обмежена, як правило, властивостями особи, які необхідні для використання з метою кримінальної профілактики, попередження та розслідування злочинів. Дослідженню цих проблем приділено достатню багато уваги у кримінологічній літературі. Ряд рис особи злочинця залишається обмеженими кримінологічною характеристикою. В свою чергу – це головним чином «професійні» навички злочинців, які відображаються в певних засобах та прийомах вчинення злочинів, залишаючи на місці події певний «почерк» злочинця. Виявлені на місці події речові докази надають інформацію про деякі його особисті соціально-психологічні властивості та якості, його злочинний досвід, професії, соціальні знання, стать, вік, взаємовідносини з потерпілою та інше.

Встановлення усіх можливих форм вираження особи, що відобразилися у первинній інформації про подію злочину дозволяє скласти уяву про загальні, а потім й індивідуальні властивості злочинця. Тотожна інформація, в повній мірі має криміналістичне значення. Так, з наукової точки зору, існує чітка класифікація криміналістично значимої інформації, яку поділяють за такими підставами: за джерелом отримання, за фізичною природою, за формою уявлення, за структурним елементом події злочину, за напрямом руху і призначенням, за процесуальним призначенням.

Аналіз зв'язку цієї інформації з виявленими даними про способи, механізм і обставини вчинення злочину створює нову самостійну інформацію, що дозволяє правильно визначити напрям та спосіб розшуку, затримання і викриття злочинця. Тому дані про те, хто частіше за все вчинює злочини даного виду, хоча й носить вираз кримінологічного характеру, проте використовується і у криміналістичній характеристиці злочину.

Криміналістично значимі дані про особу злочинця ґрунтуються на двох специфічних групах інформації. Перша з них включає в себе дані про особу невідомого злочинця за залишеними ним слідами як на місці події у пам'яті

компьютерно-технической экспертизы // Вісник Луганського інституту 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.

підприємницької економічної безпеки. – К., 1995. – 325 с.

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

свідка, так і за іншим джерелом з метою встановлення напряму та прийомів його розшуку та затримання. Частіше за все така інформація дає уявлення про загальні властивості певної групи осіб, серед яких можливо знаходиться злочинець, і винятково – про деякі якості конкретної особистості. Такі відомості з метою швидкого виявлення і пошуку злочинця повинні порівнювати з криміналістичними даними про те, хто частіше вчинює злочини даного виду. Друга група включає в себе інформацію, отриману за допомогою вивчення особи затриманого, підозрюваного або обвинуваченого з метою всебічної криміналістичної оцінки особи суб’єкта. З цією метою збирають відомості не тільки про життєві цінності, недоліки правосвідомості, антисуспільні погляди, але й про те, яка інформація про особу суб’єкта злочину, його зв’язки, способи поведінки до, під час та після вчинення злочину може допомогти слідчому або оперативному працівнику знайти з останнім необхідний контакт, отримати правдиві свідчення, допомогти в його викритті, а також вибрати найбільш ефективні засоби профілактичного впливу на нього. Вважається, що ці дані з урахуванням інформації про злочинця, враховані в інших елементах криміналістичної характеристики можуть бути покладені в основу типізації злочинців.

Виділення типових моделей різних категорій злочинців, знання основної мети цих людей дозволяє оптимізувати процес виявлення кола осіб, серед яких доцільно вести розшук злочинця та точніше визначити засоби встановлення і викриття конкретного правопорушника. Наприклад, у тих випадках, коли злочин вчинюється організованою злочинною групою або злочинним об’єднанням, воно стає самостійним об’єктом криміналістичного вивчення і відповідно до цього одним з елементів криміналістичної характеристики даного виду злочину. При цьому також, як правило, вивчаються властивості групи або об’єднання з точки зору ступеня їх організованості, структури, розгалуженості, ролевих функцій співучасників та інше. Встановлення цих властивостей дає можливість краще орієнтуватися в напрямах розкриття усіх ланок злочинної діяльності членів цих об’єднань та усіх основних епізодів цієї діяльності.

Як вже відмічалось, сам факт появи комп’ютерної злочинності в суспільстві багато дослідників ототожнюють з появою так званих «хакерів» (від англ. „*hacker*”) – користувачів обчислювальної системи (звичайної мережі ЕОМ), які займаються пошуком незаконних засобів отримання несанкціонованого (самовільного) доступу до засобів комп’ютерної техніки і даних у сукупності з їх несанкціонованим використанням з корисливою метою. Іноді у літературі і засобах масової інформації таких осіб називають «комп’ютерними»: «піратами», «злодіями», «шахраями», «електронними бандитами», «злодіями з електронними відмичками» тощо. До хакерів відносяться особи, які захоплюються комп’ютерною технікою, переважно з числа молоді – учні та студенти і спеціалізуються на зломах різних захисних систем СКТ (систем комп’ютерної техніки).

Усі вищенаведені назви у своїй сукупності визначають поняття «комп’ютерного» злочинця. Тому з криміналістичної точки зору характеристики його особи треба враховувати збиральне поняття у широкому

розумінні цього слова, хоча і з деяким поділом на самостійно відокремлені групи за низкою підстав. Розглянемо їх більш детально.

До першої групи «комп'ютерних» злочинців можна віднести особу відмінною рисою якої є стійке поєднання професіоналізму в галузі комп'ютерної техніки і програмування з елементами своєрідного фанатизму і винахідництва. На думку деяких авторів, ці суб'єкти сприймають засоби комп'ютерної техніки як своєрідний виклик їх творчим та професійним знанням, вміння і навичкам. Це й є у соціально-психологічному плані фактором спонукання до вчинення різних дій, велика кількість з яких має яскраво виражений злочинний характер. Під впливом вищевказаного фактора особам цієї групи відкриваються різні засоби несанкціонованого проникнення у комп'ютерні системи, що супроводжується переборювання засобів захисту, як постійно ускладнюються, що у свою чергу призводить до ускладнення алгоритму злочинних дій і об'єктивно сприяють збільшенню різних засобів вчинення комп'ютерних злочинів у кредитно-банківській сфері. Варто підкреслити, що характерна ознака злочинців цієї групи є відсутність в них чітко визначених протиправних намірів. Практично всі дії вчинені ними з метою прояву своїх інтелектуальних і професійних здібностей. Ситуація тут безумовно порівнюється з тією, яка виникає під впливом різноманітних комп'ютерних забав, стимулюючих розумову активність гравців, наприклад, під час гри у шахи. Коли у ролі одного гравця виступає гіпотетичний злочинець, а у ролі його суперника – загальний образ комп'ютерної системи та інтелект розробника засобів захисту від несанкціонованого доступу. Більш детальніше ця ситуація досліджена у математичній науці у теорії гри-моделі поведінки двох протиборчих сторін.

