**ЕКОНОМІКА,
ФІНАНСИ,
ПРАВО**

- ***П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк***
  КОНСОЛІДОВАНИЙ КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ, ВЧИНЕНИХ В БАНКІВСЬКІЙ СИСТЕМІ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк
  ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ФІНАНСОВИХ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Поливанюк
  ЗЛОЧИНИ В БАНКІВСЬКІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ СИСТЕМНИЙ АНАЛІЗ
- П. Біленчук, А. Кофанов, О. Кобилянський
  КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ
- П. Біленчук, А. Кофанов, О. Кобилянський
  КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНІВ, ВЧИНЕНИХ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ

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

КОНСОЛІДОВАНИЙ КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ, ВЧИНЕНИХ В БАНКІВСЬКІЙ СИСТЕМІ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

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

- Серія „Людина, право, суспільство”
- Серія „Економіка, фінанси, право”
- Серія „Безпека людини, суспільства, держави”
- Серія „Національна і міжнародна безпека”
- Серія „Міжнародне співробітництво”
- Серія „Мас-медіа”
- Серія „Криміналістична освіта XXI століття”
- Серія „Криміналістична наука в цивільному, 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

КОНСОЛІДОВАНИЙ КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ, ВЧИНЕНИХ В БАНКІВСЬКІЙ СИСТЕМІ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

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

КОНСОЛІДОВАНИЙ КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ, ВЧИНЕНИХ В БАНКІВСЬКІЙ СИСТЕМІ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

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 03.09.2010 року).

Рецензенти:
А.М. Гайдай – генеральний директор правничо-інформаційної компанії «Інтелект», Заслужений працівник освіти України
В.М. Салтинський – віце-президент Поліцейської фінансово-правової академії, Заслужений юрист України
Г.С. Семаков – завідувач кафедри правоохоронної діяльності Міжнародної академії управління персоналом, академік МКА, доктор юридичних наук, професор

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Поливанюк В.Д.
Б 61 Консолідований криміналістичний аналіз злочинів, вчинених в банківській системі з використанням сучасних інформаційних технологій. – Навчальний посібник / За ред. П.Д. Біленчука. – Київ: КИЙ, 2010. – 88 с. – (Серія „Економіка, фінанси, право").

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

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

Для студентів і викладачів юридичних навчальних закладів.

ББК 67.52я73

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.

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

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 трасологической 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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

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

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. Вашингтон. – Х., 2002. – Випуск № 6. – 308 с. – С. 234-260.

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

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

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

ПЕРЕДМОВА: БАНКІВСЬКА СИСТЕМА УКРАЇНА ЯК ОБ'ЄКТ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ (ПРАВОВІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ)

Сучасний розвиток української держави потребує розробки дієвих механізмів банківської безпеки, запровадження найбільш ефективних правових, організаційних і науково-методичних заходів запобігання, протидії та розслідування злочинних посягань у сфері банківської діяльності.

Сьогодні сфера фінансово-банківських відносин, часом через відсутнє правове регулювання нових видів діяльності, а також недосконаліть методик розслідування виявилася практично відкритою та незахищеною для незаконних посягань. У кредитно-фінансовій сфері широке розповсюдження отримали такі негативні явища як перелив неконтрольованих капіталів, «відмивання» кримінальних коштів, хабарництво, пов'язане з наданням кредитів, відкриттям розрахункових рахунків, прискоренням проведення банківських операцій, шахрайство з використанням фальшивої фінансової документації тощо. Подібний кримінал у банківській сфері не під силу одинакам. Тут частіше діє організована злочинна група, яка передбачає ланцюг учасників, детальну розробку сценарію, наявність повного технічного забезпечення та значних коштів. Тому в даному посібнику пропонується розглянути криміналістичну характеристику злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій, методи, засоби і тактичні прийоми розслідування даної категорії злочинів.

Необхідність прийняття невідкладних заходів щодо вдосконалення законодавства, розробки методики, тактики і стратегії розслідування злочинів, які вчиняються в банківській системі України, обумовлена тим, що сфера банківського капіталу, як показують новітні дослідження, стала в останні роки одним із самих криміногенних секторів як вітчизняної економіки, так і економіки більшості країн світу.

Узагальнення слідчої практики та аналіз стану наукових криміналістичних досліджень свідчать, що актуальність наукової розробки проблем методики розслідування злочинів, вчинених в банківській сфері України з використанням сучасних інформаційних технологій, викликана потребами експертної, слідчої та судової практики. Саме ці аргументи повною мірою свідчать про актуальність теми даного дослідження, про її науково-теоретичну, методичну і практичну значущість.

Емпіричну основу даного посібника склали результати опитування 152 слідчих ОВС України, 237 спеціалістів-випускників слідчої спеціалізації навчальних закладів системи МВС України і НЦБ Інтерполу в Україні за період з 1994 по 2009 рік, оприлюднені матеріали слідчої та судової практики зарубіжних країн. Було вивчено і узагальнено 3 кримінальні справи, досудове слідство за якими призупинено слідчими ОВС у Дніпропетровській та Київській областях на підставах і у порядку п.3 ст. 206 КПК України у 1995-2006 р., а також 5 кримінальних справ, розглянутих судами Запорізької,

Дніпропетровської, Київської областей за 1995-2006 р. У навчальному посібнику використаний досвід Центру дослідження проблем комп'ютерної злочинності.

Практичне значення результатів, відображених у посібнику, полягає в тому, що розроблені рекомендації та пропозиції можуть бути реалізовані: у науково-дослідній сфері – для подальшої розробки та вдосконалення теоретичних положень методики розслідування; у навчальному процесі – при вивченні дисциплін кримінального процесу, криміналістики, юридичної психології у вищих юридичних навчальних закладах, а також для підготовки відповідних навчально-методичних посібників і підручників.

Матеріали посібника можуть бути використані у навчальному процесі з дисциплін «Криміналістика», «Кримінологія», «Кримінальне право», «Оперативно-розшукова діяльність під час розслідування злочинів» та спецкурсів «Організація розкриття та розслідування злочинів», «Особливості розслідування злочинів, вчинених в економічній і фінансовій сфері».

злочинних посягань: Настільна 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.

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 Міжнародної конференції "Інформаційні технології та безпека" 23-27 червня 2003 р. м. Партеніт. – Київ: Інститут проблем реєстрації інформації НАН України, 2003. – Випуск 3. – С. 141-150.

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

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

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

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

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

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

204. Попович В.М. Правові основи банківської справи та її захист від

РОЗДІЛ 1
СИСТЕМНО-ІНФОРМАЦІЙНИЙ КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ТЕХНОЛОГІЧНИХ ЗАГРОЗ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

1.1. Правове регулювання автоматизації електронних розрахунків у банківській системі України

Банківська система України (БСУ) – один з найважливіших елементів фінансової системи держави. Сьогодні вся економіка України та її банківська система зазнають кардинальних змін, зокрема, вони торкаються структурної і функціональної її частини. Ці зміни забезпечуються новітнім банківським законодавством, розробка якого здійснюється на основі узагальнення міжнародного досвіду, досвіду економічних реформ в Україні, сучасних уявлень про суть та призначення банківських установ.

Економічна сутність банків характеризується специфічною функцією: виконувати на економічному ринку роль особливих фінансових посередників. Банки залучають вільні грошові кошти, які знаходяться в обігу 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 використання іншим.

Банк – це установа, функцією якої є кредитування суб'єктів господарської діяльності і 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 світу характеризується по-різному, але практично в усіх державах обов'язковим є закріплення в тій чи іншій формі як мінімум двох банківських функцій: кредитування та розміщення на банківських рахунках вкладів клієнтів [105, с. 52].

Саме система банків акумулює величезний фонд грошових коштів як в готівковій, так і у безготівковій формі. Але дотепер у науковій літературі ще не існує єдиного визначення поняття «банківська система», а підходи до цього питання обмежені здебільшого емпіричним рівнем оцінки.

Інколи банківська система ототожнюється або з кредитною системою, або із комерційними банками. У загальнонауковій літературі вказується, що банківська система характеризується як сукупність різних видів банків і банківських інститутів у їх взаємозв'язку, що існує в тій чи іншій країні в певний історичний період [247, с. 103]. Фахівці з банківської справи стверджують, що до складу банківської системи включаються кредитно-фінансові установи, які не є банками – фонди спеціального призначення, товариства взаємного кредитування, ломбарди, каси взаємодопомоги тощо [13, с. 12].

Банківська система є не лише механічним поєднанням банків певної країни. На думку Дзюблюка О.В., це складний фінансовий організм,

необхідність функціонування якого зумовлена цілим комплексом організаційно-економічних умов. В літературі **банківську систему** визначають як сукупність усіх банків країни, які взаємодіють між собою, підпорядковуючись встановленим нормам і правилам ведення банківської справи, з метою забезпечення можливості ефективного грошово-кредитного регулювання економіки, кредитно-розрахункового обслуговування господарського обороту, а також стабільної діяльності банківських установ [79, с. 71].

Таким чином, сутність банківської системи являє собою якісно новий, вищий рівень економічних відносин, який характеризується взаємодією банківських установ, визначаючи важливу роль в економіці держави. Разом з тим, у цьому визначенні упущені істотні правові складові банківської системи, які більш детально сформульовані в юридичній енциклопедії [268]. У ній банківська система характеризується як сукупність різних видів банків і банківських інститутів, за допомогою яких провадиться мобілізація коштів, надаються клієнтурі кредити та різноманітні послуги щодо прийому вкладів і надання кредитів. Ця система є внутрішньо організованою, взаємопов'язаною, має загальну мету і завдання. Відповідно до Закону України «Про банки і банківську діяльність» банківська система в нашій державі є дворівневою [90].

Банківська система України є одним з найбільш 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 фінансових 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 тощо) [127, с. 86].

Банківська система України складається з Національного банку України (НБУ) та інших банків, які створені і діють на території України.

Таблиця 1.

