**ЕКОНОМІКА,
ФІНАНСИ,
ПРАВО**

- ***П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк***
  **ЗЛОЧИНИ В БАНКІВСЬКІЙ ІНДУСТРІЇ:
  КРИМІНАЛІСТИЧНИЙ СИСТЕМНИЙ 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
  КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ

- П. Біленчук, А. Кофанов, О. Кобилянський
  КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНІВ, ВЧИНЕНИХ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ

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

ЗЛОЧИНИ В БАНКІВСЬКІЙ ІНДУСТРІЇ:
КРИМІНАЛІСТИЧНИЙ СИСТЕМНИЙ 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, господарському 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+Інновації”
- Серія „Електронна фотографія та відеозапис”
- Серія „Криміналістичне забезпечення органів правопорядку”
- Серія „Археологія, архітектура, історія, культура, спадщина”
- 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
Василь Дмитрович ПОЛИВАНЮК

ЗЛОЧИНИ В БАНКІВСЬКІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ СИСТЕМНИЙ АНАЛІЗ

Навчальний посібник

В авторській редакції

Підписано до друку 08.09.2010.
Формат 60×84. Папір офсетний.
Тираж 300 прим.

Видавництво „КИЙ”
Адреса: 0436, Київ-136,
вул. Гречка, 13, кім. 216.

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

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

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

ЗЛОЧИНИ В БАНКІВСЬКІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ СИСТЕМНИЙ АНАЛІЗ

Навчальний посібник

Київ 2010

ББК 67.52я73
Б 61

Схвалено і затверджено кафедрою криміналістичної техніки ННІПСК КНУВС та рекомендовано до друку вченою радою Європейського університету управління, безпеки та інформаційно-правових технологій (протокол № 10 від 07.09.2010 року).

Рецензенти:
М.Т. Задояний – перший проректор Східноєвропейського університету економіки і менеджменту, професор.
Г.С. Семаков – професор Київського університету права Національної академії наук України.

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Поливанюк В.Д.
Б 61 Злочини в банківській індустрії: криміналістичний системний аналіз. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2010. – 88 с. – (Серія „Економіка, фінанси, право”).

У навчальному посібнику аналізується банківська система України як об’єкт криміналістичного дослідження.

Системно висвітлена криміналістична характеристика злочинів, вчинених в банківській системі України.

Для студентів і викладачів юридичних навчальних закладів.

ББК 67.52я73

© Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Поливанюк В.Д.
© Навчально-науковий інститут підготовки слідчих і криміналістів КНУВС, 2010.

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

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

ЗМІСТ

ПЕРЕДМОВА:
БАНКІВСЬКА ІНДУСТРІЯ ЯК ОБ'ЄКТ СИСТЕМНОГО КРИМІНАЛІСТИЧНОГО АНАЛІЗУ

Сучасний етап розвитку українського суспільства характеризується стратегічним курсом на створення суверенної незалежної демократичної правової держави. В країні здійснюються радикальні соціально-економічні реформи, йде процес демократизації усіх сторін суспільного життя, який неможливий без закріплення законності і правопорядку, забезпечення надійної охорони конституційних прав і свобод громадян.

Разом з тим в останні роки при загальному скороченні крадіжок, пограбувань та розбійних нападів зростає кількість розкрадань грошових сум з банків та інших кредитно-фінансових закладів, кас підприємств, організацій тощо.

Дестабілізуючи вплив на обстановку в країні набирає сили організована злочинність, яка в останні роки поряд із вчиненням загально-кримінальних злочинів інтенсивно інтегрується в економічну сферу з метою отримання високих незаконних прибутків, зливаючись при цьому з економічною злочинністю. У зв'язку з цим відбувається процес розширення масштабів злочинних проявів, який характерний практично для усіх галузей економіки України.

Особливе занепокоєння в цьому плані викликає факт виникнення та розвитку в Україні нового виду злочинних посягань, раніше невідомих вітчизняній юридичній науці та практиці, пов'язаних з використанням засобів комп'ютерної техніки та інформаційно-обробної технології – комп'ютерних злочинів.

Проблемам комп'ютерної злочинності в останні роки було присвячено багато уваги вченими-криміналістами в підручниках, навчальних посібниках та наукових виданнях. Проте більша частина з них присвячена дослідженню кримінально-правових та криміналістичних аспектів комп'ютерної злочинності, як вітчизняних так і зарубіжних дослідників, таких як Я.М. Батуріна, В.Б. Вєхова, С. Гришаєва, О.М. Жодзінського, О.М. Карак'янова, П.Д. Біленчука, М.А. Зубаня, А.Ф. Попова та інших.

Незважаючи на теоретичне та практичне значення зазначених досліджень, у цих працях не розглянуто в комплексі криміналістична характеристика , а також чітко не розглянуті проблеми, які стосуються практики і методів їх розкриття та попередження. Це негативно впливає на якісний рівень професійної підготовки співробітників правоохоронних органів, призводить до зниження ефективності слідчої та оперативної роботи по злочинам розглянутої категорії.

Тому, критично оцінюючи сучасний стан криміналістичної теорії та враховуючи потреби слідчо-оперативної практики, треба відзначити, що в цілому проблеми криміналістичної характеристики і попередження комп'ютерних злочинів вивчені недостатньо. Особливо багато питань пов'язаних зі змістом поняття та криміналістичної класифікації даних

1998.

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.

происшествия. – М., 1966. – 103 с.

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. Вашінгтон. – 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,

злочинних посягань, визначення способів їх вчинення, необхідності планування й своєчасності проведення тих чи інших слідчих дій на першочерговому етапі розслідувана злочинів. Необхідність всебічного дослідження цих проблем викликано як потребами слідчої практики, так й завданням її впливу на результати боротьби з комп’ютерними злочинами у кредитно-банківській сфері.

Перш ніж перейти до розгляду основних питань даної роботи, ми хотіли б дати визначення таких понять як банківська система, банк, показати структуру банківської системи та її класифікацію, визначити коло основних функцій банків.

Банківська система – це сукупність різних видів банків, та банківських об’єднань у їх взаємозв’язку і взаємодії.

Банки – це особливі фінансові інститути, які акумулюють грошові кошти, та інші накопичення (золоті запаси, цінні папери тощо), надають кредити, здійснюють грошові розрахунки, випуск в обіг грошей та цінних паперів, виконують операції з золотом тощо.

Виходячи із зазначення поняття банку, можна виділити такі основні функції банків:

– постійне кредитування галузей і підприємств;

– посередництво у міжнародному обігу позичкових капіталів;

– надання міжнародних кредитів;

– здійснення фондових, комерційно-посередницьких, довірчих, лізингових, факторингових, страхових операцій.

Банківська система України утворена після прийняття Верховною Радою України у 1991 році Закону «Про банки і банківську діяльність». Банківська система України складається з Національного банку і банків різних видів і форм власності.

Національний банк України є центральним банком, який здійснює єдину державну грошово-кредитну політикові з метою забезпечення стабільності національної грошової одиниці.

Банки утворюються на акціонерних або пайових засадах юридичними або фізичними особами. Свої функції банки реалізують через виконання таких функцій як зарахування засобів підприємств, закладів, організацій, населення на депозитні вклади; кредитування суб’єктів державної власності і громадян, інвестиції в цінні папери, формування активів; розрахунково-касове обслуговування, виконання валютних та інших банківських операцій.

Банки у своїй діяльності керуються Конституцією України, Законом України «Про Національний банк України», «Про банки і банківську діяльність», законодавством України про акціонерні товариства та інші види товариств, нормативними актами Національного банку України і власними положеннями.

Згідно зі статтею 99 Конституції України, прийнятою в 1996 році, основною функцією центрального банку держави – Національного банку України – є забезпечення стабільності грошової одиниці – гривні.

На виконання своєї основної функції Національний банк сприяє дотриманню стабільності банківської системи, а також, у межах своїх

повноважень, – цінової стабільності.

Національний банк виконує такі функції:

– відповідно до розроблених Радою Національного банку України Основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику;

– монопольно здійснює емісію національної валюти України та організує її обіг;

– виступає кредитором останньої інстанції для банків і організує систему рефінансування;

– встановлює для банків правила проведення банківських операцій, бухгалтерського обліку і звітності, захисту інформації, коштів та майна;

– організовує створення та методологічно забезпечує систему грошово-кредитної і банківської статистичної інформації та статистики платіжного балансу;

– визначає систему, порядок і форми платежів, у тому числі між банками;

– визначає напрями розвитку сучасних електронних банківських технологій, створює, координує та контролює створення електронних платіжних засобів, платіжних систем, автоматизації банківської діяльності та засобів захисту банківської інформації;

– здійснює банківське регулювання та нагляд;

– веде Державний реєстр банків, здійснює ліцензування банківської діяльності та операцій у передбачених законами випадках;

– веде офіційний реєстр ідентифікаційних номерів емітентів платіжних карток внутрішньодержавних платіжних систем;

– здійснює сертифікацію аудиторів, які проводитимуть аудиторську перевірку банків, тимчасових адміністраторів та ліквідаторів банку;

– складає платіжний баланс, здійснює його аналіз та прогнозування;

– представляє інтереси України в центральних банках інших держав, міжнародних банках та інших кредитних установах, де співробітництво здійснюється на рівні центральних банків;

– здійснює відповідно до визначених спеціальним законом повноважень валютне регулювання, визначає порядок здійснення операцій в іноземній валюті, організовує і здійснює валютний контроль за банками та іншими фінансовими установами, які отримали ліцензію Національного банку на здійснення валютних операцій;

– забезпечує накопичення та зберігання золотовалютних резервів та здійснення операцій з ними та банківськими металами;

– аналізує стан грошово-кредитних, фінансових, цінових та валютних відносин;

– організує інкасацію та перевезення банкнот і монет та інших цінностей, видає ліцензії на право інкасації та перевезення банкнот і монет та інших цінностей;

– реалізує державну політику з питань захисту державних секретів у системі Національного банку;

– бере участь у підготовці кадрів для банківської системи України;

– визначає особливості функціонування банківської системи України в

220. Салтевский М.В., Дьяченко А.Ф., Губанов В.А. Проблемы судебной 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. – С-Пб, 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

злочинних посягань: Настольна книга з питань банківської та 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.

разі введення воєнного стану чи особливого періоду, здійснює мобілізаційну підготовку системи Національного банку;

– здійснює інші функції у фінансово-кредитній сфері в межах своєї компетенції, визначеної законом.

РОЗДІЛ 1
БАНКІВСЬКА СИСТЕМА УКРАЇНИ ЯК ОБ'ЄКТ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ: ПРАВОВІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ

1.1. Правові основи діяльності банківської системи України

Банківська система України – один з найважливіших елементів її фінансової системи. Як і вся економіка України, банківська система сьогодні зазнає кардинальних змін, які торкаються структурної і функціональної її частини. Зміни фіксуються банківським законодавством, розробка якого здійснюється на основі міжнародного досвіду та економічних реформ, які проходять в Україні, а також сучасних уявлень про суть та призначення банківських установ.

Економічна природа банків розкривається в їх специфічній функції: виконувати на економічному ринку роль особливих фінансових посередників. В такій ролі банки залучають вільні грошові кошти, які звільнюються в процесі господарської діяльності одних суб'єктів – держави, господарюючих структур, фізичних осіб – та надаються на умовах забезпеченості, повернення, строковості, платності та цільової направленості на тимчасове користування іншим.

Саме система банків акумулює величезний фонд грошових коштів як в готівковій, так і в безготівковій формі.

Банк – це установа, функцією якої є кредитування суб'єктів господарської діяльності та громадян за рахунок залучення коштів підприємств, установ, організацій, населення та інших кредитних ресурсів, касове та розрахункове обслуговування господарства держави, виконання валютних та інших банківських операцій. Визначення поняття «банк» у законодавстві різних країн мають різний набір характерних рис, але практично у всіх правових системах світу обов'язковим є закріплення в тій чи іншій формі як мінімум двох банківських функцій: кредитування та розміщення на банківських рахунках вкладів клієнтів.[1]

Банківська система України є одним із найбільш динамічно розвинутих секторів національної, економіки, де перехід до ринкових відносин відбувся досить швидко і де реально проходить процес демонополізації, поступово починає діяти конкуренція, гроші та кредит набувають ринкового змісту.

Сучасна банківська система країни – це сфера різноманітних послуг своїм клієнтам: від традиційних депозитно-позичкових і розрахунково-касових операцій, що визначають основу банківської справи, до найновіших форм грошово-кредитних і фінансових інструментів, що використовуються банківськими установами (лізинг, факторинг, траст та ін.) (рис. 1.1.1)[2].

[1] Карманов Є.В. Банківське право України: навчальний посібник для студентів юридичних спеціальностей вищих закладів освіти. – Х.: Консум, 2000. – С. 52.

[2] Костюченко О.А. Банківське право. – К.: А.С.К., 2001. – С. 86.

К: Атіка, 2001. – С. 211-227.

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 Международної 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

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

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 врутр.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. –

Банківська система України складається з Національного банку України (НБУ) та інших банків, що створені і діють на території України. На 1 липня 1999 року в Україні було зареєстровано 208 банків з 2254 філіями, в яких працювало понад 125 тис. чоловік. Із загальної чисельності банків 176 установ функціонують у формі акціонерних товариств, 2 державних банки; у тому числі 28 банків, створених за участю іноземного капіталу та 9 банків зі 100%-м іноземним капіталом.

Правові основи банків, порядок створення та основні принципи їх діяльності визначені Законом України «Про Національний банк України», «Про банки і банківську діяльність»[1].

Банківська система України очолюється та регулюється Національним банком України, який є головним її елементом. Правове положення НБУ визначається Конституцією України (ст. 99, 100), Законом України «Про Національний банк України»[2] та іншими нормативними актами.

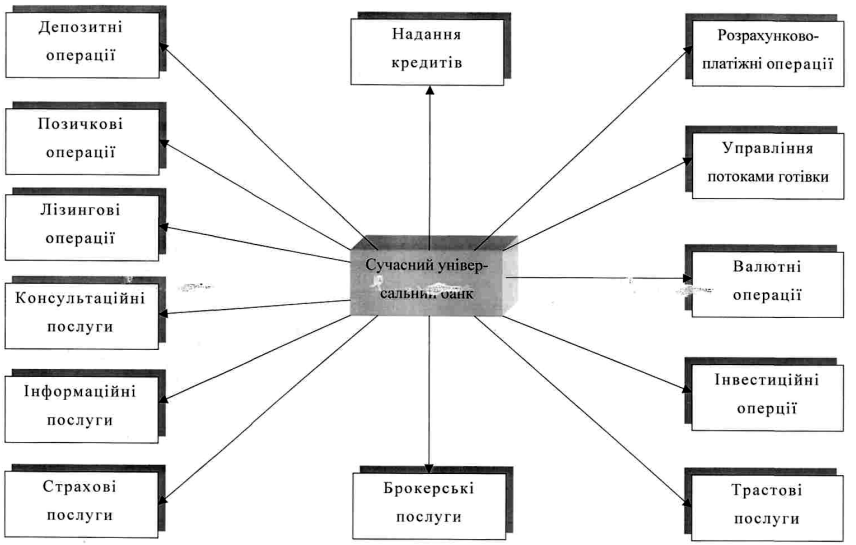

Рис.1.1.1. Операції та послуги сучасного універсального банку

Національний банк України є центральним банком України, особливим центральним органом державного управління. Він проводить єдину державну політику в галузі грошового обігу, кредиту, зміцнення грошової одиниці, організовує міжбанківські розрахунки, координує діяльність банківської системи в цілому.

[1] Відомості Верховної Ради, 2001, № 5-6, ст. 30.

[2] Відомості Верховної Ради, 1999, № 29, ст. 238, із змінами, внесеними згідно із Законами: № 1458-14 від 17.02.2000, ВВР, 2000, № 14-15-16, ст. 121; № 1658-14 від 20.04.2000, ВВР, 2000. № 29, ст. 230; № 1919-14 від 13.07.2000, ВРР, 2000, № 42, ст. 351; № 2121-14 від 07.12.2000, ВВР, 2001, № 5-6, ст. 30.

Національний банк України представляє інтереси держави у відносинах з центральними банками інших країн, у міжнародних банках та інших фінансово-кредитних організаціях, де міждержавне співробітництво передбачено на рівні центральних банків.

Структура Національного банку України будується за принципом централізації з вертикальним підпорядкуванням. До системи Національного банку України входять центральний апарат, філії (територіальні управління), розрахункові палати, Банкнотно-монетний двір, фабрика банкнотного паперу, Державна скарбниця України, Центральне сховище, спеціалізовані підприємства, банківські навчальні заклади та інші структурні одиниці і підрозділи, необхідні для забезпечення діяльності Національного банку України.

Національний банк України та його обласні управління здійснюють нагляд за діяльністю інших банків, що діють на території держави.

Національний банк України як суб'єкт правовідносин наділений специфічним правом – правом законодавчої ініціативи[1]. Варто зазначити, що для виконання своїх адміністративно-контрольних функцій Національний банк України видає нормативно-правові акти з питань, віднесених до його повноважень, які є обов'язковими для органів державної влади і органів місцевого самоврядування, банків, підприємств, організацій та установ незалежно від форм власності, а також для фізичних осіб[2]. Національний банк встановлює єдині правила бухгалтерського обліку в банках на основі комплексної автоматизації і комп'ютеризації. Нормативні акти Національного банку видаються у формі постанов правління Національного банку, а також інструкцій, положень, правил, що затверджуються постановами Правління Національного банку України. Ці нормативні акти не можуть суперечити законам України та іншим законодавчим актам України і не мають зворотної сили, крім випадків, коли вони згідно із законом пом'якшують або скасовують відповідальність.

Нормативно-правові акти Національного банку підлягають обов'язковій державній реєстрації в Міністерстві юстиції України та набирають чинності згідно з положеннями законодавства України. Нормативно-правові акти Національного банку можуть бути оскаржені відповідно до законодавства України.

Використовуючи надане йому законом право законодавчої ініціативи, Національний банк України активно займається нормотворчою діяльністю, готуючи проекти законів, інструкції, положення, вказівки та інші документи нормативного характеру, і заповнює ними прогалини в правовому середовищі функціонування банківської системи.

---

[1] Конституція України, ст. 93. – К.: Офіційне видання Верховної Ради України, 1996.

[2] Закон України «Про Національний банк України», ст. 56 // Відомості Верховної Ради України, 1999, № 29, ст. 238.

163. Матусовский Г.А. Методика расследования хищений: Учебное 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 експертизы // Следователь. – 2002. – № 7. – С. 30-32.

146. Кримінальний кодекс України. – К: Атіка, 2001. – 160 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., Цыркаль 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 розслідувння 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.

Існують різні види банків, які відрізняються формою власності, своїми функціями, організаційною структурою. За формою власності банки поділяються на державні та комерційні, а також кооперативні, акціонерні, а в залежності від операцій, які вони виконують – універсальні та спеціалізовані. За організаційною структурою виділяють банки, що мають широку мережу філіалів і такі, що їх не мають.

Законом України «Про банки та банківську діяльність» чітко визначені види операцій, які можуть здійснювати банки[1].

Це, зокрема залучення та розміщення грошових внесків і кредитів; здійснення розрахунків за дорученням клієнтів, банків-кореспондентів і їх касове обслуговування, випуск платіжних документів і цінних паперів (чеків, акредитивів, векселів, акцій, облігацій тощо); купівля, продаж і зберігання платіжних документів, цінних паперів, а також операцій з ними, видача поручительств, гарантій та інших зобов'язань за третіх осіб, що передбачає їх виконання в грошовій формі, купівля у організацій і громадян, а також продаж ним валюти.

З метою забезпечення гласності в роботі банків та доступності інформації про їх фінансовий стан, їх річні баланси, затверджені загальними зборами акціонерів, а також звіт про прибутки і збитки повинні публікуватися у пресі. А з метою оперативного кредитно-розрахункового обслуговування підприємств та організацій – клієнтів банку, територіально віддалених від місця розташування банку, він може організувати філії і представництва.