При цьому виділяють антагоністичні і неантагоністичні ігри, а також ігри, в яких одна зі сторін є людина, а інша – природа або ЕОМ. В останньому випадку взаємодія людини з комп'ютером здійснюється за визначеним грою алгоритмом з метою вивчення, тренування, імітації обставин і з розважальною метою. Особливу увагу у криміналістичній площині вивчення особи злочинця, на наш погляд, викликають фахівці-професіонали в галузі засобів комп'ютерної техніки. Узагальнюючі емпіричні дані дозволяють нам визначити такі соціально-психологічні характеристики цього кола осіб. Представники цієї спеціальності взагалі надто зацікавлені і мають непоганий інтелект та розумові здібності. При цьому вони не позбавлені певного своєрідного пустування і «спортивного» азарту. Зростання рівня захисту комп'ютерних систем ними сприймаються у психологічному плані як своєрідний виклик собі, тому вони жадають у будь-який спосіб знайти ефективний засіб доведення своєї переваги. Як правило, це й призводить до вчинення ними злочину. Поступово деякі суб'єкти даної категорії не тільки здобувають необхідний досвід, але й знаходять інтерес у цьому виді діяльності. В кінцевому випадку здійснюється орієнтація їх цілі, яка із стану «безкорисливої гри», переходить у нову якість – захоплення подібною «грою» краще за все сполучати з отриманням певної матеріальної користі. Це може проявлятися у злочинців як у відкритій формі – у різних ситуаціях при їх спілкуванні зі знайомими, друзями, родичами, співробітниками, так і у прихованій – у формі внутрішніх думок та страждань

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

180. Общие положения по назначению и производству компьютерно-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.

без яких-небудь зовнішніх проявів. Останні притаманні замкнутим за характером людям. Інші можуть демонструвати перед знайомими або співробітниками, родичами та іншими свої навички, знайти незахищені місця у комп'ютерній системі, а інколи і те, як ці слабкі місця можна використовувати в особистих цілях.

Таким чином, здійснюється розвиток та переродження «аматора-програміста» у професійного злочинця.

На наш погляд, до складу ознак, що вказують на вчинення комп'ютерного злочину особами даної категорії, можна віднести такі:

– відсутність цілеспрямованої, продуманої підготовки до злочину;

– оригінальність засобу вчинення злочину;

– використання як знаряддя злочину побутових технічних засобів та предметів;

– відкритість злочинних дій.

До розглянутої вище групи можна віднести ще одну, що включає в себе осіб, які страждають новим видом психічних захворювань – інформаційними хворобами або комп'ютерними фобіями.

Враховуючи новину та специфічність цього явища, розглянемо його більш докладно.

Виходячи з даних наукових досліджень цієї проблеми, можна виділити її складові, безпосередньо пов'язані з даним видом злочину. У спеціальній літературі відмічалося, що указана категорія захворювань викликається систематичним порушенням інформаційного режиму людини: інформаційним голодом, інформаційними перевантаженнями, втратою часу, пов'язаною з неплановим переключенням з одного інформаційного процесу на інший, нестача часу настроювання, інформаційним шумом.

У зв'язку з обладнанням робочих місць персональними комп'ютерами з метою підвищення швидкості інформаційних процесів та ефективності використання робочого часу, багато співробітників підпадають під різні стресові ситуації, деякі з яких закінчуються формуванням комп'ютерних фобій.

Насправді, це є не що інше, як професійне захворювання. Основні симптоми його прояву такі: швидка втома, різкі стрибкоподібні зміни артеріального тиску при аудіовізуальному контакті з комп'ютерною технікою, підвищене потовиділення, очні стреси, головокружіння та головні болі, тремтіння кінцівок, важке дихання, замління та інше.

Як бачимо, в основі комп'ютерної фобії лежить страх перед втратою контролю над своїми діями. Ситуація ускладнюється тим, що страждаючі фобією взагалі знають про ірраціональність їх страху, однак це робить їх більш сильними за принципом резонансу.

Комп'ютерна злочинність може вчинюватись особами, які страждають вказаними видами психічних захворювань. На наш погляд, за наявністю подібних факторів в процесі розкриття та розслідування комп'ютерного злочину, необхідне обов'язкове призначення спеціальних судово-психіатричних експертиз по даній криміналістичній справі на предмет встановлення осудності злочинця в момент вчинення ним злочинних дій. Це, в свою чергу, повинно впливати на кваліфікацію дій у випадку судового розгляду

справи.

Комп'ютерні злочини вчинені особою, хворою на психічне захворювання, в основному пов'язані зі злочинними діями, направленими на фізичне знищення або пошкодження засобів комп'ютерної техніки без злочинного умислу, з частковою або повною втратою контролю над своїми діями.

Третю і останню групу складають професіональні «комп'ютерні» злочинці з яскраво виявленою корисливою метою, так звані «профі». Відрізняючи від першої перехідної групи «любителів» і другої специфічної групи «хворих» злочинців, злочинці третьої групи характеризуються вчиненням комп'ютерних злочинів з обов'язковим використанням дій, направлених на їх приховування, і маючи в зв'язку з цим стійкі злочинні навички злочинці цієї групи є членами добре організованих, мобільних та технічно оснащених обладнанням і спеціальною технікою (нерідко оперативно-технічного характеру) злочинних груп або об'єднань. Особу, яка входить до їх складу, у більшості випадків можна охарактеризувати як висококваліфікованого спеціаліста, який має вищу технічну, юридичну або економічну освіту. Саме ця група злочинців і являє собою небезпечну загрозу для суспільства, є кадровим ядром комп'ютерної злочинності як у якісному, так і у кількісному плані. На долю саме цих злочинців припадає максимальна кількість вчинених особливо небезпечних посягань, наприклад до 79% розкрадань коштів у великих та особливо великих розмірах, вчинені з використанням засобів комп'ютерної техніки.

На підставі вищевикладеного, а також з урахуванням аналізу спеціальної літератури, що узагальнює характеристику особи «комп'ютерного» злочинця, дані, які можна віднести до будь-якої з трьох розглянутих нами груп, можна викласти так.

Вік правопорушника можна визначити у межах 24 -45 років: вік 33% злочинців не перевищував 20 років, 13% – були старші 40 років та 54% – мали вік 20-40 років.

Більша кількість осіб даної категорії складають чоловіки (83%), але кількість жінок швидко збільшується за рахунок професійної орієнтації деяких спеціальностей і професій (секретарка, бухгалтер, касир тощо).