Кількість банків в Україні у 2002-2009 рр.

№	Назва показника	на 01.01. 2002 р.	на 01.01. 2003 р.	на 01.01. 2004 р.	на 01.01. 2005 р.	на 01.01. 2006 р.	на 01.01. 2007 р.	на 01.01. 2008 р.	на 01.01. 2009 р.
1	Кількість діючих банків, од.	152	157	158	165	165	170	178	184
2	Із них: з іноземним капіталом	21	20	19	23	23	35	35	34
3	У тому числі зі 100-відсотковим іноземним капіталом	6	7	7	9	9	13	13	12
4	Вилучено з Державного реєстру банків	9	12	8	4	1	6	1	4
5	Кількість банків, що перебувають у стадії ліквідації	35	24	20	20	20	19	15	10

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 внутр.справ: Харків, 2002. – С. 262-263.

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

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

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

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, налоговедческой, компьютерно-технической експертизы // Следователь. – 2002. – № 7. – С. 30-32.

З позиції Романа Чумака, Заступника Голови Правління АКІБ «УкрСиббанк»: «Кількість банків в Україні як і раніше залишається доволі великою: у 3 рази більше, ніж у Польщі, у 5 раз більше, ніж в Чехії, Угорщини та Румунії, у 9 разів більше, ніж в Словаччині та Словенії. Водночас у розрахунку на млн. мешканців кількість банків Україні знаходиться на рівні Чехії, Словаччини та Угорщини (країн в яких населення у 5-10 разів менше). У порівнянні з найбільш населеними країнами (Польщею та Румунією), Україна має в два рази більше банків на душу населення.

Враховуючи тенденції укрупнення та концентрації банківського бізнесу в Україні, кількість банків в Україні на кінець 2010 року може скоротитися до 90-100 одиниць».

Правові основи діяльності банків, порядок створення та основні принципи їх діяльності визначені Законами України «Про банки і банківську діяльність» [90] та «Про Національний банк України» [94].

Головною ланкою банківської системи України є Національний банк України (НБУ). Правове положення НБУ визначається Конституцією України (ст. 99, 100) [124], Законом України «Про Національний банк України» [94] та іншими нормативно-правовими актами.

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.

НБУ 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 НБУ 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.

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

Необхідно зазначити, що для виконання своїх адміністративно-контрольних функцій Національний банк України видає відомчі 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 [94, с. 56]. Національний банк встановлює єдині правила бухгалтерського обліку в банках на основі комплексної автоматизації і комп'ютеризації. Нормативні акти НБУ видаються у формі постанов правління НБУ, а також інструкцій, положень, правил, що затверджуються постановами Правління НБУ. Вони не можуть суперечити законам України та

іншим законодавчим актам України і не мають зворотної сили, крім випадків, коли вони згідно з законом пом'якшують або скасовують відповідальність.

Нормативно-правові акти НБУ підлягають обов'язковій державній реєстрації в Міністерстві юстиції України та набирають чинності відповідно до законодавства України. Нормативно-правові акти НБУ можуть бути оскаржені відповідно до чинного законодавства України.

Національний банк України активно займається нормотворчою діяльністю, готуючи закони, інструкції, положення, вказівки та інші документи нормативно-правового характеру, і врегульовує ними прогалини в правовому середовищі функціонування банківської системи України.

Існують різні види банків, які відрізняються формою власності, своїми функціями, організаційною структурою. За формою власності банки поділяються на державні, кооперативні, акціонерні, а залежно від операцій, які вони виконують, – універсальні та спеціалізовані. За організаційною структурою розрізняють банки, які мають широку мережу філій і такі, які їх не мають.

У ст. 47 Закону України «Про банки та банківську діяльність» визначені конкретні види операцій, які можуть здійснювати банки. Це, зокрема залучення та розміщення грошових внесків і кредитів; здійснення розрахунків за дорученням клієнтів, банків-кореспондентів та 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 гарантій та інших зобов'язань за третіх осіб, що передбачає їх виконання у грошовій формі, купівля у організацій і громадян, а також продаж валюти [90, с. 47].

З метою забезпечення гласності в роботі банків та доступності інформації про їх фінансовий стан, річні баланси, затверджені загальними зборами акціонерів, а також звіт про прибутки і збитки повинні публікуватися у пресі. 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 [62, с. 12].

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

Розрахунки між клієнтами одного й того самого банку відбуваються шляхом здійснення 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, у безготівковому порядку повинні

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

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

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

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

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

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

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

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.

розрахуватися їх банки.

Необхідно 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 [108, с. 139].

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 [211]. 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 приймання, передачі, опрацювання 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.

Згідно п. 7 ч. 1 ст. 7 Закону України «Про Національний банк України» 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 [94].

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 вдосконалюється.

У 1994 р. НБУ було прийняте стратегічне рішення щодо 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 (автоматизоване робоче місце-3 (АРМ-3); обласний рівень НБУ, куди передаються платіжні повідомлення від КБ, представлений регіональними розрахунковими палатами (РРП) і відповідно комплексом АРМ-2; найвищий рівень – 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 узагальнений 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 [87, с. 7].

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 вдосконалюється 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 базі 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, необхідно 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, котрі 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

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:

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.,

систем, а також можуть легко переноситись з однієї платформи на іншу [87, с. 7].

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» (Розділ 11) [210]. Впровадження такої системи дає змогу клієнтові спілкуватися з банком і виконувати платежі, не виходячи зі 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 [10, с. 125].

Необхідно 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 тощо. 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.

Більшість банківських завдань, що автоматизуються зараз, це переважно облікові, які можна віднести до класу завдань OLTP (On-line Transaction Processing). Дуже незначна частка в АБС належить аналітичним завданням типу OLAP (On-line Analyse Processing Systems), за допомогою яких вирішувалися б такі завдання, як аналіз ресурсів, активів, прибутковості, стану фінансових ринків, оцінка ризиків тощо. Майже відсутні в АБС завдання класу DSS (Decision Support Systems) підтримки 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 тощо.

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 змогу банкам оперативно управляти роботою філій та контролювати їх.

2. Забезпечення надійності збереження даних за рахунок наявності механізму підтримки трансакцій та реплікацій, який забезпечує цілісність і 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 і т.п.

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

Першою і основною вимогою, яка ставиться 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 ставиться 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 виконуватись 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 у будь-якому разі розробник АБС повинен вказати конкретні шляхи вирішення проблеми нарощення системи для того чи іншого банку.

У цілому система повинна мати можливість розширення як по

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.

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.

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 проведення. 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 у часовому вимірі мати повну картину фінансового стану банку;

– 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 зі спільною базою даних, що дає змогу уникнути дублювання та забезпечує цілісність й узгодженість даних. Функціональний зв'язок дозволяє використовувати спільні процедури, що зберігаються у відповідних бібліотеках (наприклад, нарахування процентних ставок тощо).

Забезпечення багатопрофільної 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 та цілісності технології. Виконання цієї вимоги в ідеальному варіанті – це забезпечення розподіленої обробки даних в режимі On-line. Забезпечення розподіленої обробки даних у 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 із 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 різних 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 завдань, а й відбувається перехід до нових програмно-апаратних засобів.

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

1.2. Криміналістична класифікація інформаційних загроз безпеки автоматизованих банківських систем.

Розробці методів захисту і визначенні класифікації сучасних загроз інформації в автоматизованих системах приділяється значна увага у роботах провідних вітчизняних і зарубіжних фахівців Вєртузаєва М.С., Голубєва В.О., Котляревського О.І., Кухарьонка М.А., Мєльникова В.В., Снігерьова О.П., Юрченка О.М. [18; 68; 166; 231]. В науковій літературі запропоновані різні визначення загроз в залежності від їх специфіки, середовища прояву, результатів їх впливу, нанесеного збитку тощо. Під **загрозами** варто 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 комп'ютерних, обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій та комп'ютерних систем сьогодні надається перевага технічним засобам обробки інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують надійний захист інформації. 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 несанкціонованого отримання, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіотеплової, акустичної розвідок [207].

У сучасних умовах насиченості життя різними технічними засобами діяльності, різними засобами зв'язку, різного роду допоміжними системами вкрай необхідно розуміти 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

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.

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.

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 доцільним є 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 клавіатури ПЕОМ, порушник технічного захисту інформації (ТЗІ) може зняти необліковану копію, ввести несанкціоновану інформацію, викрасти або модифікувати її програмне забезпечення, а також внести комп'ютерний вірус.

Маючи доступ до інформації на екрані дисплея і на роздруківках принтера, порушник ТЗІ може несанкціоновано ознайомитись з оброблюваною інформацією. Маючи засоби завантаження (клавіатуру, дискети, CD-ROM), порушник ТЗІ може модифікувати програмне забезпечення і внести 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 захищуваної 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 радіоканалами, приймача по каналам ПЕМВН, які несуть захищувану інформацію, можуть прийматися і декодуватися на спеціальних високочутливих приймачах на відстанях до 1-3 км від працюючої ПЕОМ [104, с. 60].

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 засобів завантаження, вводу-виводу інформації, до однієї частки інформації, а користується 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 проникнення комп'ютерного вірусу, активна деструктивна робота якого, як правило, починається з затримкою в часі, термін якого невідомий.

З боку санкціонованого користувача багато способів порушити роботу ІС та одержувати, модифікувати, поширювати або знищувати захищувану 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 і 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 захищуваної інформації.

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 [104, с. 13].

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

За наявності вільного доступу у приміщення можна візуально спостерігати інформацію на засобах відбиття 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 собою безконтрольне завантаження програмного забезпечення в ІС, в якому можуть бути змінені установки, властивості, дані, алгоритми, введено «троянську» програму або 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,

ВИКОРИСТАНА І РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. / Под ред. Р.С. Белкина. – М.: НОРМА-ИНФРА-М, 1999. – 990 с.

