то досить велика частина працівників органів внутрішніх справ визнає таке вирішення проблеми цілком можливим. Більшість з них вважає, що подібна заміна необхідна в будь-якому випадку несплати штрафу (41 %). В другій за величиною групі (25 %) підкреслюється думка, що штраф можна замінювати арештом тільки в тому випадку, якщо його сума коливається в межах 200-1000 грн.

Майже третина опитаного населення (27,6 %) також припускає можливість заміни штрафу адміністративним арештом чи іншим видом стягнення. Проте, до вирішення цього питання варто підходити обережно: категорично проти заміни штрафу адміністративним арештом висловлюється 34,1 % респондентів, а 21 % обумовлює певну суму штрафу, за якої можна припустити таку заміну.

На закінчення відзначимо, що штраф як найпоширеніший вид адміністративного стягнення з погляду на проблеми його стягнення досить часто не виконує своєї превентивної і виховної функції. У зв'язку з цим необхідно приділити увагу вдосконаленню існуючого механізму і розробці нових засобів стягнення штрафу.

Список літератури: 1. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради УРСР. 1984. Додаток до № 52. Ст. 1122. 2. Адміністративна діяльність органів внутрішніх справ України в першій половині 2000 року: Аналітично-статистичний збірник. К., 2000. 3. Адміністративна відповідальність в Україні: Навч. посібник / За заг. ред. А.Т.Комзюка. Х., 1998. 4. Коломієць Т.О. Штрафи за законодавством про адміністративні правопорушення України. Запоріжжя, 2000.

Надійшла до редколегії 14.03.2001р.

О.А.Рябов,
викладач каф. криміналістики
Нац. ун-ту внутр. справ

Особливості порушення кримінальних справ по злочинам, скоєним із використанням ЕОМ

В наш час перед правоохоронними органами при розслідуванні злочинів, скоєних із використанням комп'ютерної техніки виникають криміналістичні проблеми, які характеризують водночас й специфіку цього процесу: складність у виявленні факту скоєння такого злочину та вирішенні питання про порушення кримінальної справи; складність у підготовці та проведенні окремих слідчих дій; особливості вибору та призначення необхідних судових експертиз; відсутність методики розслідування цієї категорії злочинів.

Найбільш розповсюдженими приводами для порушення кримінальних справ по цим злочинам є:

– повідомлення посадових осіб чи організацій, їх об'єднань (такі приводи складають більш третини);

– безпосереднє виявлення органом дізнання чи слідчим, прокурором даних, що вказують на ознаки злочину;

– заяви громадян;

– повідомлення в засобах масової інформації та ін.

Повідомлення про злочин, що пов'язаний із несанкціонованим проникненням у комп'ютерну систему або комп'ютерну комунікативну мережу, найчастіше надходять у правоохоронні органи безпосередньо від потерпілих – користувачів, коли нормальна робота системи стає об'єктом несанкціонованого доступу сторонніх осіб. Комп'ютер починає видавати фальшиві дані, часто відбуваються збої, знищується частина корисної інформації або вся, через що частішають скарги клієнтів комп'ютерної мережі. Усе це ознаки вчинення злочинних дій – неправомірного проникнення, застосування шкідливих програм злочинцем або порушення правил експлуатації комп'ютерної системи [1, с.15].

Сторонній спостерігач, який знаходиться в колективі користувачів комп'ютерної мережі може помічати такі особливості в поведінці окремих співробітників:

а) часте використання надурочної роботи;

б) немотивовані відмови обслуговувати комп'ютерну мережу та вимога надання відпустки;

в) несподіване придбання майна, яке дорого коштує;

г) зберігання на робочому місці різних комп'ютерних, фінансових бланків та інших таких документів;

д) поява випадків приховування переписування окремих даних без серйозних на те причин;

е) виявлення надзвичайного інтересу співробітником до змісту чужих роздруків (листингів), які виходять із принтерів [2, с. 67,68].

Певна річ, що таку інформацію (власне ознаки) про незаконні дії можна одержати, застосовуючи оперативно-розшукові заходи органів дізнання. Керівник комп'ютерної системи або індивідуальний користувач, який підключився до комп'ютерної мережі, повинен сповістити правоохоронні органи про ознаки порушення роботи системи. Звідси кримінальні справи про комп'ютерні злочини можуть бути порушені як за повідомленнями та заявами окремих громадян – користувачів комп'ютерної системи, керівників установ, фірм, у яких є такі системи, так і за матеріалами органів дізнання.

У разі надходження в правоохоронні органи заяв або повідомлень від користувачів спочатку необхідно провести попередню перевірку, яку слідчий здійснює при сприянні органів дізнання, контрольно-ревізійних органів [3, с. 123, 124].

Засоби виявлення доказів на стадії дослідчої перевірки дуже обмежені. Це огляд місця події і знайдених на ньому об'єктів, одержання пояснень громадян, витребування у посадових осіб документів та довідок, призначення та проведення за дорученням слідчого відомчих ревізій.