У професійно-класифікаційному плані коло «комп'ютерних» злочинців дуже широке. Це різні категорії спеціалістів та керівників: бухгалтера, банківські співробітники, менеджери, начальники відділів та служб, комерційні директора тощо. Усіх їх можна поділити на дві основні групи, виходячи з класифікаційної ознаки категорії доступу до засобів комп'ютерної техніки:

– внутрішні користувачі;

– зовнішні користувачі, де користувач (споживач) – суб'єкт, який звертається до інформаційної системи або посередника для отримання необхідної йому інформації і користується нею.

Користувачі бувають 2 видів: зареєстровані (санкціоновані) та незареєстровані (несанкціоновані, незаконні).

За оцінкою багатьох спеціалістів, основна небезпека в плані вчинення комп'ютерних злочинів виходить від внутрішніх користувачів: ними вчинюється 94% злочинів, тоді як зовнішніми користувачами тільки 6%, при цьому, 70% – це клієнти – користувачі комп'ютерних системи, а 24% –

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.

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 криміналістичного 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

обслуговуючий персонал. Такі злочини можна умовно поділити на три групи на підставі функціональної категорії доступу до засобів комп'ютерної техніки.

До першої групи можна віднести злочинців, які вчинили комп'ютерні злочини, що ґрунтуються на використанні програмних засобів. Частково, до них можна віднести: операторів ЕОМ, бухгалтерів, касирів, адміністраторів баз та банків даних, операторів-програмістів (системних та прикладних), інженерів-програмістів та інших.

До другої групи відносяться особи, які вчинили комп'ютерні злочини, що ґрунтуються на використанні апаратних засобів комп'ютерної техніки: операторів засобів зв'язку, інженерів по термінальному обладнанню, спеціалістів по комп'ютерному аудиту та інших.

До третьої групи відносяться особи, які вчинили комп'ютерні злочини, що ґрунтуються на непрямому доступі до засобів комп'ютерної техніки, тобто ті, хто займається управлінням організаційними питаннями: управління комп'ютерною системою, управлінням операторами, управління базами або банками даних, управлінням робіт за програмним забезпеченням, менеджери та інші.

Злочинцями з числа зовнішніх користувачів, як свідчить практика, є особи, добре поінформовані про діяльність потерпілої сторони. Їх коло дуже широке, тому їх можна систематизувати і класифікувати: ним може бути будь-яка особа, навіть випадкова людина. Наприклад, представник організації, зайнятий сервісним обслуговуванням, ремонтом, розробкою програмних засобів комп'ютерної техніки за договірною підставою, представники різних контролюючих та керівних органів або організацій, клієнтів або хаккерів.

Розглянемо мотив та мету вчинення комп'ютерних злочинів, які відіграють, на нашу думку, велике значення у формулюванні криміналістичної характеристики злочинів даної категорії справ. Мотив та мета вчинених злочинів прямо пов'язана із соціально-психологічної і криміналістичної характеристики особи злочинця. Узагальнюючи відомості про найбільш розповсюджені мотив та мету вчинення комп'ютерних злочинів – вони є одним з найважливіших компонентів криміналістичної характеристики злочину. Отже, мотив і мета злочинів, що входять у групи суб'єктивних факторів, які впливають на вибір засобів і прийомів досягнень мети, визначають характер основних дій злочинця, а відповідно, і зміст способу вчинення злочину, що являє собою комплекс вольових дій людини та підставою криміналістичної характеристики будь-якого злочинного посягання.

Мотив та мета в деяких випадках є необхідною ознакою суб'єктивної сторони умисних злочинів (наприклад, корисливий мотив при зловживанні владою або службовим становищем, метою розкрадання грошових коштів при несанкціонованому доступі до даних тощо). Зустрічаючі склади, в яких мета і мотив включені як кваліфікуючі ознаки (наприклад, хуліганське, спонукання при занесенні у комп'ютерну систему вірусу та мета приховати інший злочин при кваліфікованому розкраданні). Для більшості умисних злочинів мотив і мета не є необхідними елементами суб'єктивної сторони і, відповідно, не входять до кримінально-правової характеристики. Між іншим у всіх випадках при розслідуванні конкретного злочину мотив і мета повинні бути з'ясовані. Це

має важливе значення не тільки для визначення судом справедливого покарання за вчинене, але й сприяти повному розкриттю злочину. Відомості про найбільш поширені мотиви та мету вчинення комп'ютерних злочинів використовують при висуванні версій відносно суб'єкта і суб'єктивної сторони, а також при організації розшуку злочинця. Наприклад, слідча практика свідчить, що метою пошкодження та знищення фізичних носіїв машинної інформації у ряді випадків є приховання розкрадання матеріальних цінностей або грошей, де зберігались пошкоджені або знищені фізичні носії машинної інформації. Перевірка версій про їх повне або часткове знищення з метою приховання вчиненого розкрадання може навести на слід злочинців.

Виходячи з результатів вивчення зарубіжної та вітчизняних досліджень з цього питання можна відмітити найбільш поширені мотиви вчинення комп'ютерних злочинів:

– корисні спонукання – 66% (вчинюються, як правило, злочинцями третьої групи);

– політична мета – 17% (шпигунство, злочини, спрямовані на підрив фінансово- і кредитно-грошової політики, на дезорганізацію валютної системи країни, на підрив ринкових відносин – вчинюється винятково злочинцями третьої групи);

– дослідницький інтерес – 7% (студенти і професіональні програмісти з числа злочинців першої групи);

– хуліганські спонукання – 5% (хаккери, злочинці першої групи);

– помста – 5% (злочинці першої та другої групи).

Практика свідчить, що типовою злочинною метою для досягнення якої неправомірно використовуються комп'ютери, є: крадіжки коштів з грошових фондів; фальсифікація платіжних документів; крадіжка машинного часу; підробка рахунків і платіжних відомостей; вторинне отримання вже проведених виплат; приписка надурочних годин роботи; придбання запасних частин і рідкісних матеріалів; фіктивне підвищення по службі; внесення змін в машинну інформацію; перерахування грошей на фіктивні рахунки; здійснення покупок з фіктивною оплатою; занесення комп'ютерних вірусів з метою вимагання.

При цьому, як правило, 52% злочинців пов'язані з розкраданням коштів: 16% – з знищенням та пошкодженням засобів комп'ютерної техніки; 12% – з підміною вихідних даних; 10% – з розкраданням інформації та програм і 10% – пов'язано з розкраданням послуг.

Не менший вплив на структуру криміналістичної характеристики комп'ютерних злочинів здійснюють узагальнюючі відомості про потерпілу сторону. Криміналістично значима інформація дозволяє більш широко характеризувати особу злочинця, мотиви вчинення злочину, і відповідно допомагає точніше окреслити коло осіб, серед яких необхідно шукати злочинця, та планувати заходи з розшуку найбільш важливих доказів по справі.

