Корупція зводить нанівець правосуддя. Правим виявляється той, хто має більше грошей і не має моральних устоїв. У слідчій практиці з'явився винахід: «оплата слідчому власного арешту і обвинувального вироку». Одна з таких сум склала 150 тисяч американських доларів [5, с.17].

Існує реальна загроза демократії: громадяни не бачать моральних стимулів до участі в виборах.

Зрештою, державі неможливо досягти здійснення стратегічних задач, якщо вони суперечать інтересам олігархічних груп , які володіють значними вільними ресурсами для підкупу.

Верховна Рада не змогла прийняти Податковий кодекс, котрий зменшив би тиск на платників податків і водночас розширив базу оподаткування. М.Азаров прокоментував цю подію так: «Податковий кодекс в запропонованій редакції може перекрити джерела неконтрольованого збагачення ряду впливових осіб і політико-економічних угруповань. А це дуже великі гроші, мільярди. Їх власники в таких ситуаціях, як відомо, ні перед чим не зупиняються. На жаль, і деякі народні обранці також» [6, с.4]. Тому вже виникла ідея електронного уряду, який в інформаційному суспільстві буде конкурувати з представницькою демократією [4, с.13].

Згідно з синергетичною теорією катастроф стійкість системи має об'єктивну межу, за якою слідує її лавиноподібна і безповоротна катастрофа.

Сучасне суспільство приречене на боротьбу з корупцією в силу природного потягу до самозбереження. Рівень поширеності і суспільної небезпечності останньої повинен не заважати розвитку суспільства у відповідності з законодавчо закріпленими, і перш за все з Конституцією, цінностями і пріоритетами.

Список літератури: 1. Б.Ерасов. Хаос и криминал // Свободная мысль. № 8. 2002. 2. Д.Табачник. Нам нет смысла изобретать велосипед // Московский комсомолец в Украине. № 15. 6–13.04. 2000. 3. А.С.Ахиезер, И.Г.Яковенко. Что же такое общество?// Общественные науки и современность. № 3. 1997. 4. А.Чубатенко. Запад внимательно следит за всем, что происходит в нашей стране.// Комсомольская правда в Украине. 17.08.2001. 5. Ю.Пешехова. Взятка.// Совершенно секретно. № 2, 2002. 6. М.Азаров. Ухвалити Податковий кодекс народним депутатам завадили гроші // Юридичний вісник України. №8.2001.

Надійшла до редколегії 25.02.02

О.А. Рябов

Проблеми огляду місця події по злочинах, скоєних з використанням комп'ютерної техніки

Злочини в сфері комп'ютерної інформації, незважаючи на їх незначну питому вагу у загальній структурі злочинності, складають реальну загрозу не тільки окремим користувачам електронно-обчислювальної техніки, але й в цілому національній безпеці країни, оскільки вони все більше набувають транснаціонального організованого характеру, а спричинена ними шкода іноді не піддається підрахунку.

Знищення, блокування, модифікація інформації, важливої для дій, зв'язаних з керуючими датчиками складних комп'ютерних систем оборонного та виробничого призначення, можуть спричинити загибель людей, заподіяння

шкоди їхньому здоров'ю, непередбачений небезпечний розвиток технологічних процесів, знищення майна в значних розмірах.

Огляд об'єктів по справах вказаної категорії є найважливішим інструментом встановлення обставин розслідуваної події. При оглядах комп'ютерних засобів з їх вилученням виникає ряд загальних проблем, які пов'язані зі специфікою засобів, що оглядаються, тому в процесі підготовки до проведення цієї слідчої дії ще до виїзду на місце події необхідно вирішити ряд організаційних питань, що у подальшому забезпечать якість проведення огляду місця події.

Так, необхідно передбачити заходи безпеки, що здійснюються злочинцями з метою знищення речових доказів. Наприклад, вони можуть використовувати спеціальне обладнання, що у критичних випадках створює магнітне поле великої сили, яке знищує магнітні записи. Відома історія про хакера, що створив у дверному прорізі своєї кімнати магнітне поле такої сили, що знищувало магнітні носії інформації при виносі їх з приміщення [1, с.57].