Принципом, на якому ґрунтується діяльність банків, є економічна самостійність, що має на увазі і економічну відповідальність банку за результати своєї діяльності. Економічна самостійність передбачає свободу розпорядження власними коштами банку і залученими ресурсами, вільний вибір клієнтів і вкладників, розпорядження прибутками банку[2].

Основна функція банків – посередництво в платежах між окремими самостійними суб'єктами.

Розрахунки між клієнтами одного й того самого банку здійснюються шляхом виконання відповідних операцій за їх рахунками, обминаючи кореспондентський рахунок банку. В інших випадках банк, який виконує доручення свого клієнта про здійснення тієї чи іншої банківської операції, змушений вступати у відносини з іншим банком, що обслуговує його контрагента. Таким чином, перш ніж клієнти банків зможуть здійснити відповідні розрахунки один з одним, в безготівковому порядку повинні розрахуватися їх банки.

[1] Закон України «Про банки та банківську діяльність», ст. 47 // Відомості Верховної Ради України, 2001, № 5-6, ст. 30.

[2] Голубєв В.О. Комп'ютерні злочини в банківській діяльності. – Запоріжжя: ВЦ «Павел», 1997. – с. 12.

Варто зазначити, що якби не існувало системи міжбанківських безготівкових розрахунків, то банки мали б передавати один одному готівку, тобто перевозити гроші з банку в банк. Однак у такому випадку міжбанківські розрахунки здійснювалися б досить довго та й самі операції були б надто ризикованими[1].

Загальний регламент щодо організації міжбанківських розрахунків та їх форми визначаються «Інструкцією про міжбанківські розрахунки в Україні», затвердженою постановою Правління Національного банку України від 27 грудня 1999 р. № 621. Згідно з цим документом, міжбанківські розрахунки – це безготівкові розрахунки між банками, що обумовлені виконанням платежів клієнтів або власними зобов'язаннями одного банку перед іншим.

Міжбанківські розрахунки можуть здійснюватися:

– через систему електронних платежів НБУ – розрахунки проводяться із застосуванням електронних засобів прийому, передачі, оброблення та захисту інформації. Система електронних платежів – це комплекс програмно-технічних засобів, призначений для виконання міжбанківських розрахунків між її учасниками;

– через власну внутрішньобанківську платіжну систему – розрахунки проводяться із застосуванням програмно-технічного комплексу з власними засобами захисту інформації, який експлуатується банком або об'єднанням банків і здійснює платіжний облік між установами цього банку (об'єднання) та іншими банківськими установами поза межами системи електронних платежів;

– через прямі кореспондентські відносини між банками.

З метою організації міжбанківських розрахунків Національний банк України запровадив автоматизовану систему розрахунків з використанням електронних прогресивних технологій у банківській справі на базі Центральної розрахункової палати. Ця система обслуговується комплексом програмно-технічних засобів, що забезпечують обмін електронними документами, їх перевірку, аналіз, захист від несанкціонованого втручання.

До функцій Національного банку України також відноситься те, що НБУ «визначає напрями розвитку сучасних електронних банківських технологій, створює, координує та контролює створення електронних платіжних засобів, платіжних систем, автоматизації банківської діяльності та засобів захисту банківської інформації»[1].

Стан автоматизації банківської діяльності в банках України дуже різний. Це пов'язано з тим, що банківський сектор економіки України – це сектор, який інтенсивно розвивається і постійно удосконалюється.

[1] Качан О.О. Банківське право: Навчальний посібник. – К.: Юрінком Інтер, 2000. – с. 139.

[2] Закон України «Про Національний банк України», ст. 7 ч. 1 п. 7 // Відомості Верховної Ради України, 1999, № 29, ст. 238.

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.

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.: «Ін Юре», 2001. – 684 с.

137. Криміналістика: Підручник. / За ред. П.Д. Біленчука. – К.: 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 міськсуду 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.

1990. – 158 с.

104. Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л. Основи захисту 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.: Вища 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: Вид-во 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:

У 1994 р. НБУ було прийняте стратегічне рішення щодо створення і впровадження системи електронних міжбанківських платежів (СЕП). Ця державна платіжна система об'єднала засобами електронної пошти в єдиний інформаційний простір всі комерційні банки України. СЕП створювалась як багаторівнева безпаперова система «брутто»-розрахунків.

Впровадження СЕП дало змогу відмовитись від використання поштових та телеграфних авізо, значно підвищити швидкість, якість і надійність виконання платежів, забезпечити безпеку та конфіденційність банківської інформації. Архітектура СЕП включає три рівні: комерційні банки (КБ), де функціонують програмно-технічні комплекси АРМ-3; обласний рівень НБУ, куди передаються платіжні повідомлення від КБ, представлений регіональними розрахунковими палатами (РРП) і відповідно комплексом АРМ-2; найвищий рівень – це центральна розрахункова палата (ЦРП) і комплекс АРМ-1, який проводить облік та контроль платежів у масштабі України в цілому. СЕП побудована і функціонує за міжнародними стандартами, виконуючи обробку та передачу повідомлень. Кожний комерційний банк є самостійним учасником СЕП і може вибрати одну з моделей обслуговування кореспондентського рахунку, яких зараз налічується сім. Банки, які мають власні платіжні системи, виходять лише на рівень ЦРП із загальними консолідованими сумами. СЕП дає змогу НБУ щоденно на десяту годину ранку мати актуальний баланс банківської системи України за попередній день. За допомогою СЕП щодня обробляється більш як 300 тис. платіжних документів на суму близько одного мільярда доларів США [26].

Створення і впровадження такої системи дало змогу національній банківській системі України стати однією з досить ефективних і отримати схвальні відгуки спеціалістів. Безумовно, як будь-яка комп'ютерна система, СЕП не є чимось сталим; це – система, яка постійно удосконалюється й розвивається. Зокрема, великих змін та трансформацій СЕП зазнала у зв'язку з переходом на міжнародні стандарти бухгалтерського обліку, який відбувся у січні 1998 р.

В НБУ функціонує електронний депозитарій для управління державними цінними паперами. Створюється проект впровадження національної платіжної системи для автоматизації масових готівкових розрахунків на основі пластикових карток. Деякі великі банки вже мають відповідні засоби й обслуговують міжнародні платіжні системи карток: VISA, Europay/Master Card та ін.

Аналізуючи стан справ на рівні комерційних банків, варто зазначити, що рівень впровадження сучасних інформаційних технологій у комерційних банках України дуже різний. Це пов'язано з надто швидким зростанням кількості банківських установ та різним рівнем їх фінансових можливостей щодо впровадження комп'ютерних технологій. Взагалі банківська система України перебуває на стадії свого становлення. Тому є банки, які мають лише набір засобів для формування необхідної звітності та програмних продуктів, що дозволяють банкам, згідно з вимогами Національного банку України, бути учасниками СЕП. Поряд з такими банками, які характеризуються невисоким рівнем комп'ютеризації робіт, є банківські установи, які добре розуміють, що

сучасні інформаційні технології є основним засобом підвищення конкурентоспроможності у боротьбі за пріоритетне становище на фінансовому ринку та залучення клієнтів. Тому в таких банках при виборі комп'ютерних систем перевагу надають технологіям, які розроблені з урахуванням міжнародних стандартів і відповідають вимогам відкритих систем, а також можуть легко переноситись з однієї платформи на іншу[1].

Для залучення нових клієнтів та створення зручностей щодо їх спілкування з банком у багатьох банківських установах впроваджена й успішно функціонує на підставі постанови Правління Національного банку України № 135 від 29.03.2001 «Про затвердження Інструкції про безготівкові розрахунки в Україні в національній валюті» система «Клієнт-банк». Впровадження такої системи дає змогу клієнту спілкуватися з банком і виконувати платежі, не виходячи з свого офісу, що, безперечно, підвищує привабливість банку при виборі його клієнтом. Ця система забезпечує передачу повідомлень між клієнтом та банком у зашифрованому вигляді за допомогою сертифікованих засобів захисту. Вимога сертифікації засобів захисту означає, що клієнт банку може включатися до системи електронних платежів лише тоді, коли його програмне забезпечення буде перевірене Національним банком України з точки зору забезпечення її захисту від доступу сторонніх осіб, щоб уникнути можливості викрадення коштів, а також відповідності такої системи технології банківських розрахунків. Використання клієнтом системи електронних платежів має здійснюватись на підставі окремого договору між ним і банком. Електронні документи, що подаються клієнтом до банку, повинні відповідати формату розрахункових документів системи електронних платежів Національного банку України із зазначенням електронних цифрових підписів відповідальних осіб платника. Яким згідно з установленими документами надане право підпису[2].

Варто зазначити, що деякі українські комерційні банки є учасниками міжнародної фінансової телекомунікаційної мережі.

Але якщо характеризувати ситуацію в цілому, то більшість автоматизованих банківських систем (АБС) розроблені як файл/серверні системи, що зорієнтовані на використання персональних комп'ютерів, працюють у локальній мережі і функціонують у середовищі таких систем управління базами даних (СУБД), як Clipper, FoxPro та ін. Це стосується як систем, розроблених силами спеціалістів банку, так і більшості систем, що пропонуються фірмами-розробниками банківських систем.

Системи, зорієнтовані на використання таких засобів, безумовно, відіграли велику роль у становленні банківської технології і створенні концепції АБС, але на сьогодні такі системи застаріли і мають ряд суттєвих недоліків. Основними недоліками є збої в роботі, що вимагає значних витрат на відновлення даних, а також зниження продуктивності системи при збільшенні кількості користувачів мережі.

---

[1] Єрьоміна Н.В. Банківські інформаційні системи: Навчальний посібник. – К.: КНЕУ, 2000. – ст. 7.

[2] Банківське право України: Навчальний посібник. / За заг. ред. Селиванова А.О. – К.: ІнЮре, 2000. – с. 125.

Терміни та визначення (від 01.01.96).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

83. ДСТУ 2938–94 Системи оброблення інформації. Основні положення.

Більшість банківських задач, що автоматизуються зараз, це переважно облікові, які можна віднести до класу задач OLTP (On-line Transaction Processing). Дуже незначна частка в АБС належить аналітичним задачам типу OLAP (On-line Analyse Processing Systems), за допомогою яких вирішувалися б такі задачі, як аналіз ресурсів, активів, прибутковості, стану фінансових ринків, оцінка ризиків тощо. Майже відсутні в АБС задачі класу DSS (Decision Support Systems) підтримка прийняття рішень, за допомогою яких можливе прийняття оптимального рішення при вирішенні неструктурованих чи слабоструктурованих проблем.

Основним напрямом удосконалення інформаційних технологій в банках є перехід від «файл/серверних» систем до систем типу «клієнт/сервер» з використанням професійних розподілених реляційних СУБД, зокрема, таких як Sybase, Oracle, Informix та ін.

Інформаційні системи, розроблені в середовищі цих СУБД, надають ряд істотних переваг при роботі з банківською системою:

1. Підтримка розподіленої бази даних не лише в локальній мережі, а і в територіально-розподіленій системі, що дає можливість банкам оперативно управляти роботою філій та контролювати їх.

2. Забезпечення надійності збереження даних за рахунок наявності механізму підтримки трансакцій та реплікацій, який забезпечує цілісність й узгодженість даних.

3. Виконання вимог гарантування безпеки банківської інформації шляхом розмежування і підтримки різних рівнів доступу та автоматизованого ведення журналу, який протоколює всі дії користувачів.

4. Відсутність суттєвих обмежень при використанні в банківській сфері з точки зору обсягів інформації в базі даних, швидкості обробки тощо.

5. Наявність сучасних засобів розробки клієнт/серверних технологій, таких як CASE – засоби та об'єктно-орієнтовані мови програмування.

Отже, банківська справа на сучасному етапі – це галузь, яка є передовою з точки зору впровадження сучасних інформаційних технологій.

Першою і основною вимогою, яка пред'являються до АБС, є вимога щодо її *функціональної повноти*. Повнофункціональною можна вважати систему, якщо набір її функцій дає змогу виконувати всі операції конкретного банку. Як правило, система, яка відповідає сьогоднішнім потребам, може не задовольняти їх завтра, якщо у банку з'являться нові функції. Тому наступною вимогою, що пред'являється до АБС, є її гнучкість.

Гнучкість – це один з ключових факторів, який полягає у тому, що будь-яка банківська система повинна мати можливість розширюватись та розвиватись і не лише фірмою-розробником, а й силами спеціалістів банку. Розвиток системи може відбуватися у двох напрямах: кількісному – при збільшенні кількості філій чи клієнтів та якісному – при розширенні спектра банківських операцій і послуг. Зміни кількісного характеру призводять до необхідності *нарощування* системи, яке може відбуватись двома способами:

– за рахунок встановлення у головній конторі більш потужної ЕОМ чи шляхом розпаралелення процесу обробки на кілька ЕОМ;

– за рахунок збільшення продуктивності обчислювальних комплексів у

філіях банку і переходу на розподілену обробку даних, зберігши за центральним обчислювальним комплексом лише функції консолідації балансу та обслуговування поточних інформаційних потреб.

Вибір способу нарощування АБС залежить від стратегії розвитку банку, особливостей взаємодії головної контори та її філій, а також від прийнятого розподілу функцій та відповідальності за них. Але в будь-якому разі розробник АБС повинен вказати конкретні шляхи вирішення проблеми нарощення системи для того чи іншого банку.

В цілому система повинна мати можливість розширення як по горизонталі (збільшення кількості клієнтів, каналів зв'язку тощо), так і по вертикалі (перехід на більш потужну техніку).

При цьому мають бути зведені до мінімуму можливі зміни:

– інтерфейсу користувача;

– технології роботи з системою;

– структури файлів бази даних

Також має бути виключена або зведена до мінімуму необхідність модифікації прикладного програмного забезпечення і перепідготовки персоналу.

Надійність полягає в тому, що АБС повинна забезпечувати роботу великої кількості користувачів, які одночасно можуть вводити, коригувати документи (рахунки чи угоди), формувати звітність без будь-яких конфліктів, пов'язаних з одночасним доступом до даних.

Реальний масштаб часу після введення документа АБС повинен забезпечувати його бухгалтерське приведення. Новий стан рахунків відразу стає доступним для всіх користувачів й відображається у балансі, а також може бути використаний при обчисленні нормативів. Система, побудована з урахуванням цієї вимоги, має такі переваги:

– дозволяє в будь-який момент часу мати повну картину фінансового стану банка;

– надає можливість оперативно відстежувати інформацію, що надходить у систему;

– надає можливість отримання додаткових кредитних ресурсів.

Інтегрованість системи означає, що система повинна складатися з інформаційно та функціонально пов'язаних між собою модулів. Інформаційний зв'язок полягає у тому, що всі складові системи працюють із спільною базою даних, що дає змогу уникнути дублювання та забезпечує цілісність й узгодженість даних. Функціональний зв'язок дозволяє функціональним задачам, які характеризуються однаковою прикладною логікою, але розв'язуються на різних АРМах, використовувати спільні процедури, що зберігаються у відповідних бібліотеках (наприклад, нарахування процентних ставок та ін.).

Забезпечення багатофіліальної роботи банку полягає в тому, що для банків, які мають багато філій, і особливо для тих, структура яких є трирівневою, важливим моментом є забезпечення єдності й цілісності технології. Виконання цієї вимоги в ідеальному варіанті – це забезпечення розподіленої обробки даних в режимі On-line. Забезпечення розподіленої

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

44. Вєртузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. Посібник / За ред. С.Г. Лаптєва. – К.: 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.

обробки даних в такому режимі коштує поки що досить дорого і під силу не всім банкам. Тому більш реальним з точки зору забезпечення цієї вимоги є єдність технологій, тобто як мінімум системи всіх рівнів повинні мати однакову структуру даних, однакові інтерфейси та інструментальні засоби розробки програмного забезпечення.

Безпека та захищеність системи – це одна з життєво необхідних вимог, що ставиться до АБС. За оцінками західних спеціалістів, навіть великий і стабільний банк збанкрутує, якщо він відкриє всю свою документацію. Тому АБС має бути захищена як всередині від можливих зловживань співробітниками банку так і зовні від різного роду спроб розкриття банківської таємниці та махінацій з його коштами.

У зв'язку з переходом на міжнародні стандарти бухгалтерського обліку інформаційні банківські системи практично розробляються заново на принципово нових засадах. Змінюється не тільки склад задач, а й відбувається перехід до нових програмно-апаратних засобів.

Отже, банківська справа на сучасному етапі – це галузь, яка є передовою з точки зору впровадження сучасних інформаційних технологій для забезпечення автоматизації електронних розрахунків.

1.2. Криміналістична класифікація інформаційних загроз безпеки автоматизованих банківських систем

Класифікації загроз інформації в автоматизованих системах приділялась значна увага у роботах провідних фахівців[1]. У науковій літературі запропоновані різні визначення загроз в залежності від їх специфіки, середовища прояву, результатів їх впливу, нанесеного збитку тощо. Під загрозами будемо розуміти цілеспрямовані та випадкові дії, що підвищують уразливість зберігання, обробки та передачі інформації в автоматизованій банківській системі.

Впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам обробки інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують достатній захист інформації.

[1] Безпека комп'ютерних систем: злочинність у сфері комп'ютерної інформації та її попередження / Вертузаєв М.С., Голубєв В.О., Котляревський О.І., Юрченко О.М. / Під ред. О.П. Снігерьова. – Запоріжжя, 1998. – 315 с.; Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів / Під ред. О.П. Снігерьова. – Запоріжжя, 1998. – 144 с.; Мельников В.В. Забита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 364 с.; 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.

Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

Прогрес у різних галузях науки і техніки, призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна підключатись до ліній телекомунікацій та різноманітних технічних засобів обробки інформації вітчизняного та іноземного виробництва з метою отримання, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіо-теплової, акустичної розвідок[1].

В сучасних умовах насиченості життя різними технічними засобами діяльності, засобами зв'язку, різного роду допоміжними системами вкрай необхідно усвідомити небезпеку виникнення каналів витоку інформації саме через технічні засоби обробки інформації конфіденційного характеру. Більш того, технічні засоби відносяться до найбільш небезпечних і широко розповсюджених каналів витоку інформації.

Усі потенційні загрози несанкціонованого доступу до інформації інформаційних систем розподіляються на цілеспрямовані та випадкові.

Потенційні загрози і канали несанкціонованого доступу до інформації в ПЕОМ залежать, насамперед, від умов її експлуатації – чи використовується ПЕОМ одним користувачем, чи групою. В першому випадку необхідний захист тільки від стороннього користувача, в другому – від будь-якого з користувачів, які працюють на одній ПЕОМ.

Коли на ПЕОМ працює один користувач і відсутні засоби захисту, потенційними каналами несанкціонованого доступу можуть бути:

– термінал, кінцеві модулі, пристрої користувача (клавіатура і засоби відбиття інформації);

– засоби документування інформації;

– засоби завантаження ПЗ;

– носії інформації (машинні, паперові);

– внутрішній монтаж ПЕОМ;

– побічне електромагнітне випромінювання і наводки (ПЕМВН);

– відходи в корзині сміття та інше.

Через доступ до клавіатура ПЕОМ, порушник технічного захисту інформації (ТЗІ) може зняти необліковану копію, ввести несанкціоновану інформацію, викрасти або модифікувати її програмне забезпечення, а також занести комп'ютерний вірус.

[1] Концепція технічного захисту інформації в Україні, затверджена постановою КМУ від 08.10.97 № 1126. – Розділ 2 // Збірка нормативних документів системи технічного захисту інформації. – 1997. – № 4. – С. 3-13.

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

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

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

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

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

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

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

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

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

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

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

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

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

СПИСОК ВИКОРИСТАНИХ 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. – 216 с.
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. – 208с.
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.