2. Аверьянова Т.В. Содержание и характеристика методов судебно-экспертных исследований. – Алма-Ата, 1991. – 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. Селиванов, 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.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом: привести свої нормативно-правові акти у відповідність із цим Законом; забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України В. ЮЩЕНКО
м. Київ, 31 травня 2005 року
№ 2594-IV

вагомість яких визначається та обмежується на дуже короткий або, навпаки, на тривалий час тощо [44, с. 21-22].

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

Процеси обробки, передачі та зберігання інформації апаратними засобами ІС забезпечуються спрацюванням логічних елементів на базі 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.

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 порушення цілісності інформації в обчислювальних мережах [104, с. 13].

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 та ультрафіолетовій частині спектра);

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

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.

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

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

Аналіз фізичної природи численних 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 безліч джерел небезпечного сигналу і відповідно безліч технічних каналів витоку інформації.

Джерелом утворення акустичного каналу витоку інформації є вібруючі тіла чи механізми, такі як голосові зв'язки людини, рухливі 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 [169, с. 15-16].

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.

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;

– високу оперативність одержання інформації;

– доступність реалізації;

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

Ці особливості визначають небезпеку даного каналу витоку інформації.

У практиці промислової розвідки широко використовується одержання інформації з відходів діяльності. У залежності від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти документів, що складаються, чернетки листів, магнітні носії, копірки тощо [169, с. 25].

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 підлягає 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 за хибним шляхом, тобто відбувається несанкціонована, випадкова модифікація інформації. В процесі подальшої обробки, в залежності від змісту та призначення хибної команди, можливі або передача інформації по хибному адресу, або передача хибної інформації

відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Обов'язки уповноваженого органу у сфері захисту інформації в системах виконує центральний орган виконавчої влади у сфері криптографічного та технічного захисту інформації.

Уповноважений орган у сфері захисту інформації в системах: розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції; визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації; здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Державні органи в межах своїх повноважень за погодженням з уповноваженим органом у сфері захисту інформації встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

інформації; власники системи; користувачі; уповноважений орган у сфері захисту інформації в системах.

На підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі - розпоряднику інформації.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Стаття 5. Відносини між власником інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат

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 зміні адреси пристрою – до несанкціонованого витоку інформації.

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 розподіляються 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 стосовно 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 ланцюг, 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 через збої 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 несанкціонованого доступу до інформації ІС [104, с. 16-17].

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

1.3. Правові, організаційні і криміналістичні засади протидії злочинам, вчиненим у банківській системі з використанням інформаційних технологій: міжнародний досвід.

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 в галузі інформатики відкривають нові можливості та сприяють поштовху до розвитку великих технологічних революцій. Сучасні комп'ютерні системи та технології збільшили загальний обсяг обробки інформації, з яким може працювати людство, на 7-8 порядків і довели його до 10^{25} біт.

Інформація, яка використовується 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 можливість 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 з 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,

доступу до неї;

власник інформації – фізична або юридична особа, якій належить право власності на інформацію;

власник системи – фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі – дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: власники

– здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом: привести свої нормативно-правові акти у відповідність із цим Законом; забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України Л. КУЧМА
м. Київ, 5 липня 1994 року
№ 80/94-ВР

3.2. Закон України „Про захист інформації в автоматизованих системах".

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права

наглухо зачиненій для людини, яка не має основ комп'ютерної грамотності.

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, вже зараз ЕОМ є багатообіцяючим знаряддям вчинення корисливих злочинів [42, с. 101].

Як підкреслюють вчені-криміналісти П.Д. Біленчук, В.О. Голубєв та М.А. Зубань, сьогодні як у вітчизняній, так і світовій криміналістичній науці все ще не існує чіткого визначення поняття комп'ютерного злочину, дискутуються різні точки зору з їх класифікації. Складність у 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 [62, с. 19].

Більшість фахівців поділяють 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.

Вищевикладене дозволяє нам зробити висновок, що під **комп'ютерною злочинністю** необхідно 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.

Поширення 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 вчинено 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 м. Чикаго (США), наприклад, 7 злочинців вирішили викрасти 70 млн. доларів і були затримані в той момент, коли мали на своєму рахунку більш ніж 49 млн. доларів [81, с. 31].

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 підлягаються 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 [42, с. 101].

Вивчення та узагальнення матеріалів НЦБ Інтерполу в Україні щодо 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 у 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 [29, с. 105].

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.

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 [29, с. 111].

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

Перші спеціальні закони щодо боротьби з комп'ютерною злочинністю

забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: власники інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

На підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі – розпоряднику інформації.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі – розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Стаття 5. Відносини між власником інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи,

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 [29, с. 60]. Згодом, поступово в багатьох країнах світу прийняті законодавчі акти стосовно цієї категорії злочинів.

В лютому 1986 року Бундестагом Німеччини було прийнято Другий Закон щодо боротьби з економічною злочинністю. Завдяки цьому було закладено правову основу 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. Цей закон було введено в дію 1 серпня 1986 року.

Федеральний закон ФРН про охорону даних зобов'язує установи і організації приймати необхідні технічні та 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.

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 [81, с. 34].

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

1. Декрет № 518 від 29.12.92 року «Використання положень Європейського Економічного співтовариства за № 91/250 щодо 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 [29, с. 109].

Франція має повний юридичний і кадровий 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 зі злочинами стосовно фальсифікації даних.

Прийнятий 5 січня 1994 року Закон „Godfrran", який було названо на честь його 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 стосовно комп'ютерної злочинності в Австралії були прийняті в 1979 році.

Сектор комп'ютерних злочинів (CCS) Австралійської федеральної поліції (АРР) , який був організований у 1989 році, виконує дві функції. Перша – збір розвідувальної (оперативно-пошукової) інформації про спеціальні комп'ютерні злочини та їх розслідування. Друга – забезпечення технічної

РОЗДІЛ 3
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ЕЛЕКТРОННИХ НОСІЯХ

3.1. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

витік інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

власник інформації – фізична або юридична особа, якій належить право власності на інформацію;

власник системи – фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі – дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі – користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

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.

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 здійснення 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 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.

В умовах усезростаючої комп'ютеризації й автоматизації передачі й збереження інформації особливого значення набуває захист даних, що існують в електронному вигляді.

Одним з нормативних актів, що регулюють порядок охорони такої інформації, є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [91], прийнятий у 2003 році, який прийшов на зміну Закону «Про захист інформації в автоматизованих системах» (прийнятий 5 липня 1994 року).

Метою цього Закону є встановлення основ регулювання правових відносин у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах з метою забезпечення дотримання права власності фізичних і юридичних осіб на інформацію та їх права доступу до неї, а також права власника інформації на її захист.

Найбільш важливими розділами Закону з позиції захисту інформації є розділ III «Організація захисту інформації в системі» і розділ IV «Відповідальність за порушення законодавства у сфері захисту інформації в системі».

Статті цих розділів визначають загальні вимоги і основні принципи щодо організації захисту інформації в системі та відповідальність за порушення

законодавства [91, с. 10-18].

Захист інформації в системі забезпечується шляхом:

– запровадження комплексної системи захисту інформації;

– дотримання суб'єктами відносин, пов'язаних з обробкою інформації в системі, законодавства України та нормативних документів у сфері захисту інформації в системі;

– використання засобів електронно-обчислювальної техніки, програмного забезпечення, телекомунікаційного обладнання, а також засобів захисту інформації у системі, які відповідають вимогам законодавства України щодо захисту інформації (наявність сертифіката, експертного висновку тощо).

Комплексна система захисту інформації повинна забезпечувати захист від несанкціонованого доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, захист якої гарантується державою, що обробляється в системі, в тому числі у мережі передачі даних, зокрема Інтернет.

Відповідальність за забезпечення ЗІ, яка є власністю держави, або інформації з обмеженим доступом, захист якої гарантується державою, що обробляється в системі, покладається на власника чи розпорядника системи.

Необхідно враховувати, що порядок створення та вимоги до комплексної системи ЗІ визначаються уповноваженим центральним органом виконавчої влади у сфері криптографічного та технічного захисту інформації – Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (ДСТС ЗІ СБУ).

Для створення комплексної системи захисту використовуються засоби, які мають відповідний сертифікат чи експертний висновок або дозвіл на їх застосування, виданий уповноваженим центральним органом виконавчої влади у сфері криптографічного та технічного ЗІ.

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,

(віддаленому) доступі через комп'ютерні мережі. Вони виникають у силу того, що система, через яку провадиться доступ, має деяку інформацію, що вона запитує в особи, яка намагається з'єднатися з іншим комп'ютером. Система визначає електронну адресу, використовуване програмне забезпечення та його версію. Крім того, при доступі в мережу, як правило, запитується адреса електронної пошти, реальне ім'я та інші дані. Цю інформацію запитує системний адміністратор (провайдер) для контролю обігів на його сервер і це також дозволяє ідентифікувати особу, що проникає в мережу.

Слідами, що вказують на незаконний доступ до ЕОМ, можуть бути: перейменування каталогів і файлів; зміна розмірів і вмісту файлів; зміна стандартних реквізитів файлів, дати й часу їх створення; поява нових каталогів, файлів тощо.

Подібну класифікацію щодо таких слідів розробив і М.В. Салтевський, який виділив такі два види слідів: механічні (по суті, традиційні) та енергетичні, які є результатом фізичного впливу електричного сигналу. Вони динамічні та становлять енергетичну зміну в конкретній точці магнітного носія [223, с. 12-14].

Аналіз наукових джерел, слідчої та судової практики дозволяє виділити такі можливі носії як традиційних, так і нетрадиційних слідів одночасно: 1) засоби електронної інформації, які містять інформацію в електронній формі; 2) документи.