Зокрема, виявлення та вивчення криміналістично значимих ознак потерпілої сторони та її поведінки (перед, під час та після вчинення злочину) дає можливість глибше розібратися у багатьох обставинах злочину, особливо вказуючи на мотиви поведінки злочинця, його загальні (типові) та

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.

індивідуальні ознаки. Це пояснюється тим, що між злочинцем і потерпілою стороною частіше за все простежується певний взаємозв'язок, в силу чого злочинці не випадково вибирають їх об'єктами свого злочинного посягання. Особливо важко виявити та вивчити цей зв'язок на початку розслідування.

За даними Ю.М. Батуріна групи потерпілих сторін від комп'ютерних злочинів виглядає так:

– власники комп'ютерної техніки складають 79%;

– клієнти, які користуються їх послугами – 13%;

– треті особи – 8%.

Примітний той факт, що потерпіла сторона першої групи є власником системи, повідомляє (якщо повідомляє взагалі) у правоохоронні органи про подію вчинення комп'ютерного злочину. А вони складають більшу частину, і відповідно більша кількість й самих факторів вчинення таких злочинів, оскільки цим і можна пояснити високий рівень латентності комп'ютерних злочинів. При цьому зареєстровані комп'ютерні злочини виявляються так:

– виявляються у результаті регулювання перевірок доступу до даних служб комерційної безпеки – 31%;

– встановлення за допомогою агентурної роботи, а також при проведенні оперативних заходів по перевірці заяв громадян – 28%;

– випадково – 19%;

– у ході проведення бухгалтерських ревізій – 13%;

– у ході розслідування інших видів злочинів – 10%.

Спеціалісти виділяють такі фактори, що впливають на вирішення потерпілою стороною питання про звернення у правоохоронні органи по факту вчиненого комп'ютерного злочину:

– некомпетентність співробітників правоохоронних органів у питанні встановлення самого факту вчинення комп'ютерного злочину, не кажучи вже про процес його розкриття та розслідування;

– боязнь підриву власного авторитету у ділових колах і, як результат цього, – втрата значної кількості клієнтів. Ця обставина характерна особливо для банків, що займаються широкою автоматизацією виробничих процесів;

– неминуче розкриття у ході судового слідства системи безпеки організації;

– боязнь можливості у ході розслідування злочинів власного незаконного механізму здійснення окремих видів діяльності і проведення фінансово-економічних операцій;

– виявлення у ході розслідування комп'ютерного злочину причин, що впливають на його вчинення, можна поставити під сумнів професійну компетентність окремих посадових осіб, що в кінцевому випадку призведе до негативних для неї наслідків;

– правова і законодавча безграмотність посадових осіб у питаннях даної категорії;

– організації мають не дуже добре уявлення про реальні цінності інформації, яка знаходиться в її комп'ютерних системах.

РОЗДІЛ 3
СПОСОБИ ВЧИНЕННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ В КРЕДИТНО-ФІНАНСОВІЙ СФЕРІ

Небагатьом з історії людства кримінально-правовим інститутам вдалося здійснити такий швидкий прогрес, як це зроблено інститутом економічної злочинності. Менш ніж за сто років цей інститут зазнав значних змін, став одним з центральних кримінологічних понять (перш за все, у західній кримінології). Нажаль, що стосується кримінально-правового поняття «економічна злочинність», то його не існує й досі.

Щоб зрозуміти зміст кримінологічного поняття «економічна злочинність», треба звернутись до об'єкту економічної злочинності.

Об'єктом економічної злочинності є система виробничих ресурсів. Так, якщо на початку XX століття дуже важливим чинником виробництва була власність на його засоби, то в сучасних умовах таким чинником стала система управління. Відповідно, якщо в той самий період економічна злочинність розумілась як злочинність злиднів (різні посягання на власність), то вже в середині XX століття під нею розумілась злочинність «білих комірців».

Найбільш масштабні дослідження економічної злочинності були виконані такими вченими як Сатерленд (1939), Ньюмен (1958), Маннхейм (1965), Клинард (1979), Кайзер (1980), Тидеман (1987), Шнайдер (1987) та іншими. У 70-роки значно зростає інтерес до дослідження явищ економічної злочинності, оскільки саме тоді роль управління та інформації, можливості використання їх у злочинних цілях різко зростають. У цей час суттєво вдосконалюється законодавство в країнах з розвинутою ринковою економікою щодо боротьби з економічною злочинністю, розроблюються національні та міжнародні програми з вивчення цього явища та боротьби з ним. Разом з тим, не дивлячись на неабиякі зусилля, що здійснюються фахівцями в галузі кримінального права та кримінології, поки що не існує загальновизнаного визначення економічної злочинності.

Однією з характерних ознак економічної злочинності є суттєва економічна шкода, що заподіяна злочином. Однак вивчення технології управління діяльністю корпорації довели, що одним з масових видів економічної злочинності є свідоме порушення корпораціями техніки безпеки та законів про охорону здоров'я, охорону оточуючого середовища робітників та службовців. Такий вид злочину, дуже характерний і для економіки України, він тісно пов'язаний з існуючою системою менеджменту. За оцінками вчених, свідоме порушення менеджментом техніки безпеки праці, випуск недоброякісної продукції та порушення законів про охорону навколишнього середовища в декілька разів перевищують смертність від традиційної злочинності. Отже, найсуттєвішою шкодою для суспільства, яка пов'язана з існуванням економічної злочинності, є величезна фізична шкода.

До характерних ознак економічної злочинності з боку її суб'єкта варто віднести наявність подвійності – як фізичної, так і юридичної особи. Ознаки

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

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.

фізичної особи тісно пов'язують з її професійною економічною діяльністю, використання функцій менеджера, можливістю пристосування внутрішнього і зовнішнього середовищ управління для злочинної діяльності, свідомого використання прикриття діяльності менеджера для вчинення злочину.

Важливо звернути увагу на характерну мотивацію в поведінці економічного злочинця: саме він не відчуває себе злочинцем, вважає, що злочинну діяльність здійснює заради інтересів підприємства або держави, його дії не мають спрямування проти конкретних громадян, підприємців. Юридичні особи є традиційним суб'єктом економічної злочинності.

Однією з центральних ознак економічного злочину є його об'єкт. Під об'єктом необхідно розуміти систему управління економікою в цілому та окремі її елементи. Економічна злочинність паразитує саме за рахунок порушення нормального процесу управління економікою, використовує легальні управлінські технології у своїх злочинних цілях, свідомо порушує нормальне середовище процесів управління.

Ознаками економічної злочинності є суттєва шкода, що спричиняється суспільству. Так, за оцінками фахівців США, втрати лише від економічної злочинності корпорацій досягають від 174 до 231 млрд. дол. на рік, тобто більше 20% валового національного продукту цієї країни.