Маючи доступ до інформації на екрані дисплея і на роздруківках принтера, порушник ТЗІ може ознайомитись з оброблюваною інформацією. Маючи засоби завантаження (клавіатуру, дискети, CD-ROM) порушник ТЗІ може модифікувати програмне забезпечення і занести комп’ютерний вірус. Несанкціонований доступ до носіїв інформації може призвести до підміни, викрадення, копіювання програм та інформації, що також може призвести до витоку або порушення цілісності інформації ПЕОМ. На машинних носіях, які здаються в ремонт або передаються для інших цілей, може бути зчитана залишкова інформація, навіть якщо вона була стерта. НСД до внутрішнього монтажу може призвести до підміни вузлів і елементів монтажу, введенню складної несправності або встановленню стороннього пристрою у вигляді розвідувальної закладки, наприклад, передавача інформації по радіоканалам, приймача по каналам ПЕМВН, які несуть інформацію, можуть прийматися і декодуватися на спеціальних високочутливих приймачах на відстанях до 1-3 км від ПЕОМ[1].

Під час експлуатації ПЕОМ кількома користувачами загрозливою є ситуація, коли порушником ТЗІ є санкціонований користувач інформаційної системи (ІС), який за своїми функціональними обов’язками має санкціонований доступ до засобів завантаження, вводу-виводу інформації, до однієї частки інформації, а користуєтеся іншою за межами своїх повноважень і визначити факт НСД і дійсного порушника ТЗІ буде дуже важко, особливо у випадках порушення цілісності, модифікації та витоку інформації, а також навмисного занесення комп’ютерного вірусу, активна деструктивна робота якого, як правило, починається з затримкою в часі, термін якого не відомий.

З боку санкціонованого користувача багато способів порушити роботу ІС та одержати, модифікувати, поширити або знищити інформацію. З цією метою можуть бути використані, насамперед, привілейовані команди вводу-виведення, відсутність контролю санкціонованості або законності запиту та звернень до адресів пам’яті ОЗУ, баз і банків даних, серверів тощо. При неоднозначній ідентифікації захищуваних ресурсів ІС порушник ТЗІ може подавити системну бібліотеку своєю бібліотекою, а модуль, що завантажується з його бібліотеки, може бути введений в супервізорному режимі. Вільний доступ дозволить йому звертатись до чужих файлів і баз даних та змінювати їх випадково або навмисно.

При технічному обслуговуванні апаратури (це досить загрозливий момент несанкціонованого витоку інформації) можуть бути виявлені залишки інформації на її носіях (поверхні жорстких дисків, магнітні стрічки та інші носії). Стирання інформації звичайними методами (ресурсами операційних систем, спеціальних програмних утиліт) при цьому неефективне з точки зору ТЗІ, її залишки до 40-60% можуть бути порушником ТЗІ поновлені і прочитані, саме тому потрібні тільки спеціальні засоби стирання інформації.

[1] Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л. Основи захисту інформації від несанкціонованого доступу: Методичні рекомендації. – К.: НАВСУ, 1999. – 60 с.

При транспортуванні носіїв по неохоронюваній території існує загроза їх перехоплення і подальшого ознайомлення сторонніх осіб із захищуваною інформацією ІС.

Порушник ТЗІ може стати санкціонованим користувачем ІС в режимі розподілу часу, якщо він попередньо якось визначив порядок роботи санкціонованого користувача або якщо він працює за ним на одних і тих самих лініях зв'язку. Він може також використовувати метод проб і помилок та реалізовувати «дірки», «шлюзи» в операційній системі або прочитавши паролі. Без знання паролів він може здійснити «селективне» включення в лінію зв'язку між терміналом і процесором ЕОМ, крім того, без перерви роботи санкціонованого користувача може продовжити її від його імені, анулювавши сигнали відключення санкціонованого користувача[1].

При відсутності законного користувача, контролю та розмежування доступу до терміналу кваліфікований порушник легко використовує його функціональні можливості для НСД до інформації ІС шляхом введення відповідних запитів або команд.

При наявності вільного доступу у приміщення можна візуально спостерігати інформацію на засобах відображення і документування, а на останніх викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією: лістинги, магнітні носії тощо.

Особливу небезпеку являє безконтрольне завантаження програмного забезпечення в ІС, в якому можуть бути змінені установки, властивості, дані, алгоритми, введено «троянську» програму або занесено комп'ютерний вірус, що виконують деструктивні несанкціоновані дії. Наприклад, запис інформації на сторонній носій, незаконне передавання у канали зв'язку, несанкціоноване друкування документів, порушення цілісності документів, несанкціоноване копіювання важливої інформації, вагомість яких визначається та обмежується на дуже короткий або, навпаки, на тривалий час і тощо[2].

Перераховані потенційні канали НСД (ПКНСД) мають місце незалежно від присутності або відсутності санкціонованого користувача. Порушник ТЗІ буде використовувати найбільш зручний для нього у даний момент часу ПКНСД.

Процеси обробки, передачі та зберігання інформації апаратними засобами ІС забезпечуються спрацюванням логічних елементів на основі напівпровідникових приладів. Спрацювання логічних елементів обумовлено високочастотним зміщенням рівнів напруг і токів, що призводить до виникнення в ефірі, ланках живлення і заземлення, а також в паралельно розміщених ланках та індуктивностях сторонньої апаратури електромагнітних полів і наводок, які несуть в амплітуді, фазі і частоті своїх коливань ознаки оброблюваної інформації.

[1] Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л. Основи захисту інформації від несанкціонованого доступу: Методичні рекомендації. – К.: НАВСУ, 1999. – С. 13.

[2] 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. – С. 21-22.

безпідставна відмова від поширення певної інформації; поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи; використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків; розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю; порушення порядку зберігання інформації; навмисне знищення інформації; необґрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом.

власністю визначаються договором, укладеним між співвласниками.

Інформація, створена організаціями (юридичними особами) або придбана ними іншим законним способом, є власністю цих організацій.

Інформація, створена на кошти державного бюджету, є державною власністю. Інформацію, створену на правах індивідуальної власності, може бути віднесено до державної власності у випадках передачі її на зберігання у відповідні банки даних, фонди або архіви на договірній основі.

Власник інформації має право призначати особу, яка здійснює володіння, використання і розпорядження інформацією, і визначати правила обробки інформації та доступ до неї, а також встановлювати інші умови щодо інформації.

Розділ V
ОХОРОНА ІНФОРМАЦІЇ. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ

Стаття 45. Охорона права на інформацію

Право на інформацію охороняється законом. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації.

Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт права на інформацію може вимагати усунення будь-яких порушень його права.

Забороняється вилучення друкованих видань, експонатів, інформаційних банків, документів із архівних, бібліотечних, музейних фондів та знищення їх з ідеологічних чи політичних міркувань.

Стаття 46. Неприпустимість зловживання правом на інформацію

Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини.

Не підлягають розголошенню відомості, що становлять державну або іншу передбачену законодавством таємницю.

Не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом.

Стаття 47. Відповідальність за порушення законодавства про інформацію

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень, як: необґрунтована відмова від надання відповідної інформації; надання інформації, що не відповідає дійсності; несвоєчасне надання інформації; навмисне приховування інформації; примушення до поширення або перешкоджання поширенню чи

Використання порушником ТЗІ різних приймачів і особливо, аналізаторів спектру може призвести до несанкціонованого витоку та перехоплення дуже важливої оперативної інформації ІС. Зі зменшенням відстані між приймачем порушника ТЗІ та апаратними засобами ІС імовірність приймання інформаційних сигналів такого роду збільшується.

Несанкціоноване підключення порушником ТЗІ приймальної апаратури та спеціальних датчиків до ланцюгів електроживлення і заземлення, інженерних комунікацій та до каналів зв'язку також дозволяє несанкціоноване одержання інформації, а несанкціоноване під'єднання до каналів зв'язку в трактах передачі даних може призвести до модифікації та порушенню цілісності інформації в обчислювальних мережах[1].

Тому на підставі вищевикладеного можна виділити ще одну класифікацію каналів витоку інформації – за фізичною природою:

– радіоканали (електромагнітні випромінювання в радіодіапазоні);

– акустичні (поширення звукових коливань у будь-якому звукопровідному матеріалі);

– електричні (напруги і струми в різних струмопровідних комунікаціях);

– візуально-оптичні (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій ділянці спектра);

– матеріально-речові (папір, фото, магнітні носії, відходи тощо) (Рис. 1.2.1).

Фізичні процеси, що відбуваються в технічних засобах при їх функціонуванні, створюють у навколишньому просторі побічні випромінювання, що у тій чи іншій мірі пов'язані з оброблюваною інформацією.

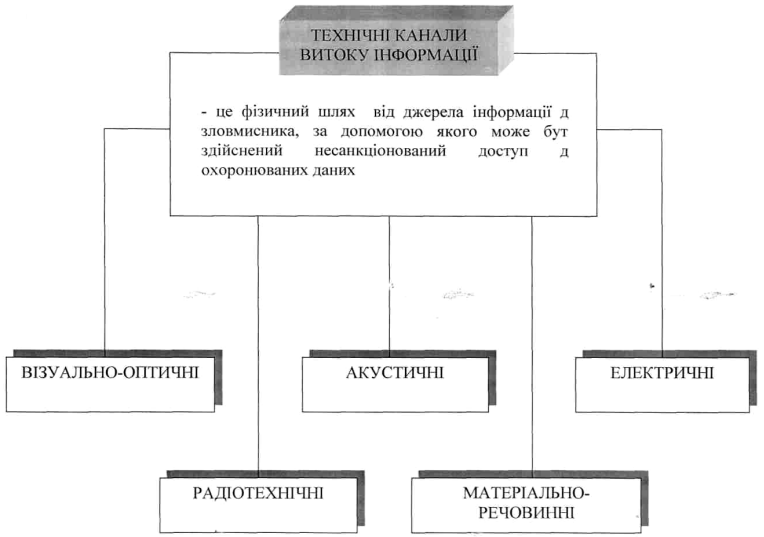

Рис. 1.2.1. Технічні канали витоку інформації.

[1] Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л. Основи захисту інформації від несанкціонованого доступу: Методичні рекомендації. – К.: НАВСУ, 1999. – С. 13.

Правомірно припускати, що утворенню технічних каналів витоку інформації сприяють певні обставини і причини технічного характеру (рис. 1.2.2.).

У сучасних умовах вкрай необхідно розуміти небезпеку виникнення каналів витоку саме через технічні засоби обробки інформації.

Аналіз фізичної природи багатьох перетворювачів і випромінювачів показує, що:

– джерелами небезпечного сигналу, є елементи, вузли і провідники технічних засобів, а також радіо- і електронна апаратура;

– кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;

– кожна електронна система, що містить у собі сукупність елементів, вузлів і провідників, має певну множину джерел небезпечного сигналу і технічних каналів витоку інформації.

Джерелом утворення акустичного каналу витоку інформації є вібруючі тіла чи механізми, такі як голосові зв'язки людини, рухомі елементи машин, телефонні апарати, звукопосилюючі системи, гучномовні засоби зв'язку, засоби звукозапису і звуковідтворення і навіть ПЕОМ, що працює в режимі вводу, виводу й обробки звукової інформації[1].

Електричні канали витоку інформації це ланцюги живлення і заземлення.

Візуально-оптичні канали утворюються як оптичний шлях від об'єкта конфіденційних устремлінь до зловмисника. Для утворення візуально-оптичних каналів необхідні певні просторові, енергетичні і тимчасові умови і відповідні засоби на стороні зловмисника.

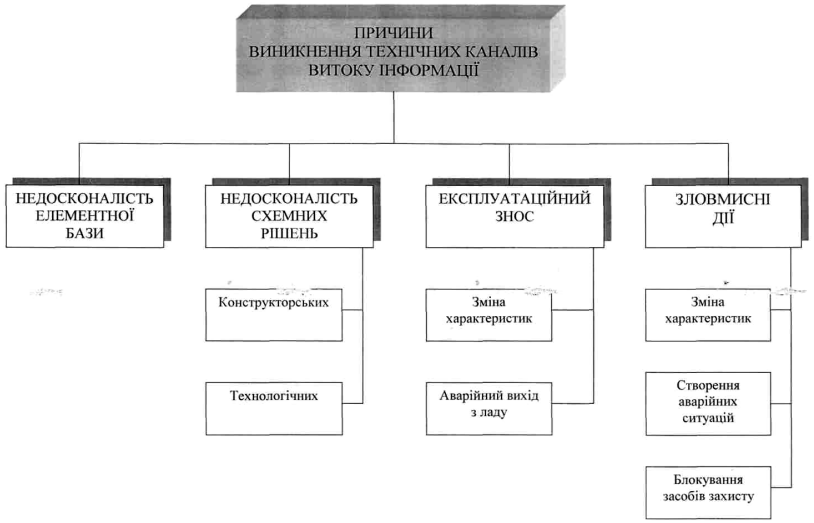

Рис. 1.2.2. Причини витоку інформації.

[1] Методы и средства защиты информации: Методические указания. – К: КМУГА, 1997. – С. 15-16.

законом.

Переважним правом на одержання інформації користуються громадяни, яким ця інформація необхідна для виконання своїх професійних обов'язків.

Стаття 30. Інформація з обмеженим доступом

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну.

Конфіденціальна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденціальної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Стаття 38. Право власності на інформацію

Право власності на інформацію – це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією.

Інформація є об'єктом права власності громадян, організацій (юридичних осіб) і держави. Інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження.

Власник інформації щодо об'єктів своєї власності має право здійснювати будь-які законні дії.

Підставами виникнення права власності на інформацію є: створення інформації своїми силами і за свій рахунок; договір на створення інформації; договір, що містить умови переходу права власності на інформацію до іншої особи.

Інформація, створена кількома громадянами або юридичними особами, є колективною власністю її творців. Порядок і правила користування такою

оголошуваної інформації громадянами, юридичними особами або державою.

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави.

Поширення інформації – це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації.

Зберігання інформації – це забезпечення належного стану інформації та її матеріальних носіїв.

Одержання, використання, поширення та зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації.

Розділ III
ГАЛУЗІ, ВИДИ, ДЖЕРЕЛА ІНФОРМАЦІЇ ТА РЕЖИМ ДОСТУПУ ДО НЕЇ

Стаття 28. Режим доступу до інформації

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Держава здійснює контроль за режимом доступу до інформації.

Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необгрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України.

У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність по забезпеченню інформацією заінтересованих осіб (кількість випадків відмови у наданні доступу до інформації із зазначенням мотивів таких відмов; кількість та обгрунтування застосування режиму обмеженого доступу до окремих видів інформації; кількість скарг на неправомірні дії посадових осіб, які відмовили у доступі до інформації, та вжиті щодо них заходи тощо).

Стаття 29. Доступ до відкритої інформації

Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової комунікації; безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Порядок і умови надання громадянам, державним органам, юридичним особам і представникам громадськості відомостей за запитами встановлюються цим Законом або договорами (угодами), якщо надання інформації здійснюється на договірній основі.

Обмеження права на одержання відкритої інформації забороняється

Візуально-оптичне спостереження є найбільш відомим, досить простим, широко розповсюдженим і добре оснащеним сучасними технічними засобами розвідки. Цей вид дій має:

– вірогідність і точність інформації, що добувається; високою оперативністю одержання інформації; доступністю реалізації;

– документальністю отриманих відомостей (фото, кіно, телебачення).

Ці особливості визначають небезпеку даного каналу витоку інформації.

У практиці промислової розвідки широко використовується одержання інформації з відходів діяльності. В залежності від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти документів, що складаються, чернетки листів, магнітні носії, копірки тощо[1].

Ми розглянули цілеспрямовані потенційні загрози. Розглянемо тепер випадкові потенційні загрози.

Випадкові загрози інформації ІС мають ряд особливостей. Дослідження досвіду проектування, виробництва, випробувань і експлуатації ІС свідчить про те, що інформація в процесі введення, зберігання, обробки, виведення і передачі піддається різним випадковим впливам на апаратному та програмному рівнях.

На апаратному рівні відбуваються фізичні зміни рівнів сигналів в цифрових кодах, що несуть інформацію. При цьому в одному або двох, трьох розрядах відбуваються зміни 1 на 0, або те і інше разом, але в різних розрядах, наслідком чого є зміна значення коду на інше. Далі, якщо засоби функціонального контролю здатні виявити ці зміни (наприклад, контроль по модулю 2 легко виявляє одноразову помилку), проводиться обрахування даного коду, а пристрій, блок, модуль або мікросхема, які беруть участь в обробці, об’являються несправними. Якщо функціональний контроль відсутній або не здатний виявити несправність на даному етапі обробки, процес обробки продовжується хибним шляхом, тобто відбувається несанкціонована, випадкова модифікація інформації. В процесі подальшої обробки в залежності від змісту та призначення хибної команди можливі або пересилання інформації на хибну адресу, або передача хибної інформації адресату , або стирання чи запис іншої інформації в ОЗУ або на ЖМД, тобто виникають несанкціоновані події: порушення, втрата, модифікація та витік інформації.

На програмному рівні в результаті випадкових впливів може бути зміна алгоритму обробки інформації на непередбачений термін: в кращому разі – зупинка обчислювального процесу, а в гіршому – його несанкціонована модифікація. Якщо засоби функціонального контролю цього не виявляють, наслідки такої модифікації алгоритму або даних можуть пройти непоміченими або призвести також до несанкціонованого випадкового порушення інформації, а при переплутуванні адреси пристрою – до несанкціонованого витоку інформації.

---

[1] Методы и средства защиты информации: Методические указания. – К: КМУГА, 1997. – С. 25.

При програмних помилках можуть також підключатись програми вводу-виводу та передачі їх на несанкціоновані пристрої.

Потенційними загрозами випадкових несанкціонованих впливів на інформацію при експлуатації ІС можуть бути:

– відмови і збої апаратури;
– перешкоди на лініях зв'язку від впливів зовнішнього середовища;
– помилки людини як частини системи;
– схемні і системотехнічні помилки розробників;
– структурні, алгоритмічні і програмні помилки;
– аварійні ситуації;
– програмно-математичні деструктивні закладки та інші впливи.

Частота випадків і збоїв апаратури залежить від її експлуатаційної надійності. Перешкоди на лініях зв'язку залежать від вірного вибору місця розміщення технічних засобів ІС відносно один одного та по відношенню до апаратури і агрегатів сусідніх систем.

При розробці складних інформаційних систем збільшується кількість схемних, телекомунікаційних, системотехнічних, структурних, алгоритмічних і програмних помилок. На їх кількість великий вплив має кваліфікація розробників, умови їх праці, наявність досвіду, повнота і якість експлуатаційної документації.

До помилок людини як частини ІС необхідно віднести помилки людини-оператора, адміністратора-програміста, невірні дії обслуговуючого персоналу. Помилки людини поділяються на логічні (невірно прийняті рішення), сенсорні (невірно сприйнята оператором інформація) та оперативні або моторні (невірна реалізація рішення). Інтенсивність помилок людини може коливатись в досить широких межах: від 1-2% до 15-40% і вище відносно загальної кількості операцій, що виконуються при вирішенні прикладної програми. Для оцінки вірогідності інформації необхідні статистичні дані по рівню помилок персоналу як частини ІС. При цьому імовірність помилок залежить від загальної кількості кнопок в ряду, кнопок, які треба натиснути одночасно, відстані між краями кнопок і т. ін.

Концептуально помилки людини як ланцюга, що приймає рішення, визначаються неповною адекватністю представлення ним реальної ситуації та властивістю людини діяти по визначеній установці і по раніше визначеній програмі. Наприклад, деякі керівники виявили , що такі ситуації були завжди, саме тому зменшують фінансування та інші ресурси ІС і тим самим сприяють помилковим рішенням. Другою важливою особливістю людини є прагнення до побудови спрощеної моделі оцінюваної ситуації загроз НСД, саме тому виключення з неї суттєво важливих ситуацій призводить до подальших помилок в наборі обов'язкових функцій захисту від спрощених загроз НСД.

Аварійні ситуації – це випадкові впливи на інформацію за рахунок відмови функціонування інформаційної системи з причин збоїв мереж електроживлення, життєзабезпечення та інших випадкових подій, наприклад, стихійні лиха.