ВИСНОВКИ, ПРОПОЗИЦІЇ, РЕКОМЕНДАЦІЇ

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

2. 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, а тому загрожує економічним основам як держави, так і світовій економічній системі. Зарубіжні та вітчизняні спеціалісти П.Д. Біленчук, В.Б. Вєхов, В.Д. Гавловський, В.О. Голубєв, М.В. Гуцалюк, В.Є. Козлов, В.В. Крилов, О.П. Снігерьов, В.С. Цимбалюк, С.С. Чернявський, М.Г. Шурухнов, О.М. Юрченко стверджують, що незаконне використання комп'ютерів дає більші прибутки з меншим ризиком, ніж пограбування банків, тому кількість таких злочинів з кожним роком буде зростати.

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

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

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

6. Організація інформаційно-технологічних систем на світовому рівні поряд з покращанням взаємодії ставить багато нових 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 контролем за 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.

7. Проведений на основі узагальнень вітчизняного та зарубіжного досвіду, класифікаційний аналіз інформаційних загроз безпеки в автоматизованих банківських системах України дозволив сформулювати систему правових, організаційних і криміналістичних методів, засобів та рекомендацій для протидії злочинам, які вчиняють у банківській системі з використанням сучасних інформаційних технологій.

дії можуть носити деструктивний характер у межах повноважень суб'єкта, що ініціює ці дії. Приклади слідів правомірних дій: зміна користувачем змісту файлу при коректуванні свого документа, автоматичне видалення коду вірусу з тіла програми програмою-монітором.

Якщо умови, перераховані вище, порушуються, сліди інформаційних взаємодій дій є слідами неправомірних дій. Приклади слідів неправомірних дій: видалення користувачем інформації з таблиці розділів, впровадження шкідливою програмою коду вірусу в тіло програми.

Особливістю слідів, що залишаються при незаконному доступі до ЕОМ є те, що вони, в основному, не розглядаються сучасною трасологією, оскільки в більшості випадків, носять інформаційний характер, тобто являють собою ті чи інші зміни в комп'ютерній інформації, що мають форму її знищення, модифікації, копіювання, блокування.

Виходячи з цього, матеріальні сліди вчинення даного виду злочинів (аналогічно до класифікації слідів вчинення комп'ютерного злочину наведеної В.О. Голубєвим [67, с. 146]) можна поділити на два таких види.

По-перше, традиційні сліди – це сліди в матеріальному середовищі (сліди-відображення, розглянуті трасологією, а так само сліди-речовини й сліди-предмети). Ними можуть бути які-небудь рукописні записи, роздруківки тощо, що свідчать про готування й вчинення злочину. Матеріальні сліди можуть залишитися й на самій обчислювальній техніці (сліди пальців рук, мікрочастинки на клавіатурі, дисководах, принтері), а також – на магнітних носіях і CD-ROM дисках. Однак необхідно зазначити, що особливістю технології вчинення злочинів у банківській системі, є те, що їх приховування пов'язане з легалізацією незаконно отриманих коштів. Тому важливе значення в методиці розслідування злочинів, які ми розглядаємо, мають сліди, що містяться у документах (на папері). Всі документи як джерела доказової інформації різнитимуться між собою об'єктивними властивостями, що містять доказову інформацію у справі. В одному випадку вони будуть доказувати своїм змістом, в другому – зовнішнім виглядом, в третьому – обставинами його виявлення [157, с. 103]. Тому інформація, яку містить документ, і буде, по суті, слідом вчинення злочину.

По-друге, нетрадиційні – це сліди в електронному середовищі, тобто, як стверджує В.О. Голубєв, інформаційні сліди, що утворюються в результаті впливу (знищення, модифікації, копіювання, блокування) на комп'ютерну інформацію шляхом доступу до неї і являють собою будь-які зміни комп'ютерної інформації, пов'язані з подією злочину. Насамперед, вони залишаються на магнітних носіях інформації й відображають зміни в інформації, що зберігається в них (у порівнянні з вихідним станом) [67, с. 145-146].

Інформаційними слідами є також результати роботи антивірусних і тестових програм. Дані сліди можуть бути виявлені при вивченні комп'ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм, а так само програмного забезпечення. Для виявлення подібних слідів необхідна участь фахівців.

Інформаційні сліди можуть залишатися й при опосередкованому

вирішення якої дозволить істотно доповнити існуючу класифікацію слідів і ознак. Разом з тим, розглядаючи файлову систему FAT, що працює під керуванням операційних систем DOS, WINDOWS, можна вибудувати кілька класифікацій слідів-відображень, пов'язаних з інформаційними взаємодіями.

За місцем розташування ці сліди можна поділити на сліди в системних ділянках файлової системи, файлах, сліди в кластерах.

Сліди в системних ділянках файлової системи поділяються на сліди в каталогах, у таблиці розділів, завантажувальних записах, сліди в таблицях розміщення файлів.

Сліди у файлах поділяються за статусом файлів у системі на сліди у файлах програм; сліди у файлах даних.

Сліди в кластерах поділяються за статусом кластерів у системі на сліди у «вільних» ("unused") кластерах, у «загублених» ("unassigned") кластерах і сліди в «зазорах» ("slack") кластерів.

За механізмом ініціації змін сліди можна поділити на сліди, ініційовані користувачем, і сліди, ініційовані програмою.

За складністю взаємодії об'єктів сліди можна поділити на сліди простої взаємодії, сліди комплексної взаємодії.

Сліди, ініційовані користувачем, програмою, мають такі особливості.

Сліди, ініційовані користувачем, виникають при будь-яких модифікаціях файлової системи або окремого файлу за командою користувача. Як правило, потрібне спеціальне дослідження для доказування того, що наявний слід був ініційований користувачем. У деяких випадках подібний висновок очевидний (наприклад, створений файл із ім'ям, що відображає участь користувача у створенні файлу).

Сліди, ініційовані програмою, виникають при будь-яких модифікаціях файлової системи або окремого файлу внаслідок автоматичної реалізації деякою програмою закладених у неї функцій при настанні певних умов. Наприклад, установка параметра «автоматичне збереження кожні 15 хвилин» у настроюваннях текстового редактора Word для Windows приведе до появи послідовності збережених файлів (у тому числі серед вилучених) з тимчасовими характеристиками, що різняться рівно на 15 хвилин.

Функціонування програмного забезпечення під управлінням операційної системи, особливості роботи програм, функціональне призначення програм і документів накладає певні обмеження на роботу користувача з документами й програмами, а також на виконання деяких програм. Багато дій у межах файлової системи покладені на строго визначені компоненти операційної системи, оскільки можуть привести до порушення складної взаємодії елементів файлової системи. Однак у межах файлової системи DOS і Windows існує багато можливостей втручання в структуру системи й порушення нормального режиму роботи програм.

У цьому сенсі будь-які дії, що ініційовані користувачем або програмами, можуть розглядатися як правомірні або неправомірні з погляду виконання діючих програмно-технічних обмежень і угод.

Сліди правомірних дій виникають за умови дотримання користувачем активною програмою діючих програмно-технічних обмежень і угод, зазначені

РОЗДІЛ 2
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ, ВЧИНЕНИХ У БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1. Загальні теоретичні положення криміналістичної характеристики злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій

Банківська система України є основою життєдіяльності нашої держави, оскільки вона пов'язана з накопиченням, розподілом і використанням державних і приватних коштів, і як свідчить кримінологічна статистика є однією з найбільш привабливих для окремих злочинців і особливо організованих злочинних груп. У даній системі на теперішній час вчинюється значна кількість різного роду фінансових афер, які вчинюються, частіше за все, при проведенні різних банківських операцій.

Для нормального функціонування економіки будь-якої держави в світі 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 і тисяч його клієнтів.

Найбільш привабливою сферою, яка широко використовується для відмивання кримінальних доходів, залишається банківська та кредитно-фінансова системи. При цьому широко використовуються міжнародні грошові розрахункові системи. Особливе занепокоєння правоохоронних органів України викликають високі темпи криміналізації банківської системи. За висновками фахівців Національного банку України, майже кожний третій український банк на сьогодні є проблемним. Банківська система перетворилася на центральну ланку технологічного ланцюга з відмивання капіталів, добутих злочинним шляхом.

Злочини, що вчиняються у 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 ст. 190 «Шахрайство», ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення», 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».

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 зведених даних для формування понять основних елементів криміналістичної характеристики комп'ютерних злочинів, вчинених у банківській системі.

Розвиток методики розслідування злочинів нерозривно пов'язаний з узагальненнями й аналізом теорії та матеріалів слідчої практики – основних джерел 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 методики розслідування злочинів визначеного виду набуває системний характер. Подальші розробки в цьому напряму привели до формулювання поняття «криміналістична характеристика злочинів», визначенню змісту її елементів [232, с. 29-30], а в подальшому перетворилось у важливу теоретичну концепцію науки криміналістики.

Свідченням визнання криміналістичної характеристики, як наукової категорії криміналістики, як відмічають О.Н. Колесниченко та В.О. Коновалова, було включення у 1984 році в програму курсу «Криміналістика» (для юридичних інститутів та університетів) самостійної теми «Криміналістична характеристика злочинів» [117, с. 7], без опису якої не обходиться зараз жодний підручник з криміналістики. Необхідно відмітити, що термін «криміналістична характеристика злочину» стосовно

його характеристики, відображають особливості створення інформаційного об'єкта й подальших впливів на нього. Істотною особливістю роботи комп'ютерних програм є, як правило, такий їх вплив на вміст файлу (документа), формат файлу і його характеристики, при якому інформація про вплив на файл у самій програмі не зберігається. Однак в окремих випадках така інформація може явно або латентно зберігатися.

Гносеологічний зміст поняття сліду злочину при розгляді злочинів з використанням документів на машинних магнітних носіях банківської інформації зберігається незмінним: слідом злочину є будь-яка зміна середовища (файлової системи), пов'язана з подією злочину. Оскільки файлова система являє собою сукупність особливих інформаційних одиниць – файлів, спеціальних службових таблиць (каталогів, таблиці розділів, таблиць розміщення файлів) і кластерів – ці зміни можуть виражатися в зміні місця розташування й вмісту файлів, зміні формату або характеристик файлів, створенні або видаленні файлів, зміні вмісту спеціальних службових таблиць (каталогів, таблиці розділів, таблиць розміщення файлів), зміні стану кластерів. При такому підході нам імпонує наукова точка зору В.С. Сорокіна, що визначає слід як різноманітні матеріальні зміни в навколишньому середовищі, пов'язані з вчиненим злочином. Ці зміни можуть виражатися в переміщенні предметів або речовин, відсутності або наявності їх у певному місці, втраті або придбанні яких-небудь властивостей [235, с. 3].