Економічна злочинність за своїм визначенням є найбільш масовий вид злочинності, тобто шкода завдається не окремим індивідам, а великому загалу.

Жертва економічного злочинця виступає як колективна та анонімна. Це підсилює небезпечність цієї злочинності, оскільки вона має більш прихований характер, ніж більшість видів загально-кримінальної злочинності. Жертва економічного злочину не відчуває себе жертвою.

Виходячи з окремих основних характеристик економічної злочинності при її кримінологічному вивченні необхідно звернути увагу на такі її особливості та ознаки:

– економічна злочинність охоплює різні зловживання влади, що посягають на порядок економічного управління;

– вчинюється в процесі професійної діяльності менеджера;

– завдає суттєву економічну шкоду інтересам держави, приватнопідприємницькій діяльності, групам громадян;

– множинність епізодів злочинів;

– вчинюється як фізичними, так і юридичними особами;

– складність персональної ідентифікації як злочинця, так і жертви економічного злочину;

– фактором, що спричиняє поширення економічної злочинності, є розвиток кризових явищ в економіці, посилення боротьби за економічну владу, за перерозподіл сфер впливу, розширення можливостей застосування кримінальних способів захоплення економічної влади.

Економічна злочинність – це протиправна діяльність, яка охоплює різні зловживання економічної влади, що посягають на порядок економічного управління, спричиняє суттєву економічну шкоду інтересам держави, приватній підприємницькій діяльності або групам громадян, вчинюється

постійно в межах та під прикриттям законної економічної діяльності менеджера з метою отримання наживи як фізичними, так і юридичними особами.

Вивчення сутності економічної злочинності потребує розгляду окремих їх видів та класифікації. Є різні системи класифікації, які визначаються основою, на якій будується окрема система.

До першої з них необхідно віднести такий вид групування економічної злочинності, який об'єднується системою порушень законів при здійсненні злочинних дій, тобто побудованих відносно законодавчої основи.

До іншої можна віднести групування щодо об'єкта посягань, який складають економічні злочини (окремі класифікації містять 20-30 складів злочинів).

А найбільш прийнятою є класифікація, що подана німецьким кримінологом А. Кайзером. А саме:

1. Злочини проти банківської та акціонерної системи обміну; кредитної системи; системи страхування та свободи конкуренції, включаючи зловживання довірою та удавані банкрутства, як і порушення авторських прав та прав маркування.

2. Ухилення від сплати податків; шахрайство з субсидіями; вимагання; хабарі.

3. Порушення законодавства про охорону праці; злочини проти споживачів, оточуючого середовища.

4. Шахрайства та спекуляція.

Недоліком цієї класифікації є те, що вона недостатньо враховує злочинність корпорацій, яка в найбільшій мірі характеризує саме економічну злочинність. До видів зазначеної класифікації можна віднести такі злочини, що становлять основу економічної злочинності у всіх країнах з економікою ринкового спрямування.

1. Злочини, що зв'язані з порушенням правил вільної конкуренції (наприклад, порушення антидемпінгового законодавства, промислове шпигунство, а також маніпуляції з цінами, змова про фіксування цін).

2. Злочини, які складають порушення прав споживачів (випуск недоброякісної продукції, різні шахрайства, що спричиняють матеріальну шкоду споживачам).

3. Злочини, що посягають на фінансову систему держави (приховування прибутку, ухилення від сплати податку, порушення контролю за торгівлею та виробництвом).

4. Злочини, що ґрунтуються на зловживаннях інвестиціями і спричиняють збитки компаньйонам, акціонерам тощо (різні шахрайства з бухгалтерськими документами, цінними паперами).

5. Злочини, які складають зловживання депозитним капіталом і спричиняють збитки депозитаріям, кредиторам, гарантам (удавані банкрутства, махінації з субсидіями, шахрайства у сфері страхування, неповернення кредитів із наступним їх розкраданням).

6. Злочини, що посягають на фінансовий комерційний сектор економіки (використання банківських документів – кредитних авізо, чеків, шахрайства

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.

68. Голубєв В.О. Програмно-технічні засоби захисту інформації від

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.: Вид-во Європ. ун-ту, 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.

52. Воры проникли в компьютерную сеть Национального банка // Голос

під виглядом конвертації гривні, використання підроблених пластикових платіжних засобів (електронних грошей).

7. Злочини, що пов'язані з незаконною експлуатацією природи і порушенням діючих економічних стандартів та нормативів у захисті оточуючого середовища, і які спричиняють йому шкоду (забруднення техногенними відходами, незаконне будівництво, виробництво шкідливих та небезпечних продуктів тощо).

8. Злочини, які складають свідоме порушення правил техніки безпеки праці з боку менеджменту та спричиняють матеріальні збитки і фізичну шкоду робітникам.

9. Злочини, які складають зловживання та шахрайства у сфері соціального страхування та пенсійного забезпечення робітників.

10. Комерційні хабарі.

11. Комп'ютерні злочини.

12. Злочини в галузі інформаційних технологій.

Існують й інші корисливі злочини, що вчинюються з використанням можливостей кредитно-банківської системи.

Істотне підвищення ефективності боротьби з економічною злочинністю може бути лише за умови проведення глибокої економічної реформи, удосконалення законодавства, що забезпечує функціонування здорового ринкового середовища, створення відповідної законодавчої бази діяльності правоохоронних органів, зокрема, діяльності апаратів ДСБЕЗ і служби ОЗ МВС України.

Питання, що стосуються аналізу злочинності взагалі, та економічної, зокрема, досить складні і багатогранні. Вони мають не тільки велике теоретичне, а й перш за все, практичне значення, оскільки саме стан економіки держави визначає всі інші сторони життя суспільства, де вирішується майбутня доля Української держави, закладається фундамент її реального суверенітету та міжнародного авторитету. Отже, визначаючи роль економіки в суспільстві, можна впевнено сказати, що вона завжди «править бал».

Проте, кримінологічна ситуація в Україні (особливо в сфері економіки) за останні роки значно погіршилась, що ускладнює проведення кардинальних економічних реформ ринкового типу, посилює соціальну напругу в суспільстві, створює додаткові труднощі в процесі розбудови самостійної, суверенної, незалежної, правової держави.

Як свідчать статистичні дані, що надходять в МВС України, економічна злочинність тільки за 1993 рік зросла на 11,9% (у 1992 році зареєстровано 36860 злочинів, у 1993 році – 41253).

Питому вагу (22,9%) складають розкрадання державного і колективного майна шляхом привласнення, далі – порушення правил торгівлі (11,3%) і спекуляція (10,7%). При цьому дуже непокоїть зростання таких небезпечних злочинів, як незаконні операції з валютними цінностями (2,1%) та хабарництво (35,2%).

Які ж ознаки економічної злочинності в Україні?