Таким чином, розглянуті нами потенційні цілеспрямовані (навмисні) та випадкові загрози є двома основними класами прояву можливих загроз

Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Стаття 10. Гарантії права на інформацію

Право на інформацію забезпечується: обов'язком органів державної влади, а також органів місцевого і регіонального самоврядування інформувати про свою діяльність та прийняті рішення; створенням у державних органах спеціальних інформаційних служб або систем, що забезпечували б у встановленому порядку доступ до інформації; вільним доступом суб'єктів інформаційних відносин до статистичних даних, архівних, бібліотечних і музейних фондів; обмеження цього доступу зумовлюються лише специфікою цінностей та особливими умовами їх схоронності, що визначаються законодавством; створенням механізму здійснення права на інформацію; здійсненням державного контролю за додержанням законодавства про інформацію; встановленням відповідальності за порушення законодавства про інформацію.

Розділ II
ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ

Стаття 12. Визначення інформаційної діяльності

Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

З метою задоволення цих потреб органи державної влади та органи місцевого і регіонального самоврядування створюють інформаційні служби, системи, мережі, бази і банки даних.

Порядок їх створення, структура, права та обов'язки визначаються Кабінетом Міністрів України або іншими органами державної влади, а також органами місцевого і регіонального самоврядування.

Стаття 13. Основні напрями інформаційної діяльності

Основними напрямами інформаційної діяльності є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо.

Держава зобов'язана постійно дбати про своєчасне створення, належне функціонування і розвиток інформаційних систем, мереж, банків і баз даних у всіх напрямах інформаційної діяльності.

Держава гарантує свободу інформаційної діяльності в цих напрямах всім громадянам та юридичним особам в межах їх прав і свобод, функцій і повноважень.

Стаття 14. Основні види інформаційної діяльності

Основними видами інформаційної діяльності є одержання, використання, поширення та зберігання інформації.

Одержання інформації – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно

РОЗДІЛ 3
ПРАВОВЕ РЕГУЛЮВАННЯ ОБІГУ ІНФОРМАЦІЇ В СУСПІЛЬСТВІ: УСТАНОВАХ, ОРГАНІЗАЦІЯХ, ВІДОМСТВАХ

3.1. Закон України „Про інформацію” (витяг).

Розділ I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення інформації

Під інформацією цей Закон розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Стаття 2. Мета і завдання Закону

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

Стаття 3. Сфера дії Закону

Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Стаття 5. Основні принципи інформаційних відносин

Основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об’єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації.

Стаття 7. Суб’єкти інформаційних відносин

Суб’єктами інформаційних відносин є: громадяни України; юридичні особи; держава.

Суб’єктами інформаційних відносин відповідно до цього Закону можуть бути також інші держави, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства.

Стаття 8. Об’єкти інформаційних відносин

Об’єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров’я, а також у соціальній, екологічній, міжнародній та інших сферах.

Стаття 9. Право на інформацію

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

несанкціонованого доступу до інформації ІС[1].

Як висновок, необхідно зазначити, що специфіка банківських автоматизованих систем, з точки зору їх уразливості, пов’язана в основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнорідними елементами. Уразливими є буквально всі основні структурно-функціональні елементи розподілених АБС: робочі станції, сервери, міжмережеві мости, канали зв’язку.

1.3. Методи і засоби міжнародної протидії злочинам, вчинених з використанням інформаційних технологій[2]

Інформація взагалі та знання зокрема є вирішальними факторами, які впливають на розвиток технології і технологічних ресурсів людства. Власне вони визначають кордони технологій та можливості в освоєнні природи і подальшого розвитку суспільства. Саме ключові революційні винаходи у галузі інформатики відкривали нові можливості та надавали поштовху до розвитку великих технологічних революцій. Комп’ютерні системи збільшили загальний обсяг інформації з яким може працювати людство, на 7-8 порядків і довели його до 10 біт.

Інформація, яка використовуєтеся в житті нашого суспільства, містить широкий спектр відомостей: від звичайних облікових даних про громадян в автоматизованих комп’ютерних системах до стратегічних державних програм. Ці відомості, особливо в умовах розширення інформатизації нашого суспільства, все більш стають предметом злочинних посягань.

Використання сучасних інформаційних технологій на основі персональних комп’ютерів, інформаційно-обчислювальних мереж і комп’ютеризованих мереж забезпечило кожній людині можливості доступу до інформації, що зберігається у відповідних банках даних, встановлення зв’язку незалежно від годин доби і від адміністративних і державних кордонів місцезнаходження абонента. Поряд з перевагами комп’ютеризація має ряд негативних наслідків. Можна стверджувати, що одним із негативних соціальних та економічних наслідків науково-технічного прогресу є поява комп’ютерної злочинності.

Комп’ютерна злочинність – це новий феномен, породжений можливостями майже безкарного вчинення протиправних дій у сфері, наглухо зачиненій для людини, яка не володіє основами комп’ютерної грамотності.

---

[1] Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л. Основи захисту інформації від несанкціонованого доступу: Методичні рекомендації. – К.: НАВСУ, 1999. – С. 16-17.

[2] За матеріалами НЦБ Інтерполу в Україні.

Термін «комп'ютерна злочинність» вперше з'явився в американській, а потім і в іншій зарубіжній пресі на початку 60-х років, коли були виявлені перші випадки злочинів, вчинених з використанням ЕОМ. Це явище посилюється не тільки в локальному, національному, а й в глобальному масштабі. На думку українських кримінологів, уже зараз ЕОМ є багатообіцяючим знаряддям вчинення корисливих злочинів[1].

Як підкреслюють вчені-криміналісти П.Д. Біленчук, М.А. Зубань та В.О. Голубєв, сьогодні у вітчизняній криміналістичній науці все ще не існує чіткого визначення поняття комп'ютерного злочину, дискутуються різні точки зору з їх класифікації. Складність в формулюваннях цих понять існує, як в наслідок неможливості виділення єдиного об'єкта злочинного посягання, так, і множинністю предметів злочинного посягання з точки зору їх кримінально-правового значення[2].

Більшість фахівців поділило комп'ютерні злочини на два типи:

1. Злочини, в яких об'єктом їх здійснення є ЕОМ:

– знешкодження або заміна даних, програмного забезпечення та обладнання;

– розкрадання вхідних, вихідних даних, програмного забезпечення та обладнання;

– економічне шпигунство та розголошення відомостей, які складають державну чи комерційну таємницю;

– інші злочинні діяння цього виду.

2. Протизаконні акції, для здійснення яких ЕОМ використовується як знаряддя в досягненні злочинної мети:

– комп'ютерний саботаж;

– вимагання та шантаж;

– розтрата;

– розкрадання коштів;

– обман споживачів, інвесторів чи користувачів;

– інші злочини.

До категорії «інші злочинні діяння» віднесено несанкціоноване використання комп'ютеру в особистих цілях.

На наш погляд, під *комп'ютерною злочинністю слід розуміти суспільно-небезпечну діяльність 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 формуванням і громадянам, а також правам особи*.

[1] Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України. – 1998. – № 1. – с. 101.

[2] Голубєв В.О. Комп'ютерні злочини в банківській діяльності. – Запоріжжя: ВЦ «Павел», 1997. – с. 19.

ґрунтується на закономірностях функціонування конкретної файлової системи, програм і вимагає подальшого вивчення файлових систем FAT 16 (операційні системи DOS, Windows), FAT 32 (операційні системи WINDOWS 95 і вище), NTFS (операційна система WINDOWS NT), а також стосовно до системних і прикладних програм, що з'явилися;

– документи на машинних магнітних носіях інформації є новим криміналістичним об'єктом, що має особливі специфічні властивості, і не дозволяють застосовувати до даних об'єктів наявні сьогодні в криміналістичній літературі поняття та визначення сліду й розроблені класифікації слідів;

– розроблені класифікації слідів-відображень і виявлені особливості цих слідів можуть бути покладені в основу розробки криміналістичної характеристики і базову модель при формуванні особливостей методики розслідування злочинів, вчинених у банківській системі з використанням сучасних інформаційних технологій, експертного дослідження електронних пластикових документів та іншої інформації, яка зберігається на електронних магнітних носіях.

ВИСНОВКИ, ПРОПОЗИЦІЇ, РЕКОМЕНДАЦІЇ

На підставі вищевикладеного можна зробити такі висновки:

Криміналістична характеристика незаконного втручання в роботу ЕОМ банківської установи, відрізняється специфікою, особливостями й містить у собі: дані про предмет злочинного посягання, відомості про способи підготовки, вчинення й приховання злочину; дані про обстановку вчинення злочину, дані про особу злочинця, а так само відомості про «слідову картину». Вище проаналізовані елементи криміналістичної характеристики дозволяють запропонувати такі новації, пропозиції і рекомендації.

1. Способи вчинення незаконного втручання в роботу ЕОМ банку доцільно поділяти на дві групи: 1) способи безпосереднього доступу до ЕОМ; 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 слідчої діяльності по кожному з них.

2. Інформацію латентного характеру можна одержати, вивчаючи типові способи протидії розслідуванню по розглянутій категорії справ. Основне інформаційне навантаження несе спосіб приховання слідів злочину. Приховування слідів злочину, пов'язаних з незаконним втручанням у роботу ЕОМ банківської установи, може виражатися в знищенні, утаюванні, маскуванні, фальсифікації, як традиційно досліджуваними криміналістикою способами (маскування зовнішності, дача неправдивих свідчень тощо), так і специфічними способами, пов'язаними з комп'ютерним обладнанням, програмним забезпеченням 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 (свідків, обвинувачених, потерпілих) або ухиленні від участі в розслідуванні.

3. Незаконне втручання в роботу ЕОМ банківської установи сьогодні в п'ять разів частіше вчинюється чоловіками, але прогностичні дані свідчать, що в майбутньому жінки зможуть їх потіснити. Більшість суб'єктів 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.

4. Узагальнення і систематизація даних, які проведені при розробці класифікацій слідів-відображень, пов'язаних з інформаційними взаємодіями, і розгляд специфічних особливостей цих слідів дозволяє зробити такі висновки:

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

– механізм утворення слідів, пов'язаних з інформаційними взаємодіями,

Розповсюдження загальних комп'ютерних знань, постійне підвищення технічних характеристик та супутнє зниження цін на обладнання, застосування комп'ютерів мабуть чи не в усіх професіях, розвиток машинних мов високого рівня, які легко засвоюються будь-якою зацікавленою особою, і як наслідок постійне зростання кількості користувачів, зумовило зростання масштабів протизаконних дій пов'язаних з використанням ЕОМ. Збільшення кількості кримінальних справ, пов'язаних з комп'ютерними злочинами, спостерігається практично у всіх промислово розвинутих країнах.

У 1988 році тільки в Європі було здійснено чотири невдалі спроби нелегального пересилання грошей з банківських рахунків (втрати в кожному випадку становили більше 50 млн. доларів США). Характерно те, що всі ці спроби виявились невдалими тільки завдяки «безмірній жадібності» злочинців. В Чикаго, наприклад, 7 злочинців вирішили викрасти 70 млн. доларів і були затримані в той момент, коли мали на своєму рахунку більш ніж 49 млн. доларів.[1]

Як вважають американські спеціалісти, пряма економічна шкода від комп'ютерних злочинів уже сьогодні стоїть на одному рівні з перевагами, отриманими від впровадження ЕОМ у практику, а соціальні і моральні втрати взагалі не піддаються оцінці. Певною мірою така оцінка гіперболічна, але факти говорять самі за себе: досить сказати, що тільки у США економічні втрати від комп'ютерної злочинності у 90-х роках наблизились до 100 млрд. доларів. При цьому, необхідно мати на увазі, що цей вид злочинності має високу латентність: лише 10-15 відсотків комп'ютерних злочинів стають відомими, оскільки організації, що потерпіли внаслідок подібних злочинів, неохоче надають інформацію, оскільки це може зашкодити їх репутації або спричинити повторні злочини[2].

Аналіз результатів різних кримінологічних досліджень розвитку комп'ютерної злочинності в Німеччині в період з 1987 до 1993 років приводить до висновків про помітне зростання загальної кількості зареєстрованих злочинів цієї категорії, а також про значну перевагу в їх структурі випадків шахрайства і маніпуляцій з інформаційною технікою в порівнянні з іншими видами комп'ютерних злочинів.

З урахуванням латентної злочинності загальні матеріальні збитки, які завдаються щорічно в результаті економічних комп'ютерних злочинів, оцінюються німецькими фахівцями в 70 млрд. марок[3].

У період 1990-1994 років поліцією Норвегії було зареєстровано 55 випадків протиправного доступу в комп'ютерні мережі та 86 злочинів комп'ютерного шахрайства, причому з кожним роком їх кількість зростає. Загальні збитки від комп'ютерних злочинів у період 1989-1992 років зросли від 270 мільйонів крон до 480 мільйонів крон.

---

[1] Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – с. 31.

[2] Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України. – 1998. – № 1. – С. 101.

[3] Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – 105 с.

У Франції, починаючи з 1990 року злочини цієї категорії зазнають регулярного підйому, наприклад, 33 – у 1991 році, 40 – у 1992 році, 58 – у 1993 році. Тенденція до зростання кількості злочинів такого типу зберігається і надалі, особливо з появою комп'ютерних мереж та відсутністю належного захисту пам'яті (інформації у запам'ятовуючих пристроях) з боку виробників та користувачів. Кількість подібних злочинів збільшується на 30-40% щорічно. Втрати від комп'ютерних злочинів досягають 1 млрд. франків на рік[1].

Виникнення комп'ютерної злочинності та масштаби збитків викликали необхідність розробки законодавчих норм, що встановлюють відповідальність за вказані злочини.

Перші спеціальні закони по боротьбі з комп'ютерною злочинністю були прийняті в 1973 році в Швеції і в 1976 році в США на федеральному рівні. Склади злочинів у сфері інформаційних технологій (комп'ютерних злочинів) були сформовані в 1979 році на Конференції американської асоціації адвокатів у Далласі, до яких увійшли: використання або спроба використання комп'ютера, обчислювальної системи або мереж комп'ютерів з метою отримання грошей, власності або послуг шляхом прикриття фальшивими кодами або видання себе за іншу особу; умисна несанкціонована дія, що має за мету зміну, пошкодження, знищення або викрадення комп'ютера, обчислювальної системи, комп'ютерної мережі або систем математичного забезпечення, що містяться в них, програм або даних; умисне незаконне порушення зв'язку між комп'ютерами, обчислювальними системами або комп'ютерними мережами[2]. Згодом, поступово в багатьох країнах світу затверджено законодавчі акти стосовно цієї категорії злочинів.

В лютому 1986 року Бундестагом Німеччини було прийнято Другий Закон по боротьбі з економічною злочинністю. Завдяки цьому було закладено правову базу для ефективного кримінально-правового переслідування економічних правопорушень нового типу, перш за все злочинів, об'єктом або знаряддям яких є ЕОМ. Ряд нових статей, які введено цим законом, вміщують спеціально сформульовані склади комп'ютерних злочинів. Закон було введено в дію 1 серпня 1986 року.

Федеральний закон ФРН про охорону даних ставить за обов'язок установам і організаціям приймати необхідні технічні й організаційні заходи для забезпечення схоронності зазначених у законі даних. Чинність закону не поширюється на широко відомі чи передані усно відомості про ту чи іншу особу, а також дані, що зберігаються в спеціальних актах і справах, доступ до яких строго обмежений.

Не підлягають охороні дані, що збираються й обробляються з метою їх наступної публікації, показу чи розголосу засобами кіно, радіо і преси. Порядок поводження з інформацією в даній сфері регламентується спеціальними законами.

[1] Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – 111 с.

[2] Там само, с. 60.

Все це призводить до того, що небажання повідомити про злочин, свідоме приховування його, сприяє знищенню слідової картини, яка і так дуже слабка. Але якщо потерпіла сторона повідомляє правоохоронні органи про вчинений злочин, то слідчо-оперативна група, прибувши на місце події, знаходить сліди злочину, які виявляються при огляді місця події.

Зокрема всі комп'ютери банківських установ мають системи попередження несанкціонованого доступу, які фіксують всі спроби такого роду. Достатньо набрати відповідну команду, і комп'ютер виведе на дисплей всю інформацію. Але злочинець може проникнути в чужий комп'ютер шляхом пошуку слабких місць у захисті системи, в цьому випадку несанкціонованого доступу зафіксовано не буде. Та при всій своїй обережності в роботі з інформацією, все ж таки інколи залишаються сліди, це може бути якась ненароком стерта інформація, або плутанина в програмі, яка могла статись при застосуванні не тієї команди, яку потрібно було б застосувати. Якщо з банка були викрадені гроші, то при більш детальній перевірці виявиться завдана матеріальна шкода. Але в багатьох випадках її важко визначити.

Левова частка комп'ютерних злочинів в основному вчинюється працівниками установ, яким була завдана шкода, людьми, які досить добре знають режим роботи системи і можуть використати можливості цієї системи в корисливих цілях. А таких людей в кожній установі не так вже й багато, то ж сліди злочину можуть залишитись на їх робочих місцях. Це можуть бути дискети, магнітні диски, на яких злочинець зберігає потрібну інформацію, роздруківки, записи на аркушах паперу (шифри, паролі).

Та, нажаль майже всі злочини вчинюються вдень на роботі під час виконання електронними злодіями їх безпосередньої службової професійної діяльності, тому затримати їх на місці злочину практично неможливо, і з цим нічого не вдієш. Єдиний вихід, це вдосконалювати системи захисту, і намагатись, щоб якомога менше осіб знали режим роботи системи. Менше обізнаних – менше коло підозрюваних.

Виходячи з вищевикладеного, інформація про зазначену обстановку, як правило, є стрижневою у криміналістичній характеристиці практично будь-якого злочину, оскільки перетинається з даними про інші її елементи. Відзначена обстановка багато в чому визначає і коректує спосіб вчинення злочину і значною мірою позначається на особливостях і структурі його механізму. В ній виявляються окремі важливі особистісні риси злочинця, що формує (частково або цілком) дану обстановку, який у більшій або меншій мірі пристосовується до неї або використовує її без якогось пристосування, а іноді і без врахування її особливостей.

– які з вищевідзначених умов і чинників безпосередньо передували злочину, супроводжували його, які були їх взаємодія, зміст і характер впливу на вчинене діяння;

– що в обстановці досліджуваної події було геніально підготовлено злочинцем, а що не залежало від нього;

– як у цілому сформоване до й у момент вчинення діяння фактичне положення було використано в злочинних цілях, зокрема при виборі способу вчинення злочину;

– що в даній обстановці сприяло і перешкоджало готуванню, вчиненню і приховуванню слідів злочину і як це враховувалося злочинцем;

– які чинники незвичайної (нетипової) властивості проявилися в ситуації, що склалася, і який вплив вони зробили на подію злочину;

– хто міг створити або скористатися об'єктивно сформованою ситуацією для вчинення злочину[1].

Однією з найбільших складностей є встановлення факту вчинення комп'ютерного злочину. Пояснюється це тим, що зовні сам факт вчинення комп'ютерного злочину, та його прояв в оточуючому середовищі зазвичай набагато скромніший, аніж при пограбуванні продуктового магазину, або зовсім непомітний. Видимого матеріального збитку, здійсненного електронним злодієм зовні не видно. Наприклад, незаконне копіювання інформації частіш за все залишається невиявленим, введення в комп'ютер вірусу найчастіше списується на ненавмисну помилку користувача, який не зміг його «відновити» при спілкуванні із зовнішнім комп'ютерним світом.

Механізм вчинення злочинів, пов'язаних з автоматизованими системами обробки інформації, часто приховані від потерпілих. Крім того, факт витоку інформації може бути прихований за допомогою електронних засобів при нормальному ході подій до того, як це буде виявлено.

В розкритті факту вчинення злочину дуже часто не зацікавлені посадові особи, в обов'язки яких входить забезпечення комп'ютерної безпеки. Визнання факту несанкціонованого доступу в підвідомчу їм систему ставить під сумнів їх професійну кваліфікацію, а неспроможність заходів по комп'ютерній безпеці, що приймається керівництвом, може призвести до серйозних внутрішніх ускладнень.