Дослідча перевірка проводиться лише у випадках, коли слідчому, органу дізнання у разі надходження матеріалів про скоєний злочин не ви-

стачає даних для прийняття рішення чи не зрозуміла кваліфікація скоєного діяння. Маючи на увазі специфіку розглянутих злочинів, можна припустити, що перевірка фактів здійснення злочинів в області комп'ютерної інформації буде зводитися до одержання наступних даних:

– уточнення способу порушення цілісності (конфіденційності) інформації;

– уточнення порядку регламентації власником роботи інформаційної системи;

– уточнення кола осіб, що мають можливість взаємодіяти із інформаційною системою, у якій відбулися порушення цілісності (конфіденційності) інформації для визначення свідоцької бази і виявлення кола запідозрених;

– уточнення даних про заподіяний власнику інформації збиток [4, с.954].

Усі ці дані при їх відсутності в матеріалах, що надійшли, повинні бути витребувані у власника інформаційної системи.

Як правило, у цей період витребуються наступні документи:

1) журнал збійних ситуацій обчислювального центра, збоїв у роботі комп'ютерної мережі, виходу окремих комп'ютерів чи технічних пристроїв з ладу (він може вестися як у конкретному підприємстві, організації, установі, фірмі, компанії, де скоєний злочин, так і в обслуговуючому даний підрозділ сервісному центрі (обчислювальному центрі);

2) журнал обліку робочого часу та передачі змін операторами ЕОМ;

3) журнал обліку роботи комп'ютерів мережі;

4) копії проведених протягом дня операцій (банківських, результати антивірусних перевірок і перевірок контрольних сум файлів) [5, с.34].

Крім вищевказаних, в цей період повинні бути витребувані матеріали:

1) фізичні (матеріальні) носії інформації. У першу чергу, необхідно вилучити жорсткий диск (вінчестер) головного комп'ютера (сервера) обчислювальної мережі, а також жорсткі диски з інших комп'ютерів.

Крім того, магнітні стрічки (при наявності підключених до комп'ютера відповідних накопичувачів), дискети, лазерні та магнітооптичні диски, роздруківки, виконані на принтері, інші носії комп'ютерної інформації;

2) програмне забезпечення ЕОМ (при неможливості вилучити фізичні носії);

3) файл адміністратора мережі, у якому фіксується вся робота мережі (моменти. вмикання та вимикання, результати тестування, протоколи збійних ситуацій);

4) акти за результатами антивірусних перевірок та контрольні суми файлів, що зберігаються у відповідних програмах. Порушення контрольних сум говорить про можливе незаконне копіювання чи використання комп'ютерної інформації;

5) перелік осіб, що мають право доступу до тієї чи іншої комп'ютерної інформації та перелік паролів, під якими вони ідентифіковані в комп'ютері;

6) роздруківки проведених на даному комп'ютері операцій при їх наявності в даному обчислювальному центрі.

Для уточнення підстав до порушення кримінальної справи необхідно відібрати пояснення у інженерів-програмістів, що займалися розробкою програмного забезпечення та його супроводом (налагодженням і обслуговуванням), операторів, електронщиків відділу технічного забезпечення ОЦ, що займаються експлуатацією та ремонтом засобів комп'ютерної техніки, системних програмістів («системщиків»), інженерів по засобам зв'язку та телекомунікаційному обладнанню, фахівців по забезпеченню безпеки комп'ютерних систем і ін.

Важливу роль у зборі даних про скоєний злочин відіграють дії посадових осіб власника інформаційної системи, що здійснюють процедури, які забезпечують цілісність (конфіденційність) інформації в системі [6, с.107].

Збір матеріалів про ознаки злочину та їх перевірку проводить орган дізнання. Перед порушенням кримінальної справи орган дізнання подає матеріали слідчому. Останній вирішує питання про порушення справи та разом з оперативним робітником розробляє план реалізації оперативних матеріалів. Як у першому, так і іншому випадках до числа невідкладних першочергових слідчих дій належать: огляд, обшук, виїмка, затримання, допит.

Список літератури: 1. Салтевський М.В. Основи методики розслідування злочинів, скоєнних з використанням ЕОМ // Учбовий та практичний посібник. – Х., 1999. 2. Шурухнов М.Г. Расследование неправомерного доступа к компьютерной информации // Практическое пособие. – М., 1999. 3. Крылов В. В. Информационные компьютерные преступления // Учебное и практическое пособие. М., 1997. 4. Белкин Р.С. Криминалистика // учебник для вузов. М., 2000. 5. Вехов В. Б. Компьютерные преступления – способы совершения // Учебное пособие. М.1996. 6. Селиванов Н.А., Дворкин А.Ч. Пособие для следователя – расследование преступлений повышенной опасности. М.,1998.

Надійшла до редколегії 16.03.2001р.

В.Б. Смелік,
магістрант Нац. ун-ту внутр. справ

Зв'язок розкрадань майна з іншими злочинами у сфері підприємництва, як елемент їх криміналістичної характеристики

Реформування економічних відносин в Україні не могло не позначитись на рівні, структурі та динаміці економічної злочинності. Стрімкі економічні та злочинні трансформаційні процеси йшли рука об руку, пристосовуючись до нестабільного і недосконалого законодавства, а іноді і випе-