Відносно об'єктів матеріального світу термін «слідовідображення» має свою специфіку: його прийнято визначати в основному як відображення на одному матеріальному об'єкті зовнішньої будови іншого матеріального об'єкта, що можна виявити візуально (безпосередньо) або опосередковано, за допомогою технічних засобів. Результат взаємодії визначається за різницею між двома станами того самого об'єкту, яка спостерігається (фізичним, хімічним, біологічним тощо). При цьому власне акт відображення, хоча в цілому й підкоряється детермінованим фізичним законам, у деталях носить випадковий характер. Завдяки значній вірогідності складової, повнота, форма та особливості відображення в сліді ознак зовнішньої будови об'єкту носять багато в чому випадковий характер, що визначає, наприклад, неможливість точного, до дрібних деталей, відтворення моделі акту відображення.

Залучені до події злочину інформаційні об'єкти на машинних носіях позбавлені такої характеристики, як «зовнішня будова». Поділяючись на активні й пасивні (програми й дані відповідно), вони взаємодіють за алгоритмами, що закладені в активні об'єкти – комп'ютерні програми. Алгоритм комп'ютерних програм, будучи повністю детермінованим, визначає як характер і деталі змін, внесених у документи на машинних магнітних носіях інформації при впливі на них, так і характер і деталі змін, що вносить власні дані програми. У цьому змісті формат містить інші особливості файлу, які в будь-який момент часу визначаються сумою попередніх впливів програм на файл, і є своєрідним відображенням особливостей алгоритмів цих програм.

У цей час найбільш актуальна проблема збору емпіричних даних про сліди, пов'язаних з інформаційними взаємодіями в різних файлових системах,

працівниками установ, яким була завдана шкода, людьми, які достатньо добре знають режим роботи банківської 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 в комп'ютері, на їх робочих місцях. Це можуть бути дискети, магнітні диски, на яких злочинець зберігає потрібну інформацію, роздруківки, записи на аркушах паперу (шифри, паролі), викинуті папери в смітнику тощо.

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 фінансового моніторингу, захисту, і намагатись, щоб якомога менше осіб знали режим роботи банківської комп'ютерної системи. Практика свідчить, що коли менше обізнаних, то і менше коло підозрюваних.

Виходячи з вищевикладеного, інформація про зазначену обстановку є визначальною у криміналістичній характеристиці майже будь-якого злочину, який вчиняється в банківській системі, оскільки перетинається з даними про інші її елементи і виступає як своєрідний початок, що систематизує всі дані, у межах даної характеристики. Всебічно досліджена обстановка вчинення злочину багато в чому визначає і коректує спосіб вчинення злочину і значною мірою позначається на особливостях і структурі механізму його вчинення. В ній виявляються окремі важливі особистісні риси злочинця, що формує (частково або цілком) дану обстановку, який у тирчи іншій мірі пристосовується до неї або використовує її без якогось пристосування, а іноді і без врахування її особливостей.

«Слідова картина» злочинів, вчинених у банківській системі з використанням інформаційних технологій. Дані про сліди незаконного доступу до ЕОМ є найважливішим елементом криміналістичної характеристики злочину. Під слідами злочину розуміються будь-які зміни середовища, що виникли в результаті вчинення в цьому середовищі злочину [22, 39]. Сліди як джерело інформації про злочинця та його дії при вчиненні злочину становлять самостійну категорію об'єктів криміналістичної ідентифікації [22; 113; 114; 179; 235; 254]. Розробляючи загальну класифікацію слідів і класифікацію ознак, що відображаються в сліді при різних сполученнях слідоутворюючих і слідосприймаючих об'єктів, вітчизняні вчені створили криміналістичне вчення про механізм слідоутворення, теоретичні положення якого докладно описані в криміналістичній літературі.

На відміну від звичних і типових криміналістичних об'єктів, середовищем існування документів на машинних магнітних носіях банківської інформації є файлова структура, створена за допомогою системного програмного забезпечення та підпорядковується заздалегідь відомим алгоритмам взаємодії інформаційних об'єктів. Формою існування цих документів є особливий інформаційний об'єкт – файл, що має фіксовану структуру (формат) та криміналістично значущі характеристики, які підтримуються операційною системою. При цьому як формат файлу, так і

предмету методики розслідування злочинів фігурує у теоретичній, методичній та навчальній літературі з криміналістики [240, с. 95].

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 [164, с. 280-282].

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 юридичній літературі є велика кількість різноманітних визначень поняття криміналістичної характеристики [133]. Усі вони в основному відображають дві точки зору. Відповідно першій з них, криміналістична характеристика складає систему тих чи інших ознак злочину. І.І. Артамонов зазначає, що це науково розроблена система найбільш суттєвих, типових криміналістичних рис, якостей, ознак певної категорії злочинів, В.А. Гуняєв – система сталих ознак певного виду (підвиду) злочину [76, с. 58-61], та інші автори.

Інша точка зору полягає в тому, що криміналістична характеристика злочину може бути представлена як типова інформаційна модель [129, с. 38], системи відомостей (інформації) про криміналістично значущі ознаки злочину, інформаційної моделі події [161], система інформації про розслідуваний злочин, що має кримінально-правове і процесуальне значення [4, с. 180].

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

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

Елементи криміналістичної характеристики злочинів розкривають їх основні риси. Слідча практика, результати наукових досліджень криміналістичної сутності злочинів показують, що незалежно від виду злочину криміналістично значимі їх ознаки в характеристиці виду й окремого злочину частіше за все можуть міститися в даних про спосіб, механізм й обстановку вчинення злочину, типологічні та інші особливості їх суб'єктів тощо. Водночас для окремих видів, груп злочинів з урахуванням криміналістичних потреб зазначені ознаки можуть міститися у відомостях

про предмет злочинного зазіхання, особу потерпілого, своєрідності діяльності організованої злочинної групи, мотивах злочину, характері злочинних наслідків, що наступили тощо.

Виходячи з викладеного, структура криміналістичної характеристики злочинів складна, але різна 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.

Теоретичні положення загальної криміналістичної характеристики злочинів були також розроблені Р.С. Бєлкіним, А.Н. Васильєвим, В.Г. Гавло, І.Ф. Герасимовим, В.Г. Гончаренком, Г.А. Гуртовим, В.А. Журавлем, Н.І. Клименко, О.Н. Колісниченком, В.О. Коноваловою, В.К. Лисиченком, В.Г. Лукашевичем, Г.А. Матусовським, В.А. Образцовим, М.В. Салтевським, М.Я. Сегаєм, В.Ю. Шепітьком, М.П. Яблоковим та іншими вченими.

Більшість авторів включає як її елементи сукупність окремих ознак, що визначають: 1) спосіб вчинення злочину; 2) механізм злочину; 3) обстановка вчинення злочину; 4) особу злочинця; 5) особу потерпілого; 6) об'єкт (предмет) злочинного посягання; 7) мотив і мета злочину; 8) закономірності злочинів [129, с. 39-50; 132, с. 48-56; 163; 232, с. 34-41; 240].

Становлять інтерес судження В.П. Корж, яка, досліджуючи поняття й структуру криміналістичної характеристики економічних злочинів, що вчинюються організованими злочинними групами (ОЗГ), виділяє їх особливості, специфіку, ознаки, обстановку вчинення злочину, сліди та інші наслідки зазначених злочинів [125, с. 107].

Н.Г. Шурухнов визначає криміналістичну характеристику злочину як відображення системи криміналістичних рис, властивостей, ознак злочину, що відобразилися в об'єктивній дійсності. Він відзначає, що криміналістична характеристика містить дані про типові способи вчинення й приховання злочину, механізм злочинного зазіхання, сліди, обстановку, в якій готувалася й відбувалася злочинна подія, предмет злочинного зазіхання, риси особистості злочинця й потерпілого, а так само обставини, що сприяють вчиненню злочинів [260, с. 119].

На думку фахівця в галузі комп'ютерної злочинності В.Б. Вєхова до структури криміналістичної характеристики необхідно включати криміналістично значимі дані про особу правопорушника, мотивацію й мету його злочинної поведінки, а також дані про потерпілу сторону [37, с. 28.]

Заслуговує на увагу точка зору криміналіста і фахівця в галузі інформаційних технологій В.Є. Козлова. Він під криміналістичною характеристикою комп'ютерних злочинів розуміє найбільш характерну, криміналістично значиму взаємозалежну інформацію про ознаки та властивості такого роду злочинів, здатну бути підставою для висування версій про подію злочину й особу злочинця [112, с. 114].

Більшість вітчизняних і закордонних вчених єдині в тому, що криміналістична характеристика є важливим елементом структури криміналістичної методики розслідування злочинів, вчинених у банківській

комп'ютер вірусу найчастіше списується на ненавмисну помилку користувача, який не зміг його «відловити» при спілкуванні із зовнішнім комп'ютерним світом.

Механізм вчинення злочинів, пов'язаних з автоматизованими системами обробки інформації, та його наслідки 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 в банківській сфері дуже часто не зацікавлені посадові особи, в обов'язки яких входить забезпечення комп'ютерної безпеки самого банку. Визнання факту несанкціонованого доступу в підвідомчу їм систему ставить під сумнів їх професійну кваліфікацію, а неспроможність заходів з комп'ютерної безпеки, що приймається керівництвом, може призвести до серйозних внутрішніх ускладнень або і звільнення з посади.

Що стосується банків, які постраждали від електронних атак, 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 банківської установи, може призвести до втрати клієнтів, коштів тощо.