Що стосується банків, які постраждали, то їх службовці зовсім не зацікавлені в реєстрації таких злочинів, а навпаки, ретельно це приховують. Адже надання гласності фактам вчинення злочинних дій проти комп'ютера банку негативно відіб'ється на авторитеті установи, може призвести до втрати клієнтів.

Більше того, якщо комп'ютерні злочини стають для даної організації регулярними, то страхові компанії збільшують для них розмір грошових внесків, або ж зовсім відмовляються від поновлення страхового полісу. Оскільки це не вигідно, то керівники організацій, в яких здійснюються комп'ютерні злочини, свідомо приховують їх.

[1] Криминалистика. Учебник для вузов / Ответственный редактор Н.П. Яблоков. – М, 1995. – с. 53.

Відповідно до закону про охорону даних, об'єктом охорони є дані, що зберігаються в картотеках і пам'яті ЕОМ, і які торкаються особистих інтересів громадян, та, будучи введеними в ЕОМ, легко можуть бути доступні третім особам[1].

В Італії законодавчими актами введені основні положення відносно найбільш важливих комп'ютерних злочинів:

1. Декрет № 518 від 29.12:32 року «Використання положень Європейського Економічного співтовариства за № 91/250 стосовно офіційного захисту комп'ютерних програм».

2. Закон № 547 від 23.12.93 «Зміна та внесення нових статей стосовно комп'ютерних злочинів в Кримінальний Кодекс».

Комп'ютерний злочин, згідно кримінального законодавства Італії – це злочин вчинений з використанням комп'ютерних технологій, як від персонального комп'ютеру так до портативних телефонних пристроїв, які створені на базі мікрочіпів.

Законодавство Італії забезпечує захист урядових організацій, військових об'єктів, банків, компаній, фірм від несанкціонованого доступу в комп'ютерні мережі, протиправного використання захищених банків даних, незаконного копіювання топографій напівпровідників (чіпів), які злочинці використовують для встановлення кодів кредитних і телефонних карток, банківських рахунків, тощо.

Щорічні втрати в Італії від комп'ютерних злочинів складають сотні мільйонів лір. Характерним для поведінки комп'ютерних злочинців є використання програмного забезпечення, яке може автоматично набирати всі алфавітно-цифрові комбінації на основі принципу генератора випадкових чисел. Завдяки цій процедурі вони здатні встановити пароль, що дозволить увійти до системи[2].

Франція має повний юридичний арсенал для боротьби з такою категорією злочинності. У 1994 році було сформовано Бригаду поліції з компетентного персоналу, яка спеціалізується у виявленні та розслідуванні комп'ютерних злочинів при тісному співробітництві із службами безпеки та цивільними організаціями.

З 1 березня 1994 року було введено в дію нову версію Кримінального Кодексу, який докорінно змінив внутрішні закони про комп'ютерну злочинність.

До Кримінального Кодексу були внесені статті з санкціями проти правопорушень, які пов'язані з обробкою інформації та із злочинами щодо фальсифікації даних.

[1] Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – с. 34.

[2] Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – с. 109.

Прийнятий 5 січня 1994 року Закон „Godfrran", який було названо на честь автора, вніс ясність та уточнив питання юриспруденції і практики відносно несанкціонованого доступу та протидії функціонуванню систем, які приносять щорічних збитків, наприклад, страховим компаніям в розмірі 5 мільярдів франків.

В Іспанії вислів «комп'ютерний злочин» має визначення:

1. Дії, які спрямовані на знищення або стирання програм чи їх складових частин, заміну, знищення накопиченої інформації, необгрунтоване використання ЕОМ.

2. Дії проти держави, національної безпеки, найближчого оточення, майна, тощо.

Єдиний закон, який передбачає покарання за комп'ютерні злочини – Кримінальний Кодекс Іспанії. Диспозиції статей Кодексу сформульовані у відповідності до норм Державного Закону № 5/92 від 2 жовтня 1992 року, який регулює процеси персональної автоматизованої обробки даних і передбачає утворення органу захисту даних для контролю за виконанням цих норм.

Перші законодавчі акти щодо комп'ютерної злочинності в Австралії були прийняті у 1979 році.

Сектор комп'ютерних злочинів (CCS) Австралійської федеральної поліції (АРР), який був організований в 1989 році, виконує дві функції. Перша – збір розвідувальної (оперативно-розшукової) інформації про спеціальні комп'ютерні злочини та їх розслідування. Друга – забезпечення технічної підтримки інших підрозділів щодо дослідження комп'ютерних засобів, які пов'язані із злочинами або допомагали в їх вчиненні.

Згідно чинного законодавства Австралії комп'ютерні злочини поділяються на три загальні види:

1. Специфічні комп'ютерні злочини.

2. Злочини пов'язані з комп'ютером.

3. Злочини, які вчинені за допомогою комп'ютерів.

Специфічні комп'ютерні злочини вміщують правопорушення в яких комп'ютерна система є об'єктом вчинення злочину. Прикладом цього виду злочинів може бути протизаконний доступ до комп'ютерної системи.

До злочинів, які пов'язані з комп'ютерами належать правопорушення, в яких комп'ютер виступає в ролі предмету або інструменту вчинення правопорушення. Одним з прикладів цієї категорії злочинів є крадіжка грошей з банку з використанням комп'ютеру, як інструменту вчинення злочину.

Третій вид злочинів – правопорушення в яких інформаційна технологія використовується як допоміжна у його вчиненні. Як приклад – використання синдикатами, які займаються розповсюдженням наркотиків, спеціальних комп'ютерів або комунікаційних засобів для безпечного зв'язку між собою.

Сьогодні Україна знаходиться перед проблемою подальшого розвитку сучасних біо- та інформаційних технологій, телекомунікаційних систем, інформатизації суспільства. Головним завданням інформатизації суспільства є створення правових, економічних, технологічних, соціальних та освітніх

Вони працюють як в самих організаціях, проти яких вчинюються діяння, так і поза ними, поодинці і в групі співучасників. Одні технічно оснащені слабо, а інші мають дорогі, престижні, науковомісткі потужні комп'ютерні системи.

На підставі викладених способів вчинення злочинів з використанням пластикових карток, класифікація суб'єктів цих злочинів може бути представлена в такому вигляді:

– персонал обслуговуючих сервісних пунктів;
– особи, які займаються крадіжками карток;
– особи, які використовують загублені картки;
– банківські службовці;
– особи, які займаються виготовленням підроблених пластикових карток;
– особи, які є законними власниками пластикових карток.

Кожний злочин відбувається в тій чи іншій обстановці, у тих чи інших умовах. Поняття обстановки вчинення злочину має важливе наукове і практичне значення, оскільки воно тісно пов'язано з питанням оптимізації як практичної, так і науково-дослідної та дидактичної криміналістичної діяльності. Зокрема, диференціація об'єктивної реалії, охоплюваної даним поняттям, дозволяє визначити коло його складових елементів, а виходить, і обставин, які необхідно з'ясувати в справі (часу доби, дня, тижні, місяця, місця вчинення злочину, наявності поблизу житлових, виробничих та інших об'єктів тощо). Визначені ознаки обстановки використовуються в якості основ класифікації злочинів на криміналістичній основі при створенні методик виявлення і розслідування злочинів (прикладом того служать методики щодо виявлення і розслідування розкрадань в певних галузях народного господарства, вбивств, вчинених на залізничному транспорті, у житлах і поза житловими приміщеннями тощо)[1].

Обстановка вчинення злочину – система різного роду взаємодіючих між собою до й у момент злочину об'єктів, явищ і процесів, що характеризують місце, час, речові, природнокліматичні, виробничі, побутові й інші умови навколишнього середовища, особливості поводження непрямих учасників протиправної події, психологічні зв'язки між ними та інші чинники об'єктивної реальності, що визначають можливість, умови та інші обставини вчинення злочину[2].

Елементи зазначеної обстановки залишають зовні різного роду власні сліди, що можуть бути виявлені при криміналістичному аналізі злочину в процесі його розслідування.

Для її з'ясування велике значення має модальна інформація з різних носіїв і джерел криміналістичної інформації. Виявлення і дослідження подібної інформації, особливо на початку розслідування, дозволяють зібрати істотні дані про виниклу до й у момент події кримінальну ситуацію. Зокрема за такими автономними слідами частіше за все можна одержати такі відомості:

[1] Криминалистика / Под ред. Образцова В.А. – М, 1995. – с. 47.

[2] Криминалистика. Учебник для вузов / Ответственный редактор Н.П. Яблоков. – М, 1995. – с. 51.

Частіше усього зазначені особи не тільки мають спеціальні навики в сфері користування ЕОМ, її пристроями, але і можуть користуватися паролями і ключами банківських програм, застосовувати свої спеціальні знання для фальсифікації програм шляхом зміни правильних вихідних даних. Це, як правило, оперативні працівники банків різного посадового рівня, програмісти й оператори комп'ютерів. Комп'ютерні злочини корисливого типу вчинюють і так звані «хакери» (одержимі програмісти) – переважно молоді люди, добре технічно і професійно підготовлені для роботи з ЕОМ і складання комп'ютерних програм[1].

Дослідження показують, що безпосередній несанкціонований доступ до ЕОМ, систем та комп'ютерних мереж вчинюється співробітниками банків: програмістами, інженерами, операторами, які є користувачами або обслуговуючим персоналом ЕОМ (41,9%). Майже в два рази менше такий доступ виконують інші співробітники банку (20,2%), а в 8,6% випадків злочин було вчинено співробітниками, що були звільнені, 25,5% – несанкціонований доступ вчинений сторонньою особою[2].

«Хакери» – комп'ютерні хулігани, які отримують задоволення від того, що проникли в чужий комп'ютер. Вони прекрасні знавці інформаційної техніки. За допомогою телефонів і домашніх комп'ютерів вони підключаються до мереж, що передають дані, пов'язані майже з усіма великими комп'ютерами, які діють в сфері економіки та банківської діяльності.

Метою хакерів може бути спочатку тільки спортивний інтерес, пов'язаний з вирішенням важкого завдання «злому» захисту програмного продукту чи створення комп'ютерних вірусів тільки для того, щоб потішити свою самозакоханість, пошуткувати. «Хакери» відрізняються високим професіоналізмом в поєднанні зі специфічним комп'ютерним фанатизмом. Потрібно підкреслити, що характерною особливістю злочинців цієї групи є відсутність у них чітко виражених протиправних намірів. Практично всі дії вчинюються ними з метою прояву своїх інтелектуальних можливостей.

Найбільшу загрозу для сфери банківської діяльності становлять професійні злочинці, в діяннях яких ярко виражені корисливі цілі, і, які мають стійкі злочинні навички. Злочини, які носять серійний, багатоепізодний характер, вчиняються багаторазово, обов'язково супроводжуються діями по приховуванню. Це найчастіше висококваліфіковані спеціалісти з вищою математичною, інженерно-технічною чи економічною освітою, які входять в організовані злочинні угрупування, добре оснащені технічно (нерідко спеціальною технікою). На долю цієї групи злочинців приходиться більшість особливо небезпечних посадових злочинів, вчинюваних з використанням засобів комп'ютерної техніки, привласнення грошових коштів в особливо великих розмірах тощо.

[1] Н.П. Яблоков Криминалистическая характеристика финансовых преступлений. // Вестник московского университета. Серия 11. Право. - 1999, № 1. – с. 42.

[2] Матеріали «Центру дослідження проблем комп'ютерної злочинності», www.crime-research.org

першооснов для забезпечення будь-якому потенційному користувачу в будь-який час в будь-якому місті країни доступу до інформації, яка необхідна для вирішення відповідних господарських, технічних, наукових, соціальних та особистих проблем.

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 спрощення розрахунків шляхом впровадження в банківську систему комп'ютерної мережі та інших технічних засобів.

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

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 системи у залежності від допуску користувачів. Коло працівників, які за технологією виконання банківських операцій мають доступ до широкого діапазону цієї інформації, досить велике. Тому система захисту електронних мереж, що ґрунтується тільки на кодуванні входів до різних видів інформації, малоефективна. Треба знайти принципово нові підходи для розробки відносно надійної системи захисту комп'ютерних мереж. Така система повинна будуватися згідно із технологією банківського документообігу та особливостями форм розрахунково-кредитних операцій.

Інформаційна технологія стала промисловим фактором. Сьогодні вона займає позицію, яка прирівнюється до таких факторів як труд та капітал. Це означає, що той хто вміє користуватися інформаційною технологією одержує можливість впливати на економічні процеси, а відтак на політику і взагалі на суспільство.

Протягом останнього десятиріччя значно розширилися масштаби протизаконного використання ЕОМ саме при вчиненні економічних злочинів.

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 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 запитами та іншими формами перевірки. Випадки крадіжок грошей за допомогою комп'ютерної техніки стають такими самими небезпечними злочинами, як викрадення дітей, вимагання, тероризм, торгівля наркотиками.

Більшості з них властива психологія користолюбців, ділків, жага до наживи, прагнення до швидкого накопичення багатства будь-яким шляхом без урахування того, що їх діяння можуть наносити часом серйозний збиток економіці України.

Серед осіб, що вчинюють названі злочини, відносно високий рівень освіченості.

До специфічної категорії такого роду правопорушників варто віднести осіб, що вчинюють розкрадання за допомогою використання комп'ютерних банківських систем.

Характеризуючи осіб, які вчиняють комп'ютерні злочини, необхідно відмітити основну відзнаку, а саме: в електронну злочинність втягнуто широке коло осіб, від висококваліфікованих фахівців, до дилетантів.

Вітчизняні і зарубіжні дослідження дають можливість скласти портрет типового комп'ютерного, електронного злочинця, тобто відповідний профіль даного соціального типу: йому в середньому 30 років, за освітою – інженер в галузі електроніки і математики, або програміст, але існують випадки, коли злочинці взагалі не мають ніякого технічного досвіду. Крім цього особи не стоять на обліках в ОВС і взагалі не мають кримінального минулого.

За матеріалами Центру дослідження комп'ютерної злочинності суб'єктами злочинів, що вчиняють за допомогою високих технологій, в 5 разів частіше є чоловіки. Більшість злочинців мають вищу або незакінчену вищу технічну освіту (53,7%), іншу вищу або незакінчену вищу освіту (19,2%). Серед них переважають особи віком від 30 до 45 років (46,5%), а також від 16 до 30 років (37,8%)[1].

З позицій людських психофізіологічних характеристик – це яскрава, думаюча, творча особа, професіонал своєї справи, готовий прийняти технічний виклик, бажаний працівник. Вони часто займають відповідальні посади і мають спеціальні знання та найновіші технології, доступ до комп'ютерних систем.

Одночасно – це особи, яка бояться втратити авторитет, або ж певний статус в рамках певної соціальної групи, або ж бояться на роботі глузувань.

Варто враховувати, що на даному етапі комп'ютерні злочини переважно вчинюються організовано. Це пояснюється тим, що організованим злочинним угрупуванням, які мають широке коло впливу, не становить великих проблем перевести гроші на закордонні банківські рахунки, або через підставні фірми «відмити» їх, щоб в подальшому, легалізувати та пустити в обіг.

Такі злочинці відзначаються уважністю і пильністю, їх дії витончені, хитромудрі, супроводжуються відмінним маскуванням. Ззовні поведінка таких людей нічим не відрізняється від встановлених у суспільстві соціальних норм.

[1] Матеріали «Центру дослідження проблем комп'ютерної злочинності», www.crime-research.org

З погляду формування криміналістичної характеристики злочинів також важливий урахування ознак, виникнення яких пов'язано з підготуванням і вчиненням злочину, подальшими діями злочинців. До числа цих ознак відносяться зміни, виникнення яких пов'язано з реалізацією намірів злочинця завуалювати, замаскувати, змінити риси своєї зовнішності (наприклад, шляхом видалення шрамів на обличчі, татуювань, вдягання масок під час вчинення злочинів), а також характер, вид, локалізація ушкоджень на тілі, одягу, іншому майні злочинця, що виникають у процесі взаємодії з іншими об'єктами при вчиненні злочину (наприклад, ушкодження тіла злочинця, які він отримав)[1].

У криміналістичному вивченні особи злочинця в даний час намітилися два специфічних напрями. Перший передбачає одержання даних про особу невідомого злочинця з урахуванням виду, місця і часу вчинення діяння, предмета посягання за залишеними ним слідами на місці злочини, у пам'яті свідків і за іншими джерелами. Це дозволяє вірніше визначити напрями і прийоми її розшуку і затримання. Частіше за все така інформація дає уяву про загальні властивості якоїсь групи осіб, серед яких може знаходитися злочинець, і рідше – про деякі якості конкретної особи. Такого роду дані з метою скорішого виявлення і розшуку злочинця повинні зіставлятися з криміналістичними даними про те, хто частіше за все вчинює злочини розслідуваного виду встановленим способом у сформованій обстановці.

Друге – вивчення особи затриманого підозрюваного або обвинувачуваного з метою вичерпної криміналістичної оцінки особистості суб'єкта. З цією метою доцільно зібрати відомості не тільки про життєву установку, ціннісні орієнтації, дефекти правосвідомості, особливості антигромадських поглядів, але головним чином і про те, яка інформація про особистість суб'єкта злочину, його зв'язки, особливості поведінки до і під час вчинення злочину допоможе налагодити з ним необхідний контакт, вибрати найбільш ефективну тактику спілкування з метою одержання від нього правдивих показань, а також визначити найбільш діючі способи профілактичного впливу на нього. Водночас ці дані з урахуванням інформації про злочинців, що враховується в інших елементах характеристики, можуть бути покладені в основу типізації злочинців[2].

У тих випадках, коли злочин вчинюється організованою злочинною групою, вона стає самостійним об'єктом криміналістичного вивчення і відповідно одним з елементів криміналістичної характеристики даного злочину. При цьому вивчаються особливості цієї групи з погляду ступеня її організованості, структури, розгалуженості, рольових функцій її учасників та інше. З'ясування цих особливостей злочинної групи дає можливість краще зорієнтуватися в напрямах розшуку фактичних даних, необхідних для розкриття всіх ланок злочинної діяльності членів групи і всіх основних епізодів їх діяльності.

[1] Криминалистика / Под ред. Образцова В.А. – М, 1995. – с. 40.

[2] Криминалистика. Учебник для вузов / Ответственный редактор Н.П. Яблоков. – М, 1995. – с. 54-55.

РОЗДІЛ 2
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ, ВЧИНЕНИХ У БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ

2.1. Поняття криміналістичної характеристики злочинів, вчинених в банківській системі України

Банківська система життєдіяльності держави, яка пов'язана з накопиченням, розподілом і використанням державних і приватних коштів, є однією з найбільш привабливих для окремих злочинців і особливо організованих злочинних груп. У даній системі вчинюється значна кількість різного роду фінансових афер, здійснюваних при різних банківських операціях.

Для нормального функціонування економіки необхідна надійна, стабільна і розвинена банківська система, при якій банки будуть здійснювати платежі, вчасно надавати своїм клієнтам кредити, послуги по операціям з цінними паперами тощо, якщо фінансове становище банку «похитнулось», то разом з ним може похитнутися і фінансове становище сотень його клієнтів.

Щорічне зростання кількості банківських злочинів збільшує розміри заподіяної ними шкоди. Дані за 1997-1998 роки свідчать, що більш ніж 75% від всіх збитків, заподіяних економічною злочинністю, припадає тільки на сферу діяльності комерційних банків [1].

Злочини, що вчинюються в банківській системі або з її використанням, можна віднести до одних з найбільш небезпечних економічних злочинів, оскільки їх негативний вплив відображається не тільки на самому банку, але і на багатьох інших суб'єктах економічної діяльності і фінансовій системі держави в цілому.

Особливо великих розмірів досягають суми, які знімаються з банківських рахунків, як вкладників, так і ресурсів самих банків, з використанням комп'ютерних систем. До таких злочинів варто віднести ті, що охоплюють склади злочинів, передбачених Кримінальним кодексом України в статтях 190 «Шахрайство», 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення», 361 «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», 362 «Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем», 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем».