Іноді «шкідлива» програма може існувати тільки в оперативній пам'яті комп'ютера. У такому випадку його вимикання спричинить за собою втрату інформації, що у свою чергу ускладнює розслідування або робить його неможливим. При цьому слідчий повинен діяти відповідно до обстановки, що склалася, щоб не допустити нанесення матеріального збитку такою програмою та по можливості зберегти характер оперативної пам'яті на носії за допомогою спеціального програмного забезпечення, що встановлюється фахівцем, присутнім при огляді.

Злочинець може включити до складу програмного забезпечення своєї машини програму, що «змусить» комп'ютер періодично вимагати пароль, і, якщо за деякий час правильний пароль не буде введений, то дані в комп'ютері автоматично знищаться. Винахідливі власники комп'ютерів встановлюють іноді сховані команди, що знищують чи архівують важливі дані, якщо деякі процедури запуску машини не супроводжуються спеціальними діями, відомими тільки їм [2, с. 68].

З метою недопущення шкідливих наслідків вказаних вище дій слідчий може дотримувати наступних положень.

Огляд місця події варто почати з вживання заходів щодо запобігання приховування злочинцем своїх дій з машинною інформацією. Для цього необхідно виключити можливість доступу до засобів обчислювальної техніки всіх осіб, які працюють на об'єкті та вимкнути всі комп'ютери. Якщо зробити це не представляється можливим через особливості функціонування системи, то потрібно вжити заходів для запобігання поширення шкідливих програм.

Перед вимиканням живлення необхідно коректно закрити всі використовувані програми, а в сумнівних випадках просто відключити комп'ютер (у деяких випадках некоректне відключення комп'ютера – шляхом перезавантаження чи вимикання живлення без попереднього виходу з програми і запису інформації на постійний носій– приводить до втрати інформації в оперативній пам'яті і навіть до стирання інформаційних ресурсів на даному комп'ютері) [3, с. 64].

При наявності засобів захисту ЕОМ від несанкціонованого доступу необхідно вжити заходів до встановлення ключів доступу (паролів, алгоритмів і т.п.). Не рекомендується намагатися на місці переглядати інформацію, що міститься на носіях. У скрутних ситуаціях варто звертатися за допомогою не до персоналу, а до фахівця, якого слід запросити для проведення слідчої дії. Необхідно вилучати всі ЕОМ, виявлені на об'єкті.

Як правильно вказується в методичних рекомендаціях під час проведення огляду необхідно вжити заходів щодо забезпечення збереження інформації на комп'ютерах, що знаходяться на місці та на магнітних носіях [1, с.93].

Для цього, крім перерахованих вище положень, необхідно забезпечити контроль за енергопостачанням об'єкта, що оглядається. У випадку, якщо на момент початку огляду електропостачання об'єкта виключене, то до його відновлення варто відключити від електромережі всі комп'ютери та периферійні пристрої, що знаходяться на об'єкті.

При наявності в приміщенні, де знаходяться комп'ютери чи магнітні носії інформації, вибухових, легкозаймистих, їдких і токсичних речовин і/чи матеріалів якомога швидше прибрати ці речовини і/чи матеріали в інше приміщення, а при неможливості — забезпечити контроль за доступом до них.

У ході огляду особливу увагу слід звернути на розміщення комп'ютерів у конкретному приміщенні, а якщо вони з'єднані в одну комп'ютерну мережу – розташування всіх комп'ютерів в ній, наявність виділеного сервера та його розташування, цілісність з'єднуючих кабелів, стан пристроїв телекомунікації (модемів, факс-модемів) та підключення їх до телефонних каналів. Це необхідно для перевірки версії про здійснення злочину по мережах телекомунікації чи локальної обчислювальної мережі. Рекомендується з'ясувати конкретне призначення кожного комп'ютера. Це повинно бути відображено в протоколі огляду. При наявності мережі необхідно накреслити схему з'єднання пристроїв. Забороняється робити роз'єднання (з'єднання) кабельних ліній, не усвідомивши попередньо їх призначення, переконавшись, що така дія не нанесе збитку. Розкриття і демонтаж засобів обчислювальної техніки повинен робити тільки фахівець.