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 озвучувати, розголошувати це не вигідно, то керівники фінансових організацій, в яких вчинюються комп'ютерні злочини, свідомо приховують їх.

Все це призводить до того, що небажання повідомити про злочин, свідоме приховування його, сприяє знищенню слідової картини, яка і так є дуже скромна і достатньо латентна. 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 атак. Достатньо набрати відповідну команду, і комп'ютер виведе на дисплей всю необхідну для нас інформацію. Але злочинець може проникнути в чужий комп'ютер шляхом пошуку слабких місць, «дірок» у захисті системи, в цьому випадку несанкціонованого доступу зафіксовано в системі не буде. Та при всій своїй обережності в роботі з інформацією, все ж таки інколи залишаються окремі сліди, але деколи це може бути якось 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 конкретно завдана матеріальна шкода. Але в багатьох випадках її достатньо важко визначити, оскільки у великих банках, як правило, могутні потоки обігових коштів.

Левова частка комп'ютерних злочинів, в основному, вчинюється

Додатковими факторами, що характеризують обстановку вчинення неправомірного доступу до банківської комп'ютерної інформації можуть бути: наявність і стан засобів захисту комп'ютерної техніки (організаційних, технічних, програмних), дисципліна, що склалася на об'єкті, вимогливість з боку керівників щодо дотримання норм і правил інформаційної безпеки й експлуатації ЕОМ тощо.

Для обстановки, у якій можливе вчинення розглянутого злочину найбільше властиво таке: невисокий техніко-організаційний рівень господарської діяльності, низький контроль за інформаційною безпекою, не налагоджена система захисту інформації, атмосфера байдужності до випадків порушення вимог інформаційної безпеки тощо.

Виявлення особливостей сформованої обстановки дозволяє швидше визначити, на що варто звернути особливу увагу при огляді місця події, вивченні комп'ютерного обладнання й документів, виклику і допиті конкретних свідків та вирішенні питань про необхідність вилучення певних документів тощо.

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 із самих різних носіїв і джерел криміналістичної інформації. Виявлення і дослідження подібної інформації, особливо на початку розслідування, як правило дозволяють зібрати істотні дані про виниклу до й у момент події кримінальну ситуацію. Зокрема за такого роду автономними слідами частіше можна одержати такі дані:

– 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 прихованню 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 й інше [132, с. 53].

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 виглядає набагато скромніше, аніж при пограбуванні продуктового магазину, або деколи і зовсім є непомітний, латентний. Видимого матеріального збитку, завданого електронним злодієм зовні взагалі не видно. Наприклад, незаконне копіювання інформації частіш за все залишається невиявленим, введення в

системі з використанням ЕОМ.

Порівнюючи різні визначення криміналістичної характеристики, можна зробити висновок, що більшість вчених-криміналістів, які вивчають економічні злочини, відзначають такі елементи криміналістичної характеристики: предмет злочинного посягання; типові слідчі ситуації; способи підготовки, вчинення та приховування злочину; типові ідеальні та матеріальні сліди злочину; дані про характеристику особи злочинця й потерпілого.

Зазначений вище підхід дозволяє виділити ряд існуючих сьогодні проблемних питань у процесі формування криміналістичної характеристики незаконного втручання в роботу ЕОМ:

– висока латентність злочинів у сфері використання електронно-обчислювальних машин. Так В.С. Цимбалюк відзначає, що основною її причиною є те, що в більшості випадків, через небажання підриву репутації, потерпілі неохоче повідомляють правоохоронним органам про факти злочинних зазіхань на їх комп'ютерні системи [250, с. 178];

– складність збору доказів на досудовому слідстві та процесі доказування в суді;

– як правило, трансрегіональний, транскордонний, міжнародний характер даного виду злочину;

– досить широкий спектр криміналістично значимих ознак комп'ютерних злочинів;

– відсутність чіткої програми боротьби з комп'ютерними злочинами як в Україні, так і в цілому світі;

– складність самого процесу розслідування комп'ютерних злочинів;

– відсутність достатньої слідчої практики щодо розслідування комп'ютерних злочинів, вчинених у банківській системі.

Злочини в сфері комп'ютерної інформації банківської системи відомі відносно недавно. Вітчизняна практика розслідування таких злочинів поки що не дуже велика, 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 й ін. Суспільна небезпека злочинних дій у зазначеній сфері стає усе більш очевидною і досвід формалізації законодавцем головним чином закордонних криміналістичних знань про «комп'ютерні злочини» відбувається на наших очах.

Недоліки правової регламентації в даній сфері 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 зробити детальна розробка особливостей криміналістичної характеристики злочинів, вчинених у банківській системі з використанням сучасних інформаційних технологій.

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

Проведене нами дослідження дозволяє зробити висновок, що основними елементами криміналістичної характеристики злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій є такі: предмет злочинного посягання; способи підготовки, вчинення та приховування злочину; особа злочинця; обставини вчинення злочину; «слідова картина».

Розглянемо їх більш детально.

Предмет злочинного посягання. 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 [9, с. 31].

В залежності від виду злочину, предмет злочинного посягання неоднаковий. Проведений нами аналіз чинного законодавства дозволяє зробити висновок, що 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 і мереж електрозв'язку (ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», ст. 361-1. «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361-2. «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється», ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»).

Більш близьким криміналістичному поняттю об'єкта злочину – є

Вінницького обласного управління НБУ, вступив у злочинну змову з Роговим Г.К., з метою таємного викрадення з Вінницького обласного управління НБУ державних грошових коштів в особливо великих розмірах, та спільно з ним розробив загальний план вчинення злочину. Згідно цього плану Коломєєц С.А. повинен був підробити електронні платіжні документи, а Рогов Г.К. – підшукати осіб, які б перевели викрадені безготівкові кошти в готівку.

Незаконне вилучення грошових засобів з Вінницького обласного управління НБУ проводилось шляхом формування Коломєйцем на службовому комп'ютері, який був підключений до локальної комп'ютерної мережі Вінницького обласного управління НБУ, фіктивних платіжних документів, якими зі спеціального рахунку, використовуючи систему електронних платежів, безготівкові грошові кошти у сумі 80 435 006 грн. перераховувались з банку на рахунки підприємств, керівники яких за матеріальну винагороду повинні були їх прийняти, частково перевести в готівку, проконвертувати, а також перерахувати на рахунки підприємств за межами України. До кримінальної відповідальності по цій справі було притягнуто 29 осіб [142].

Спираючись на результати вивчення кримінальних справ, можна дійти висновку, що для заволодіння грошима шляхом перерахування їх з одного рахунку банку на інший за ознакою стійкості злочинної спрямованості такі групи створюються як тимчасове об'єднання на період вчинення конкретного злочину.

Обстановка вчинення злочину. 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 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, тижня, місяця, місця вчинення злочину, наявності поблизу житлових, виробничих та інших об'єктів тощо). Визначені ознаки обстановки використовуються як основа 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, в приміщеннях і поза житловими помешканнями тощо) [129, с. 47].

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 та 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 [132, с. 51].

Обстановку вчинення незаконного доступу до ЕОМ банківської системи, на наш погляд, становлять речові, технічні, просторові, тимчасові, соціально-психологічні обставини вчинення розглянутого злочину. Особливістю даного злочину, як втім, й інших комп'ютерних злочинів є те, що на нього практично не впливають природнокліматичні фактори.

Потрібно підкреслити, що характерною особливістю злочинців цієї групи є відсутність у них чітко виражених протиправних намірів. Практично всі дії вчинюються ними з метою демонстрації своїх інтелектуальних можливостей.

Необхідно враховувати, що на даному етапі комп'ютерні злочини в банківській сфері переважно вчиняються 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 у подальшому, легалізувати та пустити в обіг тощо.

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

Частіше за все зазначені особи не тільки добре знають банківську систему, 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 зазвичай добре освічені економісти, юристи, оперативні працівники банків різного посадового рівня, програмісти й оператори комп'ютерів [269, с. 42].

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.

Криміналістичні аспекти боротьби з організованою злочинністю, зокрема її економічними різновидами, отримали належну увагу науковців досить нещодавно [183, с. 237]. Також цією проблемою спільно займались криміналісти М.М. Шилан, Ю.М. Кривоніс, Г.М. Бірюков [259, с. 22]. Автори зазначають, що ОЗГ існує, як багаторівнева система, яка складається з різних ланок. Основним принципом організації таких груп є ієрархічність. Місце керівника групи визначається на підставі різних якостей, притаманних його особистості.

Залежно від способу вчинення злочину у банківській системі з використанням сучасних інформаційних технологій до складу ОЗГ можуть входити: 1) організатори; 2) працівники обліку та контролю – бухгалтери, працівники відділів банку, що контролюють платежі; 3) керівники власних комерційних структур, їх бухгалтери або особи, які виконують їх роль; 4) рядові виконавці [162, с. 26].

Прикладом вчинення злочину у складі ОЗГ може бути така кримінальна справа. Коломєєц С.О., технік сектора опрацювання задач «операційний день банку», регіональної розрахункової палати центру інформатизації та платіжних систем

кримінально-правове поняття предмету злочину. Під предметом злочину розуміються речі матеріального світу, впливаючи на які, особа посягає на ті або інші суспільні відносини [179, с. 38].

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 зазіхання обумовлена насамперед тим, що вплив злочинця на цей об'єкт сполучено 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 [129, с. 41].

Як свідчить слідча та судова практика розслідування даної категорії кримінальних справ, до основного предмета можуть належати кошти у готівковій та безготівковій формі, матеріальні цінності [48, с. 40]. Спочатку зазначимо, що в юридичній літературі під матеріальними цінностями розуміють будь-яку річ, яку 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 [27, с. 30].