На початку 90-х років в Україні розпочалася глобальна комп'ютеризація суспільства, яка стала не просто фактом науково-технічного прогресу, а і надійно увійшла в професійну діяльність, побут, науку, освіту, культуру. Комп'ютери стали незамінними помічниками людини.

У нашій країні вже сьогодні знаходиться досить розвинена система електронного зв'язку, яка не може бути абсолютно надійною та захищеною. Така ситуація надає можливість злочинцям отримувати несанкціонований

доступ до комп'ютерних інформаційних систем для проведення незаконних маніпуляцій у корисливих цілях. Процес комп'ютеризації суспільства призводить до збільшення кількості комп'ютерних злочинів, зростання їх ваги за розмірами сум, що використовуються в загальній частині матеріальних витрат, у порівнянні із звичайними видами злочинів.

В даний час у вітчизняній криміналістичній науці не існує скільки-небудь зведених даних для формування понять основних елементів криміналістичної характеристики комп'ютерних злочинів, вчинених у банківській системі.

Як показують проведені дослідження, 55% опитаних респондентів не мають про ці категорії ні найменшого поняття, а 39% – лише частково знайомі з криміналістичною характеристикою осіб, схильних до вчинення комп'ютерних злочинів за ненауковими джерелами, з яких 66% – засоби масової інформації, 28% кіно- і відеофільми (як правило закордонного виробництва). І при цьому як респонденти були в основному курсанти-випускники вищих навчальних закладів системи МВС України, що у першу чергу повинні мати наукову інформацію про те, з чим їм доведеться зіштовхуватися у своїй безпосередній практичній роботі. Таке положення, природно, не можна визнати позитивним. Тому дуже актуальною як з наукової, так і з практичної точки зору, є розробка проблеми криміналістичної характеристики даних видів злочинних деліктів.

Розвиток методики розслідування нерозривно пов'язаний з узагальненнями й аналізом матеріалів слідчої практики – основного джерела розробки методичних положень і рекомендацій. Вивчення практики розслідування окремих видів злочинів ще в період становлення криміналістики дозволило встановити ряд загальних і важливих для їх розкриття ознак.

Так, в одному з перших посібників з криміналістики (Якимова І.М. Криміналістика. М., 1929) викладу питань власне методики розслідування передувало висвітлення деяких положень, що характеризують окремі види злочинів та осіб, що їх вчинюють. Наприклад, у главі про розслідування грабежів, розбоїв і бандитизму розглядалися «сучасні види цих злочинів», у главі про розслідування шахрайства – «способи вчинення шахрайства» тощо. Однак ці відомості в той час були неповні і недостатньо систематизовані.

З розвитком, теоретичних основ методики розслідування, поглибленням аналізу слідчої практики, розробкою сучасних прийомів і засобів дослідження сукупність загальних положень розслідування злочинів певного виду набуває системного характеру. Подальші розробки в цьому напряму привели до формулювання поняття «криміналістична характеристика злочинів», визначенню елементів її змісту,[1] а в подальшому перетворилось у важливу теоретичну концепцію.

[1] Советская криминалистика: методика расследованы отдельных видов преступлений / Под редакцией Лисиченко В.К. – К., 1988. – с. 29-30.

яких злочинних діянь частіше за все властивий рецидив, а які мають випадковий характер, за якими справами характерне створення злочинних груп, які особливості поводження підозрюваних та обвинувачених на слідстві тощо.

Простежування зв'язку цієї інформації з виявленими даними про спосіб, механізм й обстановку вчинення злочину створює нову самостійну інформацію, що дозволяє правильно визначити напрям і способи розшуку, затримання та подальше викриття злочинців, тобто обрати з урахуванням інших даних в справі оптимальні методи розслідування. Тому особа злочинця є об'єктом самостійного криміналістичного вивчення, а дані про неї – важливим елементом криміналістичної характеристики злочину.

Питання, пов'язані з вивченням особи злочинця розроблялися в криміналістиці протягом тривалого часу[1].

Особи, що вчинюють злочини, характеризуються з погляду їх різноманітних ознак. Мається на увазі власні властивості зазначених осіб, а також їх відношення. Ознаки першої групи поділяються на дві підгрупи: 1) незмінні природні (біологічні) властивості людини (наприклад, стать, особливості будови черепа); 2) що змінюються, соціально обумовлені властивості (професійна приналежність, освітній рівень, отримані в процесі життєдіяльності травми тощо).

Будучи різновидом власних ознак, соціально обумовлені ознаки за своєю природою неоднорідні. Однак їх об'єднує те, що всі вони є не вродженими, а являють собою продукт взаємодії із соціальним середовищем вихідних властивостей, що виражають якісно-кількісну певність людини. З цього погляду їх можна визначити як привнесені, тобто виникають у зв'язку з впливом на розглянуті об'єкти іншого об'єкта (об'єктів). До їх числа відносяться ознаки, що виникають як за бажанням й в інтересах злочинця, так і всупереч його бажанням, що відображають зміни, пов'язані з психічними і біологічним станом людського організму, із зовнішнім і внутрішнім виглядом, суспільним статусом, соціалізацією особистості.

До числа істотних у даній групі ознак звичайно відносять соціальну і професійну приналежність, освітній рівень, посадове положення, трудові функції, захоплення, спосіб життя, схильності, інтереси, наявність або відсутність фізичних вад, психічних аномалій, що виникли з тих чи інших причин у процесі життєдіяльності (в результаті самоосвіти, трудової діяльності, вчинення злочинів, захворювань тощо).

[1] Ведерников Н.Т. Личность преступника как элемент криминалистической характеристики преступления // Криминалистическая характеристика преступления: Сб. науч. трудов / Всесоюзный институт по изучению причин и разработке мер предупреждения преступности. – М., 1984. с. 74-77.; Танасевич В.Г. Криминалистическое понятие раскрытия преступления // Социалистическая законность. - 1975, № 10. - С. 57-58.

поверхню магнітної стрічки картки наносяться штрихи, виконані спеціальними «магнітними» чорнилами (містять феромагнетик);

г) підрізки, зрізання або видалення з картки магнітної стрічки з використанням хімічних реактивів, з наступною її заміною на іншу. До цього способу відноситься і варіант, коли злочинці розрізають дві пластикові картки по горизонталі під магнітною стрічкою, а потім склеюють частину однієї картки з частиною іншої. В результаті такої маніпуляції утворюється картка з зовсім іншими номером рахунку на магнітній стрічці і видавленому номері картки;

5) повна підробка, що поділяється на:

а) підробку, при якій шахраї виготовляють пластмасову заготовку картки методом «сіточного друкування». Поступово «сіточне друкування» замінили іншими, більш вдосконаленими і дешевими, через те, що фірми-виробники в усіх видах карток стали використовувати тонкий малюнок, як додатковий спосіб захисту від підробок;

б) підробку, при якій зображення на чисту пластикову заготовку наносяться з фотомеханічних друкарських форм офсетного друку. Іноді використовується також літографський спосіб нанесення зображень.

в) іншою формою підробки є використання так званої «чистої» пластмаси (White Plastic Crime). У цьому випадку зловмисники виготовляють чисту пластмасову заготовку, що збігається за формою і розмірами зі справжніми картками, і наносять на неї дійсні дані (номер картки, термін дії, відомості про власника тощо). У широкому значенні, цю форму шахрайства теж називають підробкою, але в неї є специфічна особливість, що відрізняє її від інших видів, вона полягає в механізмі отримання коштів по цих картках. Підроблені даним способом картки пред'являються власникам магазинів, що діють спільно зі злочинцями. Здійснення подібного роду шахрайства завжди припускає участь власника (або продавця) магазину і тому, якщо в ході розслідування були виявлені особи, що виготовили фальшивки, то необхідно з'ясувати, хто з персоналу магазина причетний до авторизації картки, той і є співучасником.

• Способи підробки IC-картки (картки з мікрочіпом, в яких може використовуватися додатково і магнітна стрічка як елемент захисту):

а) руйнація електронного замка мікрочіпу, шляхом впливу на мікрочіп невеликими «електричними ударами»;

б) якщо конструкція даної картки передбачає перебування модуля мікрочіпу безпосередньо на поверхні картки, то його просто виймають з гнізда вкраденої і вставляють у фальшиву з внесеними даними шахрая.

Криміналістична оцінка злочину неможлива без врахування даних про властивості особистості його суб'єкта. Результати кожної злочинної діяльності містять сліди особи, яка її здійснила, і, зокрема, дані про деякі її особисті соціально-психологічні властивості та якості, злочинний досвід, спеціальні знання, стать, вік, особливості взаємовідносин з жертвою злочинів тощо.

Класифікація окремих особливостей особи допомагає встановити, який контингент більш схильний до вчинення тих чи інших злочинів, вчинення

Свідченням визнання криміналістичної характеристики, як наукової категорії криміналістики, як відмічають О.М. Колесниченко та В.О. Коновалова, було включення у 1984 році в програму курсу «Криміналістика» (для юридичних інститутів та університетів) самостійної теми «Криміналістична характеристика злочинів»[1], без опису якої не обходиться зараз жодний підручник з криміналістики. Варто відмітити, що термін «криміналістична характеристика злочину» відносно предмету методики розслідування злочинів фігурує у теоретичній, методичній та навчальній літературі з криміналістики[2].

Постійна увага, яка приділяється розробці вчення про криміналістичну характеристику злочинів, як вказує Г.А. Матусовський, «...з'ясовується необхідністю вдосконалення методики їх розкриття на основі пізнання сутності самого злочинного діяння, його механізму, способів, закономірностей процесу слідоутворення, особливостей ознак (слідів), що відображаються»[3].

Успіх розслідування будь-якого злочину багато в чому визначається вмінням слідчого проникнути не тільки в кримінально-правову, але й у криміналістичну його сутність. Правильно ж розібратися в криміналістичній сутності вчиненого діяння слідчий може лише за певних умов. Для цього він повинен мати уявлення про типові криміналістично значимі риси різних видів злочинної діяльності, а також уміти цілеспрямовано виявляти необхідну для цього криміналістичну інформацію в кожному конкретному злочині і зіставляти її з криміналістичною характеристикою відповідного виду злочину.

В основі криміналістичної характеристики злочину лежать дані вивчення залишених ним матеріальних та ідеальних слідів – наслідків, як результат взаємодії його суб'єкта з іншими особами і матеріальними й іншими об'єктами навколишнього середовища, що вказують на криміналістично значимі ознаки злочину, злочинця, різні обставини, у тому числі і побічно пов'язані з даним діянням, можливо, і не істотні для його кваліфікації, але важливі для розкриття злочину. При цьому процес формування елементів, що складають структуру цієї характеристики, виходячи з об'єкта вивчення, не може не враховувати загальну структуру злочинної діяльності, характерну для її відповідного виду. У той самий час ця структура не може не погоджуватися певною мірою з кримінально-правовими, кримінально-процесуальними і кримінологічними напрямами пошуку відповідної інформації про злочин.

---

[1] Колесниченко А.Н., Коновалова В.Е. Криминалистическая характеристика преступления: Учеб. пособие. – Харьков, 1985. – с. 7.

[2] Танасевич В.Г., Образцов В.А. О криминалистической характеристике преступлений // Вопросы борьбы с преступностью. Вып. 25. – М., 1976. – с. 95.

[3] 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.

Криміналістична характеристика за змістом та призначенням відрізняється від інших характеристик, наприклад кримінально-правової, кримінологічної, судово-психологічної, але вони певною мірою взаємозалежні, розглядають деякі однакові елементи, але в різному плані.

Кримінально-правова – формується на основі аналізу ознак злочинів, що мають значення для вирішення питання про наявність складу злочину, правильної його кваліфікації, з'ясування інших кримінально-правових питань, у тому числі, що вирішуються при постанові вироку (ст. 324 КПК України).

Кримінологічна – містить систематизовані відомості, що мають значення для встановлення причин і умов, що сприяють вчиненню злочинів і вжиття заходів щодо їх усунення. Кримінологічна характеристика, наприклад, розкрадань державного і суспільного майна включає такі основні дані: а) стан боротьби з розкраданнями; б) класифікація розкрадань; в) класифікація злочинців, характеристика окремих типів розкрадачів і їх дій.

Судово-психологічна – відображає найбільш істотні психологічні дані про злочинців і потерпілих, типові групи свідків щодо окремих видів злочинів тощо.

У практичній діяльності щодо розкриття злочинів різні характеристики використовуються комплексно, кожна з них служить єдиній кінцевій меті – ефективному розслідуванню, встановленню істини в справі.

Криміналістична характеристика злочину на відміну від кримінально-правової не є органічною частиною загального розуміння злочину і носить допоміжний специфічний службовий характер. І хоча не може бути криміналістичного опису абстрактного злочину, загальне розуміння криміналістичної характеристики злочину є.

В юридичній літературі є велика кількість різноманітних визначень поняття криміналістичної характеристики[1]. Усі вони в основному відображають дві точки зору. Відповідно першій з них, криміналістична характеристика складає систему тих чи інших ознак злочину. Про це говорить І.І. Артамонов – «науково розроблена система найбільш суттєвих, типових криміналістичних рис, якостей, ознак певної категорії злочинів», Гуняєв В.А. – «система сталих ознак певного виду (підвиду) злочину»[2] та інші автори.

[1] Криминалистические характеристики в методике расследования преступлений / Межвуз. сб. науч. трудов. Вып. 69. – Свердловск, 1978. – 155 с.

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

Але найбільшу загрозу для системи платежів із використанням банківських пластикових карток представляє їх підробка. Цей вид злочинів розвивається найбільш динамічно і створює великі труднощі, як при розслідуванні, так і при підрахунку збитків. Злочинці використовують номера справжніх карток, причому власники карток навіть не здогадуються про це.

Розглянемо основні способи підробки пластикових карток.

• способи підробки карток з магнітною стрічкою:

1) механічний – коли зловмисник зрізає деякі цифри, літери. Літери або цифри, що вдруковано в площину картки, можуть «збривати» і, за допомогою клею, що швидко висихає, замінювати їх на інші. При підробці злочинці використовують гострі ріжучі інструменти: леза, скальпелі, ножі тощо. Іноді видалення цифр номера (літер імені власника) робиться за допомогою канцелярського діркопробивача. В отвори, що утворилися, вставляються фрагменти, видалені таким самим способом з іншої картки. До цього способу відноситься і метод, при якому злочинці розрізають дві картки по вертикалі на половинки. Потім половина однієї картки склеюється з протилежною половиною іншої. Використання такої картки можливо тільки при змові з продавцем;

2) термічний – при цьому способі для того, щоб «забрати» дані з картки, розгладжують пластмасу (перед цим зскрібають фарбу з опуклих знаків і зачищають), а після цього замість старих видавлюють нові цифри або літери. Цей спосіб підробки став відомий на початку 80-х років. Майже всі пластикові картки донедавна виготовлялися з поліхлорвінілу, що стає еластичним під дією тепла. Ця його властивість і підштовхнула зловмисників до використання різних джерел тепла: праски, свіча, гаряча вода, мікрохвильові джерела тепла тощо. Після розігрівання матеріалу картки (нагрівають зворотний бік картки), видавлені символи втискуються всередину картки, далі поверхню картки вирівнюють вручну або за допомогою гідравлічного пресу, а потім видавлюють нові знаки;

3) шляхом наклеювання на картку плівки з уже нанесеними реквізитами, а потім вдавлення опуклих знаків. Часто для наклеювання використовують апарати для проклеювання, які застосовують в аеропортах для маркування багажу. Ці наліпки приховують ушкодження і на чіпових картках, які «зламано»;

4) зміна магнітної стрічки, що здійснюється шляхом:

а) зняття захисної плівки, а потім переніс інформації з однієї магнітної стрічки на іншу;

б) буферизації, при якій інформація з магнітної стрічки переноситься на інший магнітний носій для подальшого її використання при декодуванні (кодуванні) будь-якого номера на магнітній стрічці. Буферизація призначена для відновлення початкового балансу банківської дебетової (розрахункової) картки або карток типу «електронний гаманець». На магнітній стрічці даних карток міститься закодована інформація про якусь конкретну грошову суму (баланс картки), що у процесі використання картки поступово зменшується;

в) реконструювання – подібно до буферизації, але відрізняється тільки способом зміни інформації про рахунок (баланс картки), в цьому випадку на

матеріальних цінностей та грошей.

3-й спосіб – значне поширення отримало шахрайство з пластиковими платіжними засобами, що робиться при співучасті касирів магазинів. Суть цього способу зводиться до використання свідомо підроблених сліпів, виготовлених зі справжніх пластикових карток. Сліпи виготовляються шахраями за допомогою складальних друкарських форм або шляхом застосування підроблених кліше з використанням інформації зі справжніх пластикових карток.

4-й спосіб – цей спосіб використовують продавці великих магазинів. Суть його в тому, що при друкуванні даних про продаж того чи іншого товару інформація, що переноситься з кредитної або дебетової картки в облікові дані, може бути змінена. Між копіювальним папером і копією документа про продаж поміщається аркуш паперу відповідного розміру, що перешкоджає друкуванню частини інформації. Потім, за допомогою аналогічної операції проводиться заповнення порожньої ділянки, що утворилася раніше. Таким чином, спритний продавець може змінювати номер рахунку, прізвище власника картки.

5-й спосіб – даний спосіб шахрайства став можливим після появи нових моделей «кодувальних машин» та імпринтерів, за допомогою яких можна не тільки зчитувати інформацію з магнітної стрічки картки, але і стирати старі дані, а також переносити закодовану інформацію з однієї картки на іншу.

Для 6-го способу характерне заволодіння пластиковим платіжним засобом у результаті викрадення його в утримувачів шляхом крадіжки з квартири, на транспорті або в інших місцях, а також у результаті втрати власником картки після придбання її в банку.

Картка викрадається в хазяїна, як правило, разом із документами, гаманцем та іншими речами, подія ця частіш за все не залишається непоміченою. Якщо тільки викрадач картки не кинеться відразу робити покупки, не викликавши при цьому своїм поводженням підозр з боку касира та ідеально підробить підпис, а також якщо викрадач не скористається нею в регіоні, не заявленому в «стоп-листі».

Організації, що приймають до оплати картки, періодично інформуються емітентами про номери карток, визнаних недійсними, викраденими, загубленими, фальшивими. Список номерів таких карток називається «стоп-лист». При використанні картка перевіряється на дійсність її реквізитів за «стоп-листом» і за допомогою прокатного апарата[1].

Реальну загрозу банківської індустрії пластикових платіжних засобів представляють і хакери. Вони можуть за допомогою спеціального програмного забезпечення визначати, а потім продавати номера діючих рахунків кредитних карток, а також поширювати паролі, ідентифікаційні номери, кредитну та іншу персональну інформацію через комп'ютерні мережі, чим роблять допомогу злочинцям в одержанні незаконного доступу до кредитних бюро та комп'ютерних систем фінансових установ.

[1] Н.П. Яблоков Криминалистическая характеристика финансовых преступлений // Вестник московского университета. Серия 11. Право. – 1999, № 1. – с. 36.

Друга точка зору полягає в тому, що криміналістична характеристика злочину може бути представлена як «типова інформаційна модель»[1], «система відомостей (інформації) про криміналістично значущі ознаки злочину», «інформаційна модель події»[2], «система інформації про розслідуваний злочин, що має кримінально-правове і процесуальне значення»[3].

Порівнюючи ці точки зору, можна погодитися с А.Л. Дудніковим, який справедливо вказує, що «система криміналістичних ознак злочину – це ще не характеристика, а відображення сутності події, за яким формулюється така характеристика для отримання у підсумку криміналістично значущої «картини» злочину»[4]. Друга точка зору, на наш погляд, більш точно відображає зміст криміналістичної характеристики злочину.

Криміналістична характеристик поділяється в залежності від рівня та обсягу відомостей, які в ній містяться, на три види:

– загальну, яка відноситься до усіх видів злочинів;

– виду (групи) злочинів;

– конкретного злочину[5].