По-перше, це глибока економічна криза, яка, у свою чергу, характеризується:

– значним і невпинним спадом виробництва і зменшенням обсягу валового внутрішнього продукту і національного доходу, а це вимагає кардинальних і невідкладних заходів щодо структурної перебудови всієї економіки і, зокрема, пріоритетних галузей, що визначають її подальший розвиток;

– небаченим розладом грошового обігу, стрімким зростанням цін і гіперінфляцією, остання, поєднавшись зі спадом виробництва, утворює таке дуже небезпечне економічне явище, як стагфляція;

– наявністю панування надмонополізованого державного сектора, питому вагу якого складають підприємства військово-промислового комплексу, а тому, поруч з проблемою роздержавлення, приватизації, акціонування державного сектору постає не менш складна і довгострокова проблема конверсії, що потребує часу і значних капіталовкладень;

– залежність України від імпорту енергоносіїв (нафти, газу) із закордону (переважно з Росії і Туркменістану), а також рівнем цін на них;

– розкладом довгострокових економічних зв'язків між підприємствами, регіонами, які створювались в умовах командно-адміністративної, централізовано-керованої системи колишнього Союзу, і необхідністю створення нової, притаманної ринку, системи таких зв'язків.

По-друге, нестабільність у політичному житті країни, відсутність твердого і послідовного курсу на кардинальні економічні реформи ринкового типу Верховна Рада, починаючи з листопада 1990 року, обговорювала та схвалювала в основному декілька програм переходу до ринку, та жодна з них не була реалізована. Хитання політичного курсу, нерішучість виконавчої влади під час розв'язання кардинальних питань ринкових реформ (зокрема приватизації, земельної), хибна економіка не додають впевненості іноземним інвеститорам і тому взагалі прогресивний Закон «Про іноземні інвестиції» належним чином не працює на ринок, не сприяє вкладенню іноземного капіталу в економіку України. Деякі кроки державної влади (наприклад, процес формування державного бюджету, який передбачає перерозподіл майже 90% національного доходу України) створюють враження на Заході, що тут більш зусиль здійснюється для реанімації колишньої, ще й досі до кінця не зруйнованої командно-адміністративної системи, ніж побудова нової, ринкової.

По-третє, стан економіки і політики не може не відбитися на соціальному рівні населення, більша частина якого живе за межею бідності, а значні прошарки його ледь животіють. Загострюється проблема зайнятості: багато людей працюють не повний тиждень, а інші – ідуть у вимушену відпустку без утримання. Перед багатьма підприємствами стоять проблеми виживання, як уникнути банкрутства.

Безумовно, втративши надію на краще майбутнє, не маючи відповідної соціальної підтримки з боку держави, не отримуючи платні в розмірі, що забезпечує прожитковий мінімум, певні прошарки населення втягуються в незаконне підприємництво, торгівельну діяльність тощо. Тому і злочинність у сфері економіки зростає щорічно і високими темпами.

Дуже непокоять масштаби організованої злочинності, оскільки кожний

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.: Вид-во Нац. ун-ту 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.

35. Васильев А.Н., Яблоков Н.П. Предмет, система и теоретические

СПИСОК ВИКОРИСТАНИХ І РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

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.
18. Безпека комп’ютерних систем. Злочинність у сфері комп’ютерної

третій злочин в Україні вчинено групою осіб. Особливо небезпечним є те, що більшість злочинних груп мають чітко сформовану структуру, добре озброєні і технічно забезпечені. Їх діяльність орієнована на кримінальний перерозподіл прибутків підприємств і комерційних структур шляхом вимагання (рекет), шантажу, установленню контролю над «тіньовою економікою», бізнесом, проникнення в легальні сфери економічної діяльності, кредитно-банківську систему. Особливо небезпечним у сфері економіки є злочини, спрямовані на підрив фінансово-кредитної системи держави.

По-четверте, не можна не відзначити, що існуюче законодавство та сам процес законотворення не сприяють «видужанню» економіки, не відповідають вимогам сучасності і, перш за все, такому стану розвитку суспільства, як перехід до ринкових відносин. Ще й досі не прийнято три найважливіших збірники законів, яким належить провідна роль у створенні необхідного режиму функціонування ринкової економіки (цивільний кодекс України) та правового захисту цієї економіки від кримінальних дій (Кримінальний кодекс України, Кримінально-процесуальний кодекс України), а як відомо, правовий вакуум завдає значної шкоди суспільству.

До економічних злочинів варто віднести і такі як розкрадання державного або громадського майна шляхом крадіжки, розтрат або зловживання, спекуляція, обман покупців і замовників, хабарництво тощо. За даними обстежень ці види злочинів складають близько 23,3% від усіх злочинів, передбачених кримінальним законодавством України. Питому вагу серед них складають крадіжки – 18,6% та розкрадання державного і громадського майна шляхом крадіжки; розкрадання в особливо значних розмірах складають 2,1%, розкрадання шляхом зловживання службовим становищем, розтрати і привласнення – 1,1%, хабарництво – 0,4%.

Мафіозні владні структури в умовах оголошення так званої «ринкової економіки» розтягують державу і громадську власність і намагаються шляхом створення спільних з іноземним капіталом фірм і підприємств вивезти дешеву сировину, напівфабрикати і готову продукцію за межі України, вкласти на вигідних умовах в іноземні банки певні суми грошей.

Стрижнем ринкової інфраструктури є банківська система становлення і бурхливий розвиток якої ми спостерігаємо. Через неї проходить великий обсяг грошових розрахунків і платежів підприємств, організацій і населення, це єдина система економіки. Загальноекономічні види, що були притаманні «постсоціалістичній» банківській системі, призвели до посиленої криміналізації останньої, вона стала однією з основних носіїв економічної злочинності.

Перехід до ринку, широка демократизація економічного життя вимагали подолання монополізму в усіх сферах економіки (в тому числі – в банківсько-кредитній) та створення вільного ринку позичкових капіталів.

Головним моментом у трансформації банківської сфери в 1987-1988 роках стала побудова шести спеціалізованих державних банків: Державного центрального банку (Держбанку), Промисловобудівельного банку (Промбудбанку), Агропромбанку, Банку житлово-комунального господарства

і соціального розвитку (Житлосоцбанку), Банку трудових заощаджень і кредитування населення (Ощадбанку), Банку зовнішньоекономічних зв'язків (Зовнішекономбанку).

Названа реорганізація банківської системи була проведена поспішно, без розробки визначальної концепції і необхідної організаційної підготовки. Це привело до паралелізму в роботі банків. Різко зросла чисельність управлінського персоналу, виникли труднощі в проведенні кредитно-розрахункових операцій, збільшився документообіг. Між банками стали виникати відношення неекономічної конкуренції, яка іноді переходила в антагоністичні відносини.