Безпосередню увагу привертає крадіжка грошових коштів у фінансовій сфері за допомогою інформаційних технологій. Потрібно зауважити, що в даній ситуації викрадаються кошти, не у звичному для нас розумінні, а безготівкові, які обертаються в системі електронних платежів. Під безготівковими коштами розуміють записи грошових сум на рахунках у центральному банку, його відділеннях, комерційних банках. 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 базі персональних комп'ютерів до повноцінних автоматизованих банківських систем та баз даних, що відповідають самим суворим сучасним вимогам. Активно впроваджуються міжнародні системи електронних 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 змогу змінити кількісне вираження певного рахунку. Потім особа має різні можливості використати ці, начебто, неіснуючі електронні 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 електронних пластикових платіжних засобів в Україні зумовлені взаємною зацікавленістю в цьому держави, банківської системи 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 у руках того, хто нею користується. Платіжна картка може використовуватися для заволодіння матеріальними цінностями. У цьому випадку злочинці не знімають з картки готівкові кошти, а використовують її як засіб розрахунку в торгівельних точках, де встановлені імпринтери (пристрої для зчитування інформації з картки для подальшого зняття з банківського рахунку необхідної суми). Крім цього, матеріальні цінності можна викрасти шляхом укладання договорів купівлі-продажу з віртуальними магазинами в мережі Інтернет. Злочинець використовує інформацію чужої банківської картки для замовлення певного товару через Інтернет. Прикладом такого злочину може бути кримінальна справа № 70001130, порушена 04.08.2000 року відносно громадян України Лопаткіна Д.Б., 1976 р.н., Савірського В.В., 1976 р.н., Козінця Ю.П., 1961 р.н. Встановлено, що зазначені громадяни протягом 1999-2000 років шляхом несанкціонованого проникнення до мережі Інтернет, незаконного списання з кредитних пластикових карток здійснювали крадіжку грошових коштів з рахунків комерційних банків («Приватбанк», м. Дніпропетровськ, АППБ «Аваль», м. Київ, «Парексбанк», м. Рига (Латвія).

У ході проведення трансакції, зазначені громадяни здійснювали замовлення товарів у віртуальних магазинах різноманітних компаній, розташованих в США, Ізраїлі, Англії та отримали через поштові установи товарно-матеріальні цінності, які використовували у своїх цілях [143].

Таким чином, практика діяльності фінансових установ світу і слідча практика дозволяють стверджувати про реальну латентну ймовірність крадіжки за допомогою інформаційних технологій саме безготівкових грошей, як предмету даного виду злочинного посягання, який має принципово важливе значення у криміналістичній характеристиці, оскільки чинить безпосередній вплив на інші її елементи, зокрема виступають умовою певних способів вчинення та приховування злочину, властивостей особи злочинця.

Способи підготовки, вчинення та приховування злочину. Найважливішим і визначальним елементом криміналістичної характеристики будь-якого злочину є сукупність даних, що характеризують способи його підготовки, вчинення та приховування.

Способи підготовки, вчинення та приховування злочину є об'єктом вивчення ряду наук кримінального циклу: кримінального права, кримінального процесу, кримінології, криміналістики тощо. Кримінально-правове поняття способу, що розробляється на основі кримінального закону, є базовим для інших наук [187, с. 5-20].

Криміналістично значима інформація про способи підготовки, вчинення та приховування злочину в значній мірі є модальною, а її конкретні носії і

серед них постійно збільшується й частка жінок. Це пов'язане з професійною орієнтацією деяких спеціальностей і робочих місць, орієнтованих на жінок (секретар, бухгалтер, економіст, менеджер, касир, контролер тощо), обладнаних ЕОМ та з доступом у мережу Інтернет.

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 озброєні спеціальними знаннями і найновішими технологіями, мають доступ до комп'ютерних систем.

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

Проведені дослідження показують, що безпосередній несанкціонований доступ до ЕОМ, систем та комп'ютерних мереж, як правило, самими 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.

Так, у червні 1994 року ведучий інженер-комп'ютерник регіонального управління Промінвестбанку м. Дніпропетровська Таранов О.В., маючи доступ до електронної системи «Трезор» (охоронна система входження в комп'ютерну мережу банку), вступив у злочинну змову із заступником директора фірми «АКС» м. Дніпропетровська Аляб'євим В.Л. з метою вчинення розкрадань грошових коштів в особливо великих розмірах, скопіював на свою дискету програму «Трезор» і за допомогою власного комп'ютера, встановленого у його квартирі, увійшов в локальну комп'ютерну мережу Промінвестбанку. Сформувавши фіктивний платіж розміром 864 млн. карбованців, він «вклав» його у «поштову» скриньку комп'ютера Промінвестбанку для відправки на раніше обумовлений рахунок Дніпропетровської фірми «Вік-Сервіс» в обласному відділенні Укрексімбанку через електронну пошту облуправління Національного банку України. Після зарахування вказаної суми на розрахунковий рахунок «Вік-Сервіс» Таранов та Аляб'єв були затримані при спробі розпорядитися викраденою сумою [29, с. 114-115].

«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 важкої задачі «злому» захисту програмного продукту чи створення комп'ютерних вірусів тільки для того, щоб потішити свою самозакоханість, пожартувати. «Хакери» відрізняються високим професіоналізмом в поєднанні зі специфічним комп'ютерним фанатизмом.

намітилися два специфічних напрями. Перший передбачає одержання даних про особу невідомого злочинця з урахуванням виду, місця і часу вчинення діяння, предмета зазіхання за залишеними ним слідам на місці злочину, у пам'яті свідків та за іншими джерелами. Це дозволяє вірніше визначити напрями і прийоми його розшуку та 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 характеристики особи. 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 особу 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 [132, с. 54-55].

Серед осіб, що вчинюють названі злочини, достатньо високий рівень професійних знань.

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.

Проведений аналіз вітчизняних і зарубіжних досліджень дозволяє намалювати орієнтовний портрет типового комп'ютерного, електронного злочинця, тобто виявити 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.

Дослідження, проведені Центром дослідження комп'ютерної злочинності показали, що вік 33% зловмисників на момент вчинення злочину не перевищував 20 років; 54% – від 20 до 40 років; 13% – були старше 40 років [58].

Злочини, пов'язані з незаконним доступом до ЕОМ в 5 разів частіше вчинюються особами чоловічої статі. Більшість суб'єктів таких злочинів мають вищу або незакінчену вищу технічну освіту (53,7%), а також іншу вищу або незакінчену вищу освіту (19,2%) [29, с. 123]. Але останнім часом

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 розслідування злочину.

Під способом підготовки, вчинення та приховування злочину в криміналістичному змісті 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 злочинного поводження правопорушника, його окремих особистісних даних і відповідно визначити найбільш оптимальні методи вирішення завдань розслідування злочину [271, с. 327].

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

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 відбитка основних властивостей обраного способу досягнення злочинних цілей. У цьому зв'язку велику цінність представляють сліди, що вказують на те, яким способом злочинець потрапив на місце злочину, що робив на місці злочину, яким шляхом пішов із нього, як переборов різного роду перепони, як використовував своє службове положення, як виконав намічену злочинну ціль, які підроблені документи, навики, знання і фізичні зусилля застосовував, чи намагався (або не намагався) приховати сліди вчиненого діяння тощо. Не менш істотні і сліди, що свідчать про характер зв'язку злочинця з предметом злочинного зазіхання тощо.

Саме такого роду ознаки, що виявляються зовні, дозволяють створити основу для найбільш швидкого розпізнання в початкових даних, отриманих слідчим у справі про особливості того чи іншого характерного способу вчинення розслідуваного злочину навіть за окремими специфічними його 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 продумано, заготовлено правопорушником, а що з'явилося результатом пристосування до конкретної ситуації, обстановки, що склалася на момент безпосереднього вчинення злочину. Ці дані дозволяють слідчому і суду краще розібратися в механізмі вчинення розслідуваного злочину.

Структура способу вчинення злочину в криміналістичному, та й у

кримінально-правовому змісті – категорія непостійна. В залежності від своєрідності винної поведінки, особливостей ситуацій, що виникають до, в момент і після вчинення злочину, та інших обставин, що їх характеризують вона може бути триланковою (що включає поведінку суб'єкта до, під час і після вчинення злочину), дволанковою (у різних комбінаціях) і одноланковою (характеризувати поведінку суб'єкта лише під час самого злочинного діяння).

Значення встановлення способу вчинення злочину визначається важливістю завдань з його розслідування, способів доказування у кримінальній справі (ст. 64 КПК України), правильної кваліфікації злочину, з'ясуванню обтяжуючих обставин, коли застосування способу пов'язане з участю в розкраданні організованої групи (ст. 28 і п. 2 ст. 41 КК України).

Необхідно мати на увазі те, що спосіб вчинення злочину враховується судом для індивідуалізації покарання винного, оскільки він характеризує не тільки сам вчинок, але й суб'єкта злочину. Все це обумовлює необхідність опису способу вчинення 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 досудового слідства, планування та організацію процесу розслідування [117; 163; 167; 213].

Способи вчинення злочинів у банківській сфері дуже різноманітні. Відповідно до нашого предмету дослідження розглянемо більш детально ті з них, що вчинюються в банківській системі з використанням сучасних інформаційних технологій.

В даний час особливого поширення набули розкрадання в банківській діяльності з використанням електронно-обчислювальних машин (ЕОМ) або комп'ютерних мереж. Цей вид розкрадання характеризується тим, що злочинці, скориставшись професійною та службовою можливістю для неправомірного доступу до комп'ютерної інформації фінансового характеру, зосередженої в обчислювальних центрах банківських установ, і виявивши недоліки, прогалини в діяльності ревізійних служб, проводять кримінальні операції з зазначеною інформацією, що знаходиться в ЕОМ або на її машинних носіях.

На сьогоднішній день основні способи вчинення комп'ютерних злочинів у банківській системі можна умовно поділити на чотири 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

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 наступне 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 нього – важливим елементом криміналістичної характеристики злочину.

Питання, пов'язані з вивченням особи злочинця розроблялися М.Т. Ведерніковим та В.Г. Танасевичем в криміналістиці протягом тривалого часу [36; 234].