Перший вид передбачає розробку основ криміналістичної характеристики всієї сукупності різноманітних злочинів. Їх формування відбувається шляхом вивчення та порівняльного аналізу криміналістичних характеристик окремих груп, видів та різновидів злочинів. Як вказує В.А. Образцов, такого роду характеристика «...має орієнтуючу роль, виступає як теоретична основа розробки та вдосконалення типових криміналістичних характеристик окремих категорій злочинів, визначає однаковий підхід до розуміння сутності, структури, форм і способів використання даних, що в них містяться[6].

Видова криміналістична характеристика, як вказує більшість авторів, складає основу для розробки методики розслідування окремих видів злочинів (наприклад, розкрадань), а також певних груп злочинів (наприклад, економічних злочинів), або різновидів злочинів (наприклад, розкрадань, які здійснюються в процесі приватизації державного майна). Як зазначає М.П. Яблоков «видові і групові криміналістичні характеристики через їх специфічність повинні бути типовими, тобто містити цілісне науково узагальнене уявлення про відповідний вид і групу злочинів»[7].

[1] Криминалистика. Под ред. Образцова В.А. – М. Юрист, 1995. – с. 38.

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

[3] Андреев И., Грамович Г.И. Криминалистика: учебное пособие. – Минск. 1997, – с. 180.

[4] Дудников А.Л. Криминалистическая система признаков хищений, совершаемых путем злоупотребления служебным положением, и использование ее данных в расследовании преступлений. Автореф. дисс... канд. юрид. наук: 12.00.09 / Харьк. юрид. ин-т. – Х., 1989. – с. 49.

[5] Матусовский Г.А. Методика расследования хищений / Учебное пособие. – К., 1988. - с. 6.

[6] Криминалистика / Под ред. Образцова В.А. – М., 1995. – с. 39.

[7] Криминалистика. Учебник для вузов / Ответственный редактор Яблоков Н.П. – М. – с. 46.

Підхід на рівні окремого припускає криміналістичну характеристику конкретного діяння як єдиного у своєму роді, унікального явища реальності. Це – не що інше, як уявна модель даного конкретного об'єкта, досліджуваного в кримінальному процесі, що відображає той чи інший комплекс специфічних ознак, якими він відрізняється не тільки від інших подій, але і від подій того ж порядку, тобто інших індивідуально визначених злочинів. З цього приводу в літературі існують різноманітні точки зору. І.Ф. Пантелєєв вважає, що «існує криміналістична характеристика виду або групи злочинів, а також окремого конкретного злочину, але не злочину взагалі»[1]. М.П. Яблоков вказує, що «криміналістична характеристика зобов'язана бути суто криміналістичним описом злочину», і що «можливо говорити не тільки про криміналістичну характеристику індивідуальну, видову; та групову, але й про криміналістичну характеристику злочину взагалі»[2], «криміналістична характеристика окремого злочину, отримана в процесі його розслідування, завжди є індивідуальною, але в той же час частіше за все близькою до якогось її типу»[3].

До висновку щодо можливості криміналістичних характеристик окремих злочинів приходить також А.Г. Філіппов, вважаючи, що в даних випадках мова йде лише про обставини одного злочину, які можуть бути зовсім нетиповими[4].

Інші вчені, зокрема, О.М. Колісниченко, В.О. Коновалова, не вважають оптимальним відносити термін «криміналістична характеристика» до конкретного, одиничного злочину та вважають, що «віднесення поняття «криміналістична характеристика» тільки до виду (групи) злочинів є одним з необхідних умов теоретичної чіткості та практичної корисності відповідних рекомендацій»[5].

Враховуючи наведені вище точки зору на поняття та види криміналістичної характеристики, а також щодо цього дослідження, можна погодитись з визначенням, сформульованим В.К. Лисиченком, оскільки воно відображає найбільш суттєві ознаки криміналістичної характеристики злочинів. Це «система відомостей про криміналістично значимі ознаки злочинів даного виду, що відображає закономірні зв'язки між ними і, яка служить побудові і перевірці слідчих версій для вирішення основних завдань розслідування»[6].

---

[1] Криминалистика / Под ред. Пантелеева И.Ф., Селиванова Н.А. – М., 1993, – с. 26.

[2] Васильева А.И., Яблоков Н.П. Предмет, система и теоретические основы криминалистики. – М., 1984. – с. 115.

[3] Криминалистика. Учебник для вузов / Ответственный редактор Яблоков Н.П. – М., 1995. – с. 46.

[4] Герасимов И В Криминалистические характеристики преступлений в структуре частных методик // Криминалистические характеристики в методике расследования преступлений / Межвуз сб. науч. Трудов. – Выл 69. – Свердловск, 1978. – с. 23.

[5] Колесниченко А.Н., Коновалова В.Е. Криминалистическая характеристика преступлений: Учеб. пособие – Харьков, 1985. – с. 13.

[6] Советская криминалистика: методика расследования отдельных видов преступлений / Под редакцией Лисиченко В.К. – К., 1988. – с. 30.

4.2. Крадіжка грошей шляхом маніпуляції з комп'ютером. Цей метод являє собою операцію підміни даних для ЕОМ з метою отримання фальшивих чеків. Для здійснення цього способу використовуються також прийоми «підміна даних» і «непостійний вибір».

4.3. Крадіжка грошей завдяки отримання секретних кодів. Реалізується на практиці шляхом збору і негайного використання секретних даних. Тут використовуються в поєднанні такі прийоми: «маскарад», «відкачування даних» і «за дурнем».

4.4. Крадіжка грошей шляхом комп'ютерного переказу. Спосіб полягає в таємному використанні міжбанківської комунікаційної мережі за допомогою прийомів «підміна даних і відкачування даних». Крім розглянутих нами вище методів вчинення комп'ютерних злочинів існують також й інші. Найпоширеніший метод присвоєння грошей за допомогою ЕОМ – програмування фіктивних рахунків на вигаданих співробітників при оплаті робіт.

Вчиненню цих злочинів передує певна підготовка, характер якої залежить від ступеня зв'язку правопорушників з діяльністю обчислювального центру банку. Сторонні особи обмірковують шляхи доступу до комп'ютерної системи, намагаються з'ясувати паролі та ключі програм. Програмісти, оператори та інші працівники комп'ютерного центру й інших підрозділів банку, що замишляють подібну аферу, вибирають найбільш сприятливу для її вчинення обстановку, можуть створювати підставну фірму з розрахунковим рахунком для перекачування викрадених грошей тощо.

Злочинна акція, по суті, складається з початку контактних дій правопорушника з ЕОМ або машинними носіями і зняття необхідної інформації або грошей з електронних рахунків клієнтів банку, їх безпосереднього присвоєння або переказу на рахунки «липових» організацій.

Приховання такого злочину відбувається шляхом відновлення початкової програми, що зазнала змін в процесі злочинного доступу до банківської комп'ютерної інформації. Це звичайно буває під силу тільки фахівцям дуже високої кваліфікації і ступеня доступу до банківського програмного забезпечення.

4.5. Шахрайство з пластиковими платіжними засобами та їх підробка.

В залежності від суб'єктів, шахрайство здійснюється такими способами:

1-й спосіб – характеризується тим, що в ньому реалізуються прийоми вчинення шахрайства, пов'язані з використанням банківських службовців з метою одержання від них інформації про грошові внески і про утримувачів пластикових карток з великими внесками за хабар.

Характерним способом шахрайства є перерахування грошей з одного рахунку на інший за фальшивими телексами, після чого шахрай витрачає ці гроші вже зі своєї картки.

2-й спосіб – характеризується участю в шахрайстві обслуговуючого персоналу таких сервісних точок як ресторани, кафе, бари, мотелі тощо. Працівники таких підприємств, користуючись неуважністю клієнта, або умисно відволікають його, роблять декілька додаткових відбитків пластикових карток (сліпів), що потім використовують для привласнення

підвищується.

3.6. «Логічна бомба». Спосіб таємного введення в комп'ютерну програму відповідного набору команд, які повинні обов'язково спрацювати при конкретно визначених умовах, наприклад, через визначений час або конкретну дату тощо. Інколи цей спосіб називають «годинниковою бомбою».

3.7. «Асинхронна атака». Це досить складний спосіб вчинення комп'ютерних злочинів. Виконується він високоерудованими, висококваліфікованими спеціалістами, оскільки вимагає доброго знання операційної системи, професійно-грамотного і вмілого використання ситуації для внесення змін в операційну систему чи направлення її на досягнення своєї мети. Необхідно підкреслити, що всі ці зміни поза системою не будуть помітні.

3.8. «Моделювання». Один з найновіших і перспективних методів вчинення комп'ютерних злочинів. Моделюються ті процеси, в які злочинці бажають втрутитися, і заплановані способи вчинення злочинів. Це дозволяє значно оптимізувати вчинення злочинів. Одним із варіантів є реверсивна модель, коли створюється модель конкретної системи, в яку вводяться реальні вихідні дані і враховуються заплановані дії. З отримання правильних результатів підбираються правдоподібні, бажані. Потім методом прогону моделі назад, до початку, з'ясовують результати і встановлюють, які маніпуляції з вихідними даними треба провести. Таких операцій може бути декілька. Після цього залишається тільки здійснити задумане.

3.9. «Повітряний змій». Спосіб вчинення цього злочину винятково простий. Виконується він так: одночасно в двох банках відкриваються невеликі рахунки, далі гроші переказуються з одного банку в інший, і навпаки, з поступовим збільшенням сум. Хитрість полягає в тому, щоб до того, як в банку виявиться, що доручення про переказ не забезпечено необхідною сумою, приходило б оповіщення про переказ в цей банк, так щоб загальна сума покривала вимогу про перший переказ. Цей цикл повторюється велику кількість разів («повітряний змій» піднімається все вище і вище) до тих пір, поки на рахунку не накопичується велика сума (фактично вона постійно «перескакує» з одного рахунку на інший, збільшуючи свої розміри). Потім гроші швидко знімаються і власник рахунку зникає. Цей спосіб вимагає дуже точного розрахунку, але для двох банків його можна зробити і без комп'ютера. На практиці в таку гру включають велику кількість банків: так сума накопичується швидше і кількість доручень про переказ не досягає підозрілої частоти. Але керувати цим процесом можна тільки за допомогою комп'ютера.

4. Комплексні методи отримання і використання інформації зі злочинною метою.

В перших трьох пунктах ми розглянули типові способи вчинення комп'ютерних злочинів. Але варто зауважити, що злочини такого типу, як правило, вчинення за допомогою поєднання тих чи інших способів та прийомів. Отже є потреба коротко зупинитись на них.

4.1. Внесення змін в програму являє собою поєднання прийомів «маскарад» і «салямі».

Як ознаки й елементи змісту криміналістичної характеристики можна виділити наступне:

1. Відомості про криміналістично значимі ознаки злочинів даного виду. Деякі з них мають значення для кримінально-правової кваліфікації злочину, правильного розгляду кримінальної справи, інші – для прийняття кримінально-процесуальних рішень (наприклад, для обрання запобіжного заходу), треті – для розслідування, четверті – для їх попередження тощо. Цей розподіл має відносний характер, оскільки всі ознаки взаємозалежні (у тому числі з «центральними», що не мають істотного значення) і нерідко у своєму сполученні служать вирішенню декількох завдань, виконують різні функції.

Виділення ознак, що мають значення для обрання ефективної системи слідчих дій і оперативно-пошукових заходів у розслідуванні, обумовлено в основному двома обставинами: а) існують ознаки, що мають тільки криміналістичне значення (наприклад, викрути (хитрощі) злочинця); б) дослідження і використання криміналістичних та інших ознак, що мають різне, у тому числі криміналістичне значення, здійснюються в специфічних цілях – успішного вирішення завдань, що забезпечує швидке, повне і всебічне розслідування.

2. Система відомостей про криміналістично значимі ознаки. Ознаки, що складають зміст криміналістичної характеристики, відносяться як до обставин вчинення злочину, так і супутнім і послідуючим за ним. Останні відіграють важливу роль у виявленні латентних злочинів, а також невідомих злочинців.

Основою системи ознак є їх відношення до предмета доказування (ст. 64 КПК України), а також положення кримінального права про склад злочину і його елементи. При цьому враховується криміналістичне значення окремих груп ознак (наприклад, що відносяться до способу вчинення злочину). Конкретне вираження система криміналістичної характеристики знаходить у її елементах.

3. Система відомостей, що включає дані про закономірні зв'язки між: ознаками злочинів. Це найважливіша частина криміналістичної характеристики. Їх виявлення відбувається на основі досліджень значного емпіричного матеріалу.

Закономірні зв'язки в криміналістичній характеристиці можуть відображати вірогідну взаємозалежність і взаємозв'язок різних груп ознак. Найбільш істотними є закономірні зв'язки між групами ознак, що характеризують сліди злочину (у широкому розумінні), його наслідки, і групами ознак, що відносяться до злочинця і його дій. Це пояснюється тим, що розслідування в відбувається від слідів злочину до з'ясування обставин його вчинення, встановлення злочинця і його дій.

Практичне значення криміналістичної характеристики полягає в тому, що за наявності одних ознак (наприклад, що відносяться до слідів знарядь і інструментів) слідчий може запропонувати наявність інших (певних професійних навиків у злочинця) і провести необхідні слідчі дії (наприклад, щодо встановлення і затримання злочинця).

4. Система відомостей, яка служить побудові і перевірці слідчих версій

для вирішення основних завдань розслідування. Відомості, що складають зміст криміналістичної характеристики, являють собою систематизовані криміналістичні дані, які відносяться до виду злочинів. Слідчий же завжди розслідує конкретний злочин – одиничне антигромадське явище з властивими йому специфічними ознаками. Тому дані криміналістичної характеристики можуть лише зазначити на певну імовірність шуканих ознак у конкретному розслідуваному злочині. Іншими словами, на підставі аналізу й оцінки особливостей конкретного злочину, зіставлення встановлених про нього даних із криміналістичною характеристикою висуваються слідчі версії. Ця робота полегшується, коли в методиках наводяться системи типових версій, побудованих з урахуванням криміналістичних характеристик[1].

Кожна характеристика являє собою опис істотних сторін, властивостей, закономірностей відображеного в ній об'єкта реальної дійсності в цілому або певних компонентів, фрагментів, якими він відрізняється від інших об'єктів навколишнього світу.

Своєрідність криміналістичної характеристики злочинів визначається двома моментами: по-перше, особливостями відображеної в ній реальності та її ознак; по-друге, специфікою цілей подібного відображення.

Елементи криміналістичної характеристики злочинів розкривають їх основні риси. Практика, результати наукових досліджень криміналістичної змісту злочинів показують, що незалежно від виду злочину криміналістично значимі його ознаки в характеристиці виду й окремого злочину частіше можуть міститися в даних про спосіб, механізм й обстановку вчинення злочину, типологічні та інші особливості їх суб'єктів. Водночас для окремих видів, груп злочинів з урахуванням криміналістичних потреб зазначені ознаки можуть міститися в відомостях про предмет злочинного посягання, особистісних особливостях потерпілого, своєрідності організованої злочинної групи, мотивах злочину, характері злочинного результату, що настав тощо.

Виходячи з вищевикладеного, структура криміналістичної характеристики злочинів складна, не повною мірою однакова для окремих видів і груп злочинів. Водночас в залежності від виду злочину, форми провини і окремих його особливостей ті самі структурні елементи в характеристиках різних злочинів можуть бути різними за значенням, походженням (в залежності від характеру джерел їх виникнення) та інше. Наприклад, в одних випадках вони можуть бути головними, в інших – другорядними, первинними і похідними тощо. Так, дані про спосіб вчинення навмисних злочинів в їх криміналістичній характеристиці, як правило, є головними і найбільш важливими, а в характеристиці необережних злочинів – другорядними або, які не мають значення. У той самий час дані про особу злочинця, в залежності від того, чи утворюються вони шляхом вивчення безпосередньої або опосередкованої інформації, можуть бути первинними і похідними.

[1] Советская криминалистика: методика расследования отдельных видов преступлений /Под редакцией Лисиченко В.К. – К., 1988. – с. 32.

інструмент в руках електронного рекетира.

2.10. «Склад без стін». Даний комп'ютерний злочин, як правило, вчинюється шляхом несанкціонованого доступу в комп'ютерну мережу в момент її системної неполадки. Наприклад, коли деякі файли користувача залишаються відкритими, зловмисник може отримати доступ до часток банку даних, що йому не належать. Простіше цей спосіб можна пояснити так: наприклад, уявіть собі, що клієнт банку приходить у виділене для нього сховище-кімнату і виявляє, що в цьому сховищі немає однієї стіни. В такому випадку він може проникнути в чужі сейфи і викрасти все, що там знаходиться.

3. Способи маніпуляції з інформацією.

3.1. Підміна даних. Цей комп'ютерний злочин здійснюється шляхом зміни інформації (або введення і виведення даних з ЕОМ). Цей спосіб досить простий, а тому широко розповсюджений.

3.2. «Троянський кінь». Цей метод полягає в тому, що в чужу програму таємно вводяться команди, які видозмінюють її дії. Це дозволяє здійснювати нові функції, не заплановані власником цієї програми, але одночасно зберігати попередню працездатність. Як правило, за допомогою цього способу злочинці переводять на свій рахунок відповідну суму з кожної операції.

Такі маніпуляції дуже важко виявити, оскільки «Троянський кінь», який може складатися з декількох десятків команд, навряд чи може бути помітним серед сотень тисяч, а інколи і мільйонів команд, що є в комп'ютерних програмах.

3.3. «Троянський кінь в ланцюгах». Відрізняється від попереднього способу тим, що тут мова йде про «троянських коней» в електронних ланцюгах комп'ютерів. Правда, цей спосіб використовується нечасто. Пояснюється це тим, що його можна здійснити в побутових комп'ютерах попередніх поколінь, або ж у заводських умовах на рівні конструкторських розробок і виробництва чіпів.

3.4. «Троянська матрьошка». Цей спосіб є різновидом «троянського коня». Його особливість полягає в тому, що в звичайну частину програми вставляється не команда, що виконує чорнову роботу, а команда, що її формує і після виконання знищує. Отже, щоб електронній нишпорці знайти «троянського коня», то необхідно шукати не його самого, а набір команд, які його формують.

3.5. «Салямі». Це тактика використання «троянського коня». Спосіб ґрунтується на тому, що суми, які відраховуються із вкрадених грошей, невеликі і їх втрати практично непомітні. Накопичення грошей здійснюється за рахунок великої кількості операцій. Це і називається «салямі». Як правило, відраховуються дрібні частини суми грошей, вартістю менше, ніж одна найменша одиниця, оскільки в таких ситуаціях робиться заокруглення. Наприклад, вкладник, перевіряючи свій рахунок, практично не виявляє крадіжки, оскільки сума дуже мала. Якщо ж навіть і помітить, то це не викличе серйозних наслідків. Але коли сума мала в процентному відношенні від значних грошових переведень, вірогідність розкриття значно

зберігається у цій мережі, а також копіювати її.

2.5. «Пролом». Несанкціонований доступ до файлів законного користувача здійснюється також через виявлення слабких місць в захисті системи. Один раз, виявивши їх, правопорушник може, не поспішаючи, досліджувати інформацію, яка знаходиться в системі, копіювати її, повертатися до неї багато разів, як покупець роздивляється товар на вітрині. Електронний злочинець в даному випадку шукає пролом, і знайшовши, користується ним багато разів.

2.6. «Люк». Це спосіб, який дозволяє розірвати програму в якомусь конкретному місці, і вставити туди одну, або декілька своїх команд. Цей «люк» «відкривається» по мірі необхідності, а команди автоматично здійснюють своє завдання.

Найчастіше даний прийом використовують проектувальники інформаційних мереж і працівники організацій, які проводять профілактику і ремонт комп'ютерних систем.

2.7. «Системні роззяви». В основу цього способу покладено несанкціонований доступ шляхом виявлення «пролому» тобто програму входу в комп'ютерну систему (імена, коди, шифри / ключі тощо).