У 1989 році почався перехід до дворівневої банківської системи. А з 1991 року Україна стала самостійно провадити на своїй території реформу кредитної системи.

Переформована кредитна система України включає в себе як банки, так і не банківські кредитні інститути.

Сучасна банківська система в нашій країні складається з двох рівнів банків: перший рівень – Центральний банк – (Національний банк України) з відповідною ланкою своїх установ, другий рівень – комерційні банки.

Національний банк України – разом з управлінням Центрального банку Республіки Крим та державними банківськими установами всіх рівнів утворює єдину систему, яка ґрунтується на спільній грошовій одиниці і виконує функції резервної системи.

Він виконує такі функції:

– здійснює емісію грошей та організацію їх обігу;

– організує розрахунки між банками;

– обслуговує державний борг України;

– проводить операції на ринку цінних паперів та валютному ринку;

– видає комерційним банкам ліцензії на проведення банківських операцій та операцій з іноземною валютою;

– здійснює контроль за діяльністю комерційних банків.

Національний банк України підзвітний Верховній Раді України. Йому належить виключне право випуску готівки в обіг та її вилучення з обігу відповідно до функцій резервної системи. У цьому зв'язку Національний банк України:

– встановлює порядок ведення касових операцій в народному господарстві;

– організує виготовлення банкнот і металевих грошей;

– встановлює правила перевезення, зберігання та інкасації готівки;

– забезпечує утворення резервних фондів банкнот і металевих грошей;

– визначає порядок обліку пошкоджених банкнот та їх знищення.

Крім того Національний банк управляє грошовим обігом у країні і щорічно розроблює проект головних напрямів єдиної державної грошово-кредитної політики, який затверджується Верховною Радою України, здійснює контроль за дотриманням комерційними банками банківського законодавства. У випадку систематичного порушення ними цієї вимоги має право:

– ставити перед засновниками комерційних банків питання про

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

проведення заходів фінансового оздоровлення їх діяльності (збільшення власних коштів, зміну структури активів тощо), про реорганізацію чи ліквідацію банків;

– застосовувати санкції у вигляді:

а) стягнення грошового штрафу у розмірі додаткового доходу, одержаного внаслідок неправомірних дій банку;

б) підвищення норми обов'язкових резервів;

в) призначення тимчасової адміністрації по управлінню банком на строк, необхідний для його фінансового оздоровлення;

г) відкладання ліцензії на здійснення банківських операцій.

Комерційні банки – це кредитні установи, що здійснюють універсальні банківські операції для підприємств усіх галузей господарства, головним чином – за рахунок грошових капіталів і заощаджень, залучених у вигляді внесків.

Комерційні банки здійснюють на договірних умовах кредитно-розрахункове та інше банківське обслуговування юридичних осіб та громадян шляхом здійснення операцій і вчинення інших банківських послуг.

Комерційні банки відрізняються:

– за призначенням статутного фонду та засобу його формування. У цьому зв'язку вони виступають у формі акціонерних товариств та товариств з обмеженою відповідальністю;

– за видами здійснюваних операцій банки бувають універсальні або спеціалізовані;

– за територією діяльності – республіканські, регіональні.

Банки здійснюють свою діяльність на основі ліцензій на ведення банківських операцій, одержаних від Національного банку України.

Водночас з видачею ліцензій на проведення банківських операцій Національний банк України реєструє комерційні банки в своїй книзі.

Крім банків, кредитна система включає в себе спеціальні фінансово-кредитні інститути. В Україні до небанківських кредитних установ відносяться каси взаємодопомоги, ломбарди, пенсійні фонди, органи державного та акціонерного страхування. А недавно почався процес утворення лізингових, інвестиційних та фінансових компаній.

Соціально-економічні проблеми перехідного періоду, нерозвиненість ринкових структур, глибокі прорахунки в механізмах створення та функціонування фінансово-кредитної системи, відсутність підприємницької культури, ефективної, сталої нормативно-правової бази та відносно повільне створення правоохоронних структур протидії злочинним проявам, створили сприятливі умови для бурхливого розвитку зловживань в банківській сфері та фінансових махінацій. Фінансово-кредитна система, враховуючи її виняткове значення для механізмів ринку, з одного боку, і ступінь криміногенного ураження з іншого, перетворюється на найпотужніший генератор економічної злочинності. Це загрожує подальшою криміналізацією сфер економічного життя України, крахом спроб добитися економічної та соціальної стабільності.

Досвід країн з розвитою ринковою економікою свідчить про сталу

тенденцію до зростання фінансових зловживань і банківських злочинів. Збитки лише в 1990 році становили понад 6% від суми загального обсягу банківських операцій, тобто сотні мільярдів доларів. Це робить банківсько-кредитну сферу об'єктом пильної уваги законодавця та правоохоронних органів, взаємодії останніх з банківськими структурами, яке постійно вдосконалюється.

Одним із найпоширеніших явищ, яке тісно пов'язане з корупцією, банківською злочинністю є використання штучно дешевих кредитних ресурсів. Ніде у світі централізований кредит, тобто емісія, не продається. Це спеціалізовані гроші, які дуже жорстко контролюються по сумі, по своєму витрачанню. В Україні не створена і продовжує діяти система, коли не ринки, а Національний банк, якому вигідно тримати низьку ставку Ощадбанку. Ця ставка суттєво нижча за інфляцією, що означає – держава постійно бере із кишені звичайного вкладника.

Гострота економічних протиріч у банківсько-кредитній системі України полягає в тому, що на середину 1994 року на 95% акціонованій банківській системі протистоїть на ті ж 95% державна форма власності. Але ж фінансова стійкість банку України на 90% залежить від економічної стійкості клієнтів, що є підприємствами народного господарства. Банки та банківська система – це дуже крихкий але й великовартістний інструмент управління народним господарством, економічною реформою, а отже, і захистом від економічної злочинності. Саме банківська система України здатна виконати роль щита від криміналізації економіки.

Національна фінансово-кредитна система на етапі формування багатоукладної економіки з відповідними формами власності переживає складний етап становлення як банківської системи, так і небанківських кредитно-фінансових інститутів. На сьогодні вже закріпилися на ринку фінансово-кредитних послуг і розгорнули свої операції страхові організації, пенсійні фонди, інвестиційні компанії. Діяльність інших небанківських кредитно-фінансових інститутів, таких як лізингові та факторингові компанії, довірчі товариства тільки розгортається.

Банківська система стає центральною ланкою криміналізації технологічного ланцюга по «відмиванню капіталів», здобутих злочинним шляхом, а також основним виконавцем випуску в безготівковий обіг фіктивно утворених грошових коштів. Усе це супроводжується інтернаціоналізацією ділків тіньової економіки зарубіжних країн (особливо країн СНД) при наявності процесуальних бар'єрів для працівників правоохоронних органів, що виникли внаслідок руйнування єдиного правового простору між суб'єктами колишнього СРСР.