Застосування засобів криміналістичної техніки (магнітних пошукачів, ультрафіолетових освітлювачів, джерел інфрачервоного випромінювання, електронно-оптичних перетворювачів) повинно бути погоджено з фахівцем, щоб уникнути руйнування носіїв інформації та мікросхем ЕОМ.

Речові докази у вигляді ЕОМ, машинних носіїв вимагають особливої акуратності при транспортуванні та зберіганні. Їм протипоказані різкі кидки, удари, підвищені температури, вологість, задимленість (у тому числі тютюновий дим) та запиленість. Всі ці зовнішні фактори можуть спричинити втрату даних, інформації та властивостей апаратури. При роботі з магнітними носіями інформації забороняється доторкатися руками до робочої поверхні дисків, піддавати їх електромагнітному впливу, підвергати деформації, зберігати без спеціальних контейнерів. Необхідно уникати попадання дрібних часток та порошків на робочі частини пристроїв введення-виведення інформації

комп'ютерів. Слід пам'ятати, що діапазон припустимих температур при зберіганні та транспортуванні даних засобів – від 0 до 50 °С [4, с.126].

Оскільки деякі користувачі (особливо некваліфіковані) записують на окремих паперових листках процедуру входу та виходу з комп'ютерної системи, а також паролі доступу, варто вилучити також всі записи, що відносяться до роботи ЕОМ.

В наслідок того, що багато комерційних та державних структур звертаються до послуг позаштатних і тимчасово працюючих фахівців щодо обслуговування ЕОМ, варто встановити дані всіх осіб, які знаходяться на об'єкті, незалежно від їх пояснень мети перебування на об'єкті.

Слід пам'ятати, що при оглядах необхідно збирати і «традиційні» об'єкти – відбитки пальців на клавіатурі, вимикачах та тумблерах, шифровані рукописні записи та ін. Огляду підлягають всі пристрої конкретної ЕОМ. Цей огляд при аналізі його результатів за участю фахівців допоможе відтворити механізм дій зловмисників та одержати важливі докази.

Список літератури: 1. Крилов В. В. Інформаційні комп'ютерні злочини. М., 1997. 2. Вехов В. Б. Комп'ютерні злочини: способи здійснення і розкриття // Право і Закон. М., 1996. 3. Шурухнов М.Г. Розслідування неправомірного доступу до комп'ютерної інформації. М., 1999. 4. Айков Д., Сейгер К., Фонсторх У. *Комп'ютерні злочини*. М., 1999.

Надійшла до редколегії 27.02.02

К.Л. Бугайчук

ОСОБА ПОРУШНИКА НОРМ АДМІНІСТРАТИВНОГО ПРАВА ТА ЙОГО ПРОТИПРАВНА ПОВЕДІНКА

Особа як цілісне утворення, як відомо, являє собою соціальну сутність людини. Однак вона не надається з дня його народження, а формується в процесі суспільних відносин, тобто є продуктом соціалізації людини. В той же час людина є продуктом подвійної детермінації, оскільки її природа біосоціальна.

Щодо природи та сутності людини – це не тотожні категорії. Якщо перша містить генетичні та соціальні зв'язки людини, то друга охоплює соціальні ознаки. Людині властиві свідомість та самосвідомість. Для того, щоб бути особою, безумовно, необхідно усвідомлювати навколишню дійсність та самого себе у відношеннях із цією дійсністю. З твердження, що особа неможлива без свідомості, не витікає, що свідомість дорівнює особі, бо вчиняє поступки не свідомість, а особа, яка регулює свої дії з її допомогою. Тому справедливо буде визнати свідомість внутрішньою сутністю особи. Інша сторона сутності особи пов'язана з соціальною діяльністю людини.

Через діяльність співвідносяться внутрішнє та зовнішнє, зовнішнє проникає у внутрішнє (суспільні відносини перетворюються у риси особи), а внутрішнє у зовнішнє (особа опредмечує себе, змінюючи суспільні відносини та духовний світ). Цей аналіз призводить до розуміння особи в двох аспектах:

1) інтраіндивідуальному, який відображається в соціальній діяльності людини;

2) інтеріндивідуальному, відображаючому внутрішній світ особи, та який проявляється в її соціальній спрямованості.