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) не змінні 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 не однорідні. 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 виникаючі 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 відбивають 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 як правило відносять соціальну і професійну приналежність, освітній рівень, посадове становище, трудові функції, захоплення, спосіб життя, схильності, інтереси, наявність або відсутність фізичних вад, психічних аномалій, що виникнули з тих чи інших причин у процесі життєдіяльності (в результаті самоосвіти, трудової діяльності, вчинення злочинів, захворювань тощо).

З погляду формування криміналістичної характеристики злочинів також важливе врахування ознак, виникнення яких пов'язано з підготуванням і вчиненням злочину, подальшими діями злочинців. Серед цих ознак особливо виділяються 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) [129, с. 40].

У криміналістичному значенні вивчення особи злочинця в даний час

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 розміщується аркуш паперу відповідного розміру, що перешкоджає друку 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 «кодуючих 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 характерно 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 отримання 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 й 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 [269, с. 36].

Реальну загрозу банківській 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.

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

Класифікація окремих особливостей особи допомагає встановити, який контингент більш прихильний до вчинення тих чи інших злочинів, вчиненню яких злочинних діянь частіше властивий рецидив, а які мають випадковий

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 [27, с. 23].

Розглянемо кожну з груп більш детально.

1. Способи перехоплення інформації:

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

1.2. Електромагнітний перехват. Використовуються пристрої, які перехоплюють інформацію та працюють без прямого контакту. 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.

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, установки 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.

Так, Б., працюючи в АКБ «Україна» в с. Кіровське АР Крим на посаді старшого інженера-програміста зі супроводження комп'ютерного забезпечення АС банківського обслуговування «Сарс-Сбон» здійснював зняття грошей та зарахування їх на власний рахунок, які потім отримував у

касі названого банку за спеціально розробленою схемою. Робоче місце Б. було в одному приміщенні з робочим місцем касира банку, до обов'язків якого належало нарахування грошей на рахунки працівників банку. Злодій помітив, що касир часто виходить з приміщення, залишаючи свою ЕОМ в АС банку в робочому стані. В такі моменти Б. з корисливих мотивів, використовуючи ЕОМ касира, незаконно втручався до системи електронних розрахунків і з розрахункового рахунку АКБ «Україна» та рахунків клієнтів банку перераховував на власний рахунок у цьому самому банку певну суму грошей у малих розмірах, які отримував у касі банку. Використовуючи той факт, що його власний рахунок в банку також обслуговувався АС «Сарс-Сбон», та користуючись своїми владними повноваженнями щодо комп'ютерного супроводження вказаної АС, після заволодіння грошима готівкою Б. як законний користувач входив до АС та знищував інформацію про вказані операції, здійснені з ЕОМ касира. Таким чином Б. було викрадено гроші АКБ «Україна» на загальну суму 4066 грн. [145].

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. 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 любителем. У 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 здійснення комп'ютерного злочину.

2.4. «Непостійний вибір». Спосіб здійснення 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 зберігається у цій мережі, а також копіювати її.

2.5. «Пролом». Несанкціонований доступ до файлів законного

банківської інформації. Під **приховванням злочину** розуміється діяльність (елемент злочинної діяльності), спрямована на утворення перешкод розслідуванню шляхом утаювання, знищення, маскування або фальсифікації слідів злочину й злочинця та їх носіїв [40, с. 364].

Способи приховання незаконного доступу до ЕОМ у певній мірі детерміновані способами його вчинення. У випадку безпосереднього доступу до ЕОМ приховання слідів злочину зводиться до поновлення обстановки, що передує вчиненню злочину, тобто, знищення залишених слідів (пальців рук, взуття, мікрочастинок тощо). При опосередкованому (віддаленому) доступі приховання полягає саме в способі вчинення злочину, що ускладнює виявлення незаконного доступу. Це досягається використанням чужих паролів, засобів розмежування доступу тощо. Такі дії бувають під силу тільки фахівцям дуже високої кваліфікації і ступеня доступу до банківського програмного забезпечення.

4.5. Шахрайство з пластиковими платіжними засобами та їх підробка.

Підробка пластикових платіжних банківських карток та їх використання (кардинг), досить розповсюджений вид злочинів у сфері сучасних інформаційних технологій. Ми розглядаємо саме ці способи вчинення злочинів, оскільки: по-перше, через те, що кваліфікувати цей злочин варто за статтями 200 та ч. 3 ст. 190 КК України. Згідно з ч. 3 ст. 190 КК України дії суб'єкту злочину щодо протиправного використання платіжної картки законодавцем характеризуються як ті, що вчиняються з використанням електронно-обчислювальної техніки. По-друге, як відомо операції з використанням пластикових платіжних карток вчиняються з використанням відповідного технічного устаткування, яке можна віднести до сучасних інформаційних технологій, а також використовуються безпосередньо за допомогою комп'ютерних систем та їх мереж.

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 у шахрайстві обслуговуючого персоналу таких сервісних точок як ресторани, кафе, бари, мотелі тощо. Працівники таких підприємств, користуючись неуважністю клієнта, або зумисне відволікають його, роблять декілька додаткових відбитків пластикових карток (сліпів), що потім використовують для привласнення 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 підроблених сліпів, виготовлених зі справжніх пластикових карток. Сліпи виготовляються шахраями за допомогою складальних друкарських форм або шляхом застосування

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

В перших трьох пунктах ми розглянули типові способи вчинення комп'ютерних злочинів. Але варто зауважити, що злочини такого типу, як правило, вчинюються 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».

4.2. Крадіжка грошей шляхом маніпуляції з комп'ютером. Цей метод являє собою операцію підміни даних для ЕОМ з метою отримання фальшивих чеків. Для вчинення 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» або «підміна даних» і «за дурнем». Так, у липні 1995 року, використовуючи спосіб «маскарад» та спосіб «підміна даних», невстановлена особа внесла до ПЕОМ, що пов'язана з електронною комп'ютерною системою міжбанківського міжнародного зв'язку одного з банків м. Києва, завідомо незаконну інформацію про перерахунок валютних коштів. А саме, ця особа змінила пароль для входу до комп'ютерної системи банку, внаслідок чого банк не мав можливості зв'язатися зі своїми партнерами в закордонному банку. Скориставшись таким положенням, невідомою особою були надіслані платіжні доручення, за якими з рахунків цього банку незаконно були списані та направлені до зарубіжних банків валютні кошти у сумі 172 000 доларів США [138].

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 способів вчинення комп'ютерних злочинів існують також й інші. Найпоширеніший спосіб 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 із діяльністю обчислювального центру банку. Сторонні особи продумують 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 замислюють подібну аферу, вибирають найбільш сприятливу для її вчинення обстановку, можуть створювати підставну фірму з розрахунковим рахунком для перекачування викрадених грошей і т.д.

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.

Дані про способи приховання неправомірного доступу до комп'ютерної

користувача здійснюється також через знаходження слабких місць в захисті системи. Один раз, виявивши їх, правопорушник може, непоспішаючи, 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 вбудовані 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 здійснення 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 і мав намір. Господар системи, з якої вийшло фактичне підключення, формуючи правдоподібні відгуки, може підтримувати цю помилку на протязі певного часу і так 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 інструмент в руках електронного рекетира.

2.10. «Склад без стін». Даний комп'ютерний злочин, як правило,

здійснюється шляхом несанкціонованого доступу в комп'ютерну мережу в момент її системної неполадки. Наприклад, коли деякі файли користувача залишаються відкритими, зловмисник може отримати доступ до елементів банку даних, що йому не належать. Простіше цей спосіб можна пояснити так: наприклад, 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.

Начальник відділу комп'ютеризації Черкаської обласної дирекції Укрсоцбанку Ц. вступив у злочинну змову з К. та невстановленими в ході слідства особами. Працюючи спеціалістом зі збереження електронної пошти, 02.09.94 з метою викрадення з рахунку Черкаського АТ «Інвестверк» на рахунок АТ «Фінанси та кредит» у Київському АКБ «Ажіо» незаконно перерахував гроші на загальну суму 990 млн. крб. З метою приховування злочину для створення уяви нормальної роботи банку Ц. знищив електронні архіви операційного дня банку, журнали криптографічного захисту та інші електронні документи за 02.09.94, а також з 02.09 до 09.09.94 умисно шляхом коректування бази комп'ютерних даних банку щоденно вносив на баланс банку неправдиві відомості: вводив в обіг банку на початку кожного робочого дня і виводив наприкінці суму в 990 млн. крб. Тоді ж К. забезпечив оформлення документації, за допомогою якої планувалося заволодіти грошима у готівковій формі.

Під час слідства свідки Б. та М., які працюють економістами і до обов'язку яких входить введення інформації з платіжних доручень до комп'ютера для здійснення за ними перерахування грошей, пояснили, що 02.09.94 ніяких платіжних доручень на перерахування грошей з рахунку АТ «Інвестверк» на рахунок АТ «Фінанси та кредит» до ЕОМ не вводили. Паролі для входу до мережі банку і здійснення перерахування грошей нікому не повідомляли, чому останні були використані пояснити не можуть. Ніхто зі сторонніх осіб до приміщення банку, де безпосередньо здійснюються електронні перерахування, не заходив [140].

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 із декількох десятків команд, навряд чи може бути помітним серед сотень тисяч, а інколи і мільйонів команд, що є в комп'ютерних програмах.

3.3. «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», необхідно шукати не його самого, а набір команд, які його формують.

3.4. «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 переводів, вірогідність розкриття значно підвищується.

3.5. «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 і т. ін. Інколи цей спосіб називають «годинниковою бомбою».

3.6. «Асинхронна атака». Це досить складний спосіб здійснення 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.

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

3.8. «Повітряний змій». Спосіб здійснення цього злочину достатньо 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 число доручень про переказ не досягає підозрілої частоти. Але керувати цим процесом можна тільки за допомогою комп'ютера.