2.8. «Маскарад» («самозванство», «узурпація особистості»). Суть цього способу вчинення злочину полягає в тому, що електронний злодій проникає в комп'ютерну мережу під виглядом законного користувача. Тому діючі сьогодні інформаційні системи, які не мають засобів автентичної ідентифікації з функціональних і фізіологічних характеристик особистості (наприклад, за відбитками пальців, малюнками сітчатки ока, голосом, запахом тощо) залишаються незахищеними від цього способу вчинення злочину.

Найпростіший шлях його вчинення – отримати коди, інші ідентифікуючі шифри законних користувачів. Це можна зробити:

– придбанням (підкуп персоналу) списку користувачів із всією необхідною інформацією;

– виявлення такого документу в організаціях, де не налагоджений достатній контроль за їх зберіганням;

– підслуховування через телефонні лінії.

Інколи трапляється, як, наприклад з помилковими телефонними дзвінками, що користувач з віддаленого термінала підключається до чиєїсь системи, будучи абсолютно впевненим, що він працює з тією системою, з якою ї мав намір. Господар системи, з якої вийшло фактичне підключення, формуючи правдоподібні відгуки, може підтримувати цю помилку протягом певного часу і таким чином отримати деяку інформацію, безпосередні коди. Такий метод має назву «містифікація».

2.9. «Аварійний». Загальновідомо, що у будь-якому комп'ютерному центрі є особлива програма, яка застосовується як системний інструмент у випадках великих збоїв чи інших відхилень у роботі ЕОМ. Тобто своєрідний алгоритм діяльності у критичних, екстремальних ситуаціях, аналог пристроїв, що розміщається в транспорті під надписом «РОЗБИТИ СКЛО У ВИПАДКУ АВАРІЇ». Зрозуміло, що така програма – це могутній і небезпечний

Комплекс взаємозалежних криміналістичних особливостей злочинів, що складають їх криміналістичну характеристику, є певною системою. Виходячи з цього, сукупність ознак, що утворюють криміналістичну характеристику злочинного діяння, є множиною, складові елементи якої органічно пов'язані між собою. При цьому можна виділити форми таких зв'язків між елементами криміналістичної характеристики, притаманні зв'язкам елементів відповідної злочинної діяльності. З погляду потреб криміналістики найбільший інтерес являють виділення і вивчення таких видів зв'язків елементів характеристики, що носять характер певних закономірностей, спираються на дані узагальнення слідчої практики, на вивчені кримінальних справ і характеризують ступінь жорсткості такого зв'язку. Вивчення слідчої практики показує, що елементам криміналістичної характеристики злочинів, відомим на початку розслідування, відповідають інші, ще невідомі в даний момент.

Більшість авторів, що приділяли увагу розробці питання криміналістичної характеристики злочину, включають як її елементи сукупність ознак, що визначають: 1) спосіб вчинення злочину; 2) механізм злочину; 3) обстановка вчинення злочину; 4) особа злочинця; 5) особа потерпілого; 6) об'єкт (предмет) злочинного посягання; 7) мотив і мета злочину; 8) закономірності злочинів[1].

Злочини в сфері комп'ютерної інформації відомі відносно недавно. Вітчизняна практика розслідування таких злочинів поки невелика, оскільки лише в останні роки в результаті розвитку програмно-технічних засобів і підвищення «комп'ютерної освіченості», інформаційні системи впроваджені в такі галузі, як бухгалтерський облік, економічні розрахунки, банківська справа тощо. 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 в даній галузі і дефіцит у слідчих 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 надати детальна розробка криміналістичної характеристики злочинів даного виду.

[1] Криминалистика. Учебник для вузов / Ответственный редактор Н.П. Яблоков. – М., 1995, С. 48-56; Танасевич В.Г., Образцов В.А. О криминалистической характеристике преступлений // Вопросы борьбы с преступностью. – Вып.25. – М., 1976. – С. 94-105; Матусовский Г.А. Методика расследования хищений. – Киев, 1988. – 88 с.; Криминалистика / Под редакцией Образцова В.А. – М., 1995, – С. 39-50; Советская криминалистика: методика расследования отдельных видов преступлений / Под редакцией Лисиченко В.К. – К., 1988. – с. 34-41.

2.2. Елементи криміналістичної характеристики злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій

Дослідження даного елементу криміналістичної характеристики злочину, передусім, вимагає висвітлення сутності та співвідношення понять об'єкта та предмету злочину, які застосовуються в кримінальному праві. Об'єктом злочину вважають суспільні відносини, на які посягає злочин, яким він спричиняє шкоду, наносить збиток, та які захищаються нормами кримінального права[1].

В залежності від виду злочину, предмет злочинного посягання неоднаковий. Злочинні посягання в банківській сфері за кримінально-правовою ознакою кваліфікуються залежно від обставин за статтями різних глав Кримінального Кодексу України:

1. Злочини проти власності – «шахрайство» (ст. 190);
2. Злочини у сфері господарської діяльності – «незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення» (ст. 200);
3. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361 «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», ст. 362 «Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем», ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем»).

Більш близьким криміналістичному поняттю об'єкта злочину – є кримінально-правове поняття предмету злочину. Під предметом злочину розуміються речі матеріального світу, впливаючи на які, особа посягає на ті чи інші суспільні відносини[2].

Тлумачення кримінального закону дозволяє вважати, що законодавець під предметом злочину розуміє лише матеріальний субстрат об'єкта відношення, що у процесі вчинення злочину піддано знищенню, викраденню, видозмінено тощо.

Криміналістична значимість вивчення об'єкта посягання обумовлена насамперед тим, що вплив злочинця на цей об'єкт пов'язано з виникненням різних змін. Ці зміни локалізуються:

– на місці злочинної дії;
– у місцях наступного його перебування, приховування, реалізації;
– на знаряддях злочину, технічних засобах, використаних злочинцем[3].

[1] Бажанов М.И. Уголовное право Украины. Общая часть. – Днепропетровск: Пороги, 1992. – с. 31.
[2] Образцов В.А. Криминалистика: курс лекций. – М., 1996. – с. 38.
[3] Криминалистика / Под ред. Образцова В.А. – М, 1995. – с. 41.

2. Способи несанкціонованого доступу.

Несанкціонований доступ здійснюється, як правило, з використанням чужого імені, зміною фізичних адрес технічних пристроїв, використанням інформації, яка залишилась після вирішення завдань, модифікацією програмного та інформаційного забезпечення, викраденням носія інформації, встановленням апаратури запису, що підключається до каналів передачі даних.

2.1. «За дурнем». Цей прийом часто використовують для проникнення в закриті зони, як просторові, так і електронні. Фізичний варіант полягає в тому, щоб взявши в руки якомога більше предметів, пов'язаних з роботою на комп'ютері і чекати біля закритих дверей, за якими знаходиться термінал, і, коли з'явиться законний користувач впевнено пройти в двері разом з ним.

Подібним шляхом здійснюється і електронний варіант, коли комп'ютерний термінал незаконного користувача підключається до лінії , законного користувача через телефонні канали, (Інтернет), або ж коли законний користувач ненадовго виходить, залишаючи термінал в робочому режимі.

2.2. «За хвіст». В даному випадку незаконний користувач, підключившись до лінії зв'язку законного користувача, чекає сигнал, який вказує на кінець роботи, перехоплює його, і після закінчення активного режиму, здійснює доступ до комп'ютерної системи.

2.3. «Комп'ютерний абордаж». Хакери (від англ. „hack" – розрубати) – програмісти чи кваліфіковані користувачі ЕОМ, які займаються пошуком способів отримання несанкціонованого (самовільного) доступу до комп'ютерної інформації і технічних засобів [6]. Вони по черзі набирають навмання один кодовий номер за іншим, і терпляче чекають відповіді чужого комп'ютера. Після цього телефон підключається до приймача сигналів в особистій ЕОМ – і зв'язок встановлений. Якщо після цього вдається вгадати код, що буває нескладно, оскільки слова, які є паролем, часто банальні і беруться, як правило, з інструкцій по використанню комп'ютера, то процедура входу в чужу комп'ютерну мережу, можна сказати забезпечено.

Зрозуміло, що проникнення чужого комп'ютера в інформаційну мережу не проходить без наслідків. Хакери, при всій своїй обережності в роботі з інформацією, інколи залишають сліди.

Той, хто відчув такий напад, негайно міняє систему захисту інформації. Після цього хакери намагаються навмисне залишити сліди у першому комп'ютері інформаційної мережі, щоб персонал, який відповідає за комп'ютерну безпеку інформаційної мережі, вважав, що має справу з аматором. В результаті служба комп'ютерної безпеки послаблює увагу до контролю за іншими системами, в той час, як пірати отримують до неї доступ через який-небудь пролом.

Необхідно відзначити, що «комп'ютерний абордаж» є підготовчою стадією вчинення комп'ютерного злочину.

2.4. «Непостійний вибір». Спосіб вчинення цього злочину полягає в пошуку слабких місць в захисті системи, після чого злочинець може щоденно і багато разів, не поспішаючи досліджувати інформацію, яка його цікавить і

електронно-обчислювальних машин (ЕОМ) або комп'ютерних мереж. Цей вид розкрадання характеризується тим, що злочинці, скориставшись службовою можливістю для неправомірного доступу до комп'ютерної інформації фінансового характеру, зосередженої в обчислювальних центрах банківських установ, і виявивши прогалини в діяльності ревізійних служб, здійснюють кримінальні операції із зазначеною інформацією, що знаходиться в ЕОМ або на машинних носіях.

Основні способи комп'ютерних злочинів можна поділити на 4 основні групи:

1. Перехоплення інформації: безпосереднє перехоплення, і електромагнітне перехоплення.

2. Несанкціонований доступ до інформації: «комп'ютерний абордаж», «містифікація», «маскування», «непостійний вибір», «за хвіст», «аварійний», «за дурнем», «пролом», «люк», «склад без стін», «системні роззяви».

3. Маніпуляції з інформацією: «троянський кінь в ланцюгах», «троянська матрьошка», підміна даних, підміна коду, комп'ютерні віруси, «салямі», «логічна бомба», «асинхронна атака», моделювання, «повітряний змій», «пастка на живця».

4. Отримання і використання інформації зі злочинною метою: крадіжка програмного забезпечення, крадіжка устаткування за допомогою комп'ютерних операцій, крадіжка грошей за допомогою отримання секретних кодів, крадіжка грошей шляхом комп'ютерного пересилання, крадіжка грошей шляхом маніпуляції з комп'ютером, внесення змін в програму, підробка кредитних карток[1].

1. Способи перехоплення інформації:

1.1. Безпосереднє перехоплення. Потрібне устаткування можна придбати у магазинах: мікрофон, радіоприймач, касетний диктофон, модем, принтер. Перехоплення даних здійснюється або безпосередньо через телефонний канал системи, або підключається до комп'ютерних мереж. Вся інформація зчитується з кабельних, дротових, а також наземних мікрохвильових систем, систем супутникового і спеціального урядового зв'язку.

1.2. Електромагнітне перехоплення. Використовуються пристрої перехоплення безконтактної дії. Можна вловити випромінювання, яке дає центральний процесор, дисплей, телефон, принтер, лінії мікрохвильового зв'язку, зчитувати дані з дисплейних терміналів, за допомогою доступних кожному найпростіших технічних засобів (дипольної антени, телевізора). Злочинці, знаходячись в автомобілі чи просто з приймачем в портфелі на деякій відстані від споруди, можуть, не привертаючи до себе уваги, легко добувати дані, які зберігаються в пам'яті ЕОМ чи використовуються в процесі роботи. Під час експериментів вдавалося отримувати відомості, які виводились одночасно на 25 дисплейних терміналах, розташованих в безпосередній близькості один від одного, і відокремлювати виведені на кожен екран дані. Якщо до телевізора підключити відеомагнітофон, то інформацію можна не тільки накопичувати, а і спокійно проаналізувати пізніше.

[1] Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: Навч. Посіб. – К: Українська академія внутрішніх справ, 1994. – с. 23.

Предмет вказаних злочинних посягань відразу або в кінцевому результаті складають грошові кошти держави чи приватних фірм, підприємств та осіб у гривневій та іноземній валюті, інформація, інші матеріальні цінності. Під матеріальними цінностями розуміють будь-яку річ, котру можна викрасти. Це пов'язано з тим, що внаслідок управління технічними засобами різних сфер життя людини відбулись крадіжки таких речей як залізничні потяги, космічні супутники[1].

Безпосередню увагу привертає крадіжка грошових коштів за допомогою інформаційних технологій. Потрібно зауважити, що в даній ситуації викрадаються кошти, не в звичному для нас розумінні, а безготівкові. Але це ті самі гроші, які мають лише незвичну форму. За останні роки український ринок банківських технологій пройшов шлях від початкової стадії комп'ютеризації – реалізації найпростіших банківських операцій на основі персональних комп'ютерів до повноцінних автоматизованих банківських систем, що відповідають найсуворішим сучасним вимогам. Активно впроваджуються міжнародні системи платежів.

Здійснення різних фінансових операцій між окремими як фізичними, так і юридичними особами відбувається шляхом електронного зв'язку. Купівля товарів, оплата послуг стала можливою завдяки новітнім інформаційним технологіям.

Вони можуть бути використанні не тільки для правомірних дій, а й для злочинних. Коли особа за допомогою комп'ютера проникає в банківську електронну систему шляхом її зламу, вона забезпечує собі доступ до банківських рахунків, які є фактично інформацією про певну грошову цінність даного рахунку чи вкладу, маючи можливість змінити кількісне вираження певного рахунку. Потім особа має різні можливості використати ці, начебто, неіснуючі гроші: отримати готівку, купити будь-які товари тощо.

Сучасний стан інформаційних систем та обчислювальної техніки дозволяє впроваджувати усе більш тонкі і цікаві для користувача технології. Одна з них – так звані «електронні гаманці». Поява і розповсюдження пластикових платіжних засобів в Україні зумовлені взаємною зацікавленістю в цьому держави і власника пластикових карток. Для держави це один з засобів зниження потреби в готівковій грошовій масі.

Сама по собі картка не є цінністю. Вона – інструмент в руках того, хто нею користується. Розміри картки регламентуються міжнародним стандартом. Основна функція будь-якої пластикової картки – ідентифікація її пред'явника. Тобто в спрощеному варіанті це може бути картка, на якій написані ім'я і прізвище. У дійсності справа виглядає набагато складніше. На лицевій стороні картки, як правило, приблизно одну третину займає поле, в якому розташовується торгова марка емітента. На звороті картки частіше за все розташовується магнітна смуга, під нею – смуга для підпису, виготовлена з паперу або шляхом напилювання. Ще нижче подається інформація про емітента і про те, як з ним зв'язатися.

[1] Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: Навч. посіб. – К: Українська академія внутрішніх справ, 1994. – с. 30.

Захищаючи картку від підробки, фірми, що виготовляють пластикові заготовки, наносять у процесі виготовлення на картку спеціальні елементи захисту. На сьогоднішній день картки мають по 7-10 ступенів захисту від підробки. У такому вигляді заготовки надходять до емітента.

Як тільки визначиться людина, яка буде користуватися карткою, емітент робить персоналізацію конкретної картки. На неї наносять персональні дані про емітента і про людину, у чиїх руках вона буде перебувати.

Тому можна стверджувати про ймовірність крадіжки за допомогою інформаційних технологій саме безготівкових грошей.

Найважливішим і визначальним елементом криміналістичної характеристики будь-якого злочину є сукупність даних, що характеризують спосіб його вчинення.

Спосіб вчинення злочину є об'єктом вивчення ряду наук кримінального циклу: кримінального права, кримінального процесу, кримінології, криміналістики. Кримінально-правове поняття способу, що розробляється на основі кримінального закону, є базовим для інших наук[1].

Криміналістично значима інформація про спосіб вчинення злочину в значній мірі є модальною, а її конкретні носії і джерела, в залежності від виду вчиненого злочину, можуть бути всіх трьох видів (гомологічною, предметною і документальною). Саме такого роду характер даних дозволяє швидше і вірніше орієнтуватися в суті й особливостях вчиненого злочину, його обставинах, колі осіб, серед яких варто шукати злочинця і намітити оптимальні методи розкриття злочину.

Під способом вчинення злочину в криміналістичному значенні доцільно розуміти об'єктивно і суб'єктивно обумовлену систему поведінки суб'єкта до, у момент і після вчинення злочину, що залишає різного роду характерні сліди зовні, що дозволяють за допомогою криміналістичних прийомів і засобів одержати уяву про суть того, що сталося, своєрідності злочинної поведінки правопорушника, його окремих особистісних даних і відповідно визначити найбільш оптимальні методи вирішення завдань розкриття злочину[2].

Іншими словами, спосіб вчинення злочину складається з комплексу специфічних дій правопорушника щодо підготовки, вчинення та приховування злочину. У багатьох випадках ці дії являють собою систему з багатьма її елементами і залишають у зовнішній обстановці відповідні відображення, що представляють в інформаційному плані своєрідну модель злочину.

---

[1] Панов Н.И Уголовно-правовое значение способа совершения преступления. – Х., 1984. – с. 5-20.

[2] Яблоков Н.П., Колдин В.Я. Криминалистика. Учебник. – М: МГУ, 1990. – с. 327.

Криміналістичне розуміння способу вчинення злочину відрізняє від кримінально-правового його тлумачення. Для криміналістів у способі вчинення злочинів на перший план виступають ті його інформаційні сторони (риси), що є результатом прояву зовні закономірностей відображення основних властивостей обраного способу досягнення злочинних цілей. У цьому зв'язку велику цінність представляють сліди, що вказують на те, яким способом злочинець здійснив наступне: потрапив на місце злочину, пішов з нього, переборов різного роду перепони, використовував своє службове становище, виконав намічену злочинну ціль, які підроблені документи, навики, знання і фізичні зусилля застосував, намагався (або не намагався) приховати сліди вчиненого діяння. Не менш істотні і сліди, що свідчать про характер зв'язку злочинця з предметом злочинного посягання та інше.

Саме такого роду ознаки, що виявляються зовні, дозволяють створити основу для найбільш швидкого розпізнання в початкових слідчих даних у справі того чи іншого характерного способу вчинення розслідуваного злочину навіть за окремими ознаками. Це відповідно дає можливість точніше визначити напрями і методи виявлення інших відсутніх даних про передбачуваний спосіб вчинення злочину і злочинця. При цьому з криміналістичної точки зору важливо не тільки виявити всі зовнішні прояви застосованого способу вчинення злочину, але й встановити, що в ньому було заздалегідь заготовлено правопорушником, а що з'явилося результатом пристосування до обстановки, що склалася на момент злочину. Ці дані дозволяють краще розібратися в механізмі вчинення злочину.

Структура способу вчинення злочину в криміналістичному та у кримінально-правовому значенні – категорія непостійна. В залежності від своєрідності винної поведінки, особливостей ситуацій, що виникають до і після вчинення злочину, та інших обставин вона може бути тричленною (що включає поведінку суб'єкта до, під час і після вчинення злочину), двочленною (у різних комбінаціях) і одночленною (характеризувати поводження суб'єкта лише під час самого злочинного діяння).

Значення встановлення способу вчинення злочину визначається важливістю завдань з його розкриття, доказування у кримінальній справі (ст. 64 КПК України), правильної кваліфікації, з'ясуванню обтяжуючих обставин, коли застосування способу пов'язане з участю в розкраданні організованої групи (п. 2 ст. 41 КК України).

Спосіб вчинення злочину враховується судом для індивідуалізації покарання винного, оскільки він характеризує не тільки самий вчинок, але й суб'єкта злочину. Все це обумовлює необхідність опису способу злочину в обвинувальному висновку та мотивувальній частині обвинувального вироку (ст. 223, 334 КПК України).

У криміналістичній літературі спосіб розкрадання прийнято вважати ключовим елементом криміналістичної характеристики, оскільки він в значній мірі визначає методику і тактику слідства, планування та організацію розслідування.

Способи вчинення банківських злочинів дуже різноманітні. В даний час поширення одержали розкрадання в банківській діяльності з використанням