Вивчення досвіду боротьби органів внутрішніх справ України країн СНД з економічною злочинністю, обґрунтований аналітичний прогноз можливих правопорушень у сфері банківської діяльності дають можливість детальніше розглянути детальніше кримінологічні процеси, що проходять в основній ланці фінансово-кредитної системи.

За технологією вчинення таких злочинів, структурою та колом учасників цих протиправних діянь, їх способи можна поділити на такі, що

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.

здійснюються безпосередньо в банках, і ті, що скоюються у сфері підприємства, з використанням установ банківської системи. Діапазон способів розкрадань, які здійснюються безпосередньо в банках, досить широкий – від привласнення грошових вкладів з рахунків полярних вкладників, які не зробили заповідального розпорядження чи не мають спадкоємців, до простого привласнення, яке часто розглядається як «тимчасове запозичення» касирами та іншими матеріально відповідальними і посадовими особами довірених їм грошових коштів та вилучення грошей з інкасаторських сумок шляхом їх замаскованого розпорювання інкасаторами. Однак, перераховані способи прості за виконанням, а сума збитків не є небезпечною. Вони були відомі й раніше і тому деталізації не потребують.

Найбільш поширеною та суспільно небезпечною є категорія зловживань, пов'язаних з утворенням, «відмиванням» та протиправним використанням фіктивних грошових коштів.

За способом вчинення ці зловживання поділяються на ті, що здійснюються шляхом використання:

– платіжних доручень, супроводжуваних фіктивними кредитовими авізо;

– незабезпечених лімітованих чекових книжок;

– незабезпечених чекових книжок у комбінації з кредитовим або дебетовим авізо;

– акредитива;

– векселя.

Необхідно зазначити, що фахівці в галузі комп'ютерних систем і деякі банківські керівники пов'язують надійність електронних банківських мереж із засобами їх зовнішнього захисту, тобто з шифруванням входу в саму комп'ютерну систему та її рівнів інформації в залежності від допуску тієї чи іншої групи користувачів. Коло операційних працівників, які за технологією виконання банківських операцій матимуть доступ до широкого діапазону цієї інформації, досить велика. А це, перш за все, широке коло людей, яким притаманні різного виду недоліки. Тому система захисту електронних мереж, що ґрунтується тільки на управлінні входів до різних видів інформації, є малоефективна. Щоб зробити відносно надійну систему захисту банківських електронних мереж, поряд зі старими потрібні принципово нові підходи. Така програма повинна будуватись на технології банківського документообігу та особливостях вчинення злочину з використанням тієї чи іншої форми розрахунково-кредитних операцій.

Правоохоронні органи країни, де поширені комп'ютерні злочини, стикаються з великими труднощами в розробці методології їх викриття та розслідування. Причиною цього є те, що фірми намагаються не виносити такі факти за межі підприємства, щоб не зашкодити своїй репутації. У Німеччині правоохоронним органам залишаються невідомими 80-90% комп'ютерних злочинів.

Розслідування комп'ютерних злочинів потребують ретельної підготовки і передбачають насамперед збір електронних доказів, які дуже легко можуть бути зниженні простим натисканням кнопки. Тактика перевірки та момент легалізації матеріалів повинен готуватись набагато старанніше, ніж при

злочинах, сліди яких зафіксовано в тих чи інших документах.

Не менш важким є судовий процес комп'ютерних злочинів, оскільки їх більшість вчинюється в анонімній атмосфері. Виявлені поліцією (міліцією) такі технічні засоби, як термінал чи персональний комп'ютер, не завжди можуть бути доказом вчинення злочину.

В якому напряму вирішується ця проблема країнами, де електронні банківські операції не супроводжуються відповідними платіжними документами? Як відзначив у виступі на міжнародній конференції з проблем «відмивання» грошей (Київ, 15-17 грудня 1993 р.) начальник відділу по розслідуванню фінансових злочинів МВС Франції Рене Уок, країни-члени Ради Європи ставлять собі за мету запровадити на законодавчому рівні документальне супроводження банківських електронних операцій. Про це також говорили деякі інші зарубіжні доповідачі. Тому при розробці програм для електронних банківських мереж у нашій країні цю проблему необхідно враховувати, щоб не зруйнувати існуючу систему документообігу, а потім повертатися до неї, на що знову будуть потрібні значні матеріальні та інтелектуальні витрати.

Вивчення і осмислення досвіду боротьби зі злочинністю у сфері економіки розвинутих країн відіграють велику роль у створенні правового забезпечення діяльності органів внутрішніх справ, розробці нових напрямів її попередження та профілактики.

При розробці стратегії боротьби з корисливим злочинами в кредитно-банківській сфері, основна увага держав з розвинутою ринковою економікою була зосереджена на контролі за «відмиванням» грошей, який є головною ланкою у вирішенні цієї проблеми. Ефективність його забезпечується системою організаційних, правових, економічних та інших заходів, які передбачають:

– наявність правової бази та урегульованість відносин у цій сфері нормами кримінального, адміністративного і цивільного права;

– створення системи тісно пов'язаних між собою органів соціального контролю, які наділені широкими повноваженнями для виконання покладених на них обов'язків;

– встановлення суворої відповідальності, і перш за все, економічної за порушення правових норм.

Інтенсивне впровадження автоматичної обробки інформації в економіці, промисловості, правлінні обумовило появу комп'ютерної злочинності. З кожним роком кількість таких злочинів різко зростає. Якщо тридцять років тому у США було зареєстровано перший комп'ютерний злочин, то на початку 1984 року їх уже налічувалось 1200 (за даними Стенфордського дослідного інституту).

Поряд із США широке розповсюдження комп'ютерної злочинності набуло у західноєвропейських та інших країнах, у таких як Великобританія, Нідерланди, Німеччина, Швейцарія, Канада, Австралія.

Для боротьби з комп'ютерними злочинами в Німеччині створена спеціальна служба, яка в 1984 році зареєструвала 222 повідомлення про протиправні дії в цій сфері, у 1985 році тут уже було зареєстровано 567

повідомлень про вчинення 635 комп'ютерних злочинів.

На думку зарубіжних спеціалістів, злочинний світ може найближчим часом відмовитися від пограбування банків, оскільки незаконне використання комп'ютерів обіцяє великі прибутки з меншим ризиком.

Умовно комп'ютерні злочини можна поділити на чотири основних види:

– шахрайство та маніпуляція з інформаційною технікою;

– незаконне використання машинного часу;

– крадіжки програмного забезпечення;

– комп'ютерний саботаж.