Організація підготовки фахівців по боротьбі   
зі злочинністю у сфері високих технологій

Боротьба зі злочинністю в інформаційній та комунікаційній сферах сьогодні набула особливої гостроти та актуальності в усьому світі. Так, за даними Федерального міністерства внутрішніх справ Німеччини, за останні 10 років кількість таких злочинів там зросла у 10 разів (від 5 тисяч випадків у 1990 р. до майже 50 тисяч – у 1999 р.). Лише в Баварії за 1999 рік вчинено 4451 злочин цього виду, у 2000 р. тільки в м. Мюнхені порушено вже понад 300 кримінальних справ, пов’язаних з такими злочинами.

Боротьба з цим видом злочинності потребує певної законодавчої бази. Відповідно до Рекомендацій Ради Європи від 1990 р. парламентам країн Європи пропонувалося вдосконалити та уніфікувати національне законодавство з проблем, що розглядаються. Так, у Німеччині з 1986 р. Кримінальний кодекс містить п’ять статей, що стосуються злочинності в інформаційній і комунікаційній сферах. Відповідне законодавство існує у переважній більшості країн. Як було зазначено на засіданні Робочої групи у м. Мюнстері, з 16-ти країн - учасниць зустрічі тільки Україна і Албанія не провели відповідних змін у законодавстві. Єдина стаття (1981) у Кримінальному кодексі України не охоплює всього спектру комп’ютерних злочинів та не відповідає Рекомендаціям Комітету у справах законодавства Ради Європи 1990 р.

Проект нового Кримінального кодексу України містить вже три статті, що стосуються цього виду злочинності:

ст.373. Незаконне втручання в роботу автоматизованих електронно-обчислювальних систем;

ст.374. Викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства або зловживанням особи своїм службовим становищем;

ст.375. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем.

У зв’язку з різким поширенням цього виду злочинів у всьому світі сьогодні існують чи створюються відповідні підрозділи по боротьбі з ними. Наприклад, у Німеччині функціонують підрозділи по вилученню речових доказів комп’ютерних злочинів. Позитивні зміни у цьому напрямі можна спостерігати і у країнах СНД. Так, у складі МВС Російської Федерації у 1998 р. створене та діє Головне управління по боротьбі зі злочинами у сфері високих технологій. В Україні у цьому році створено перший подібний підрозділ (у складі ГУБОЗ МВС України).

Боротьба з цим видом злочинності в Україні сьогодні визнана одним з головних напрямів діяльності органів внутрішніх справ. Про це, зокрема, йшла мова на нараді керівництва МВС України 10 квітня 2000 р. Про актуальність проблеми свідчить той факт, що за даними ГУБОЗ МВС України на вересень 2000 р. в Україні було порушено 18 кримінальних справ, і лише по одній з них матеріальний збиток склав 249 млн грн. Національна академія внутрішніх справ України направила в цьому році свої пропозиції щодо удосконалення боротьби з цим видом злочинів (до п.6 зазначеної наради). Зокрема, висловлювалися пропозиції щодо удосконалення законодавства України стосовно цього виду злочинності; доцільності створення окремого підрозділу в МВС України та відповідних підрозділів в областях (містах), завданням яких повинно стати розкриття, розслідування та попередження таких видів злочинів; узагальнення передового досвіду з цієї проблеми. Для цього потрібно виявити та зібрати для проведення 1-2 тижневого семінару в НАВСУ працівників слідчих та оперативних підрозділів ОВС України, які брали участь у розкритті та розслідуванні комп’ютерних злочинів, зобов’язавши їх зробити копії відповідних кримінальних справ та підготувати реферати з цієї тематики.

Стосовно підготовки та перепідготовки кадрів цієї галузі, на нашу думку, в Україні треба готувати фахівців для підрозділів БОЗ та БЕЗ за спеціальною програмою в НАВСУ на базі профілюючої вищої технічної та економічної освіти.

Крім вивчення ними основних юридичних дисциплін профілюючі знання, вміння та навички можуть бути набуті ними через впровадження в НАВСУ нових спеціалізованих дисциплін за такою орієнтовною тематикою: “Методика розкриття, розслідування та попередження злочинів в інформаційній та комунікаційній сфері”. У перспективі можливо впровадження дисципліни: “Комп’ютерні технології в оперативній та інформаційно-аналітичній роботі” та ін.

Йдеться про те, що широке розповсюдження комп’ютерних технологій, їх масове використання у різних галузях, в тому числі зі злочинними намірами, створює об’єктивну основу для отримання цінної оперативної інформації, документування злочинних дій певних осіб шляхом прихованого контролю комп’ютерних масивів інформації, повідомлень, що передаються комп’ютерними мережами. Серед оперативно-розшукових заходів особливе місце сьогодні посідають заходи скритого отримання комп’ютерної інформації. Відповідно до чинного законодавства України і відомчих нормативних актів такі дії можуть здійснюватися в рамках проведення відповідних оперативно-технічних заходів.

Однак, з урахуванням специфіки об’єктів, засобів і методів дослідження – це досить складний інструмент ОРД, що вимагає спеціальної підготовки оперативних працівників. Зокрема, вони повинні володіти правовими та організаційними основами проведення зазначених дій, своїми правами щодо зміни чи знищення при цьому комп’ютерної інформації, знати вимоги кримінально-процесуального законодавства щодо процедур отримання та використання цієї інформації в ході проведення окремих слідчих дій. Крім того, треба бути обізнаними з порядком оформлення завдань і одержання судових рішень на проведення ОРД такого виду, подання їх результатів органу дізнання, слідчому, прокурору чи суду.

Потребують окремого розгляду питання, пов’язані із засобами, а також тактикою прихованого отримання інформації із захищених комп’ютерних систем. Тому особа, яка досліджує комп’ютер, повинна орієнтуватися стосовно уразливих місць типових механізмів захисту і можливих недоліків в організації їх використання, володіти методикою подолання механізмів парольного захисту, вміти застосовувати засоби і прийоми подолання захисних функцій BIOS, прихованого контролю вмісту екранів відеомоніторів, даних клавіатури й інших периферійних пристроїв ПК, бути обізнаною з порядком оформлення результатів проведення оперативно-технічних заходів.

Крім того, треба знати основи архітектури і функціонування локальних та глобальних комп’ютерних мереж, види мережних протоколів, операційних систем, особливості мережних захисних механізмів, засоби й прийоми дослідження топології та логічної структури мережі: сканування мережних адрес і портів, моніторингу інформаційних потоків, а також вміти виявляти інформаційні ресурси, що представляють оперативний інтерес у відкритих джерелах глобальної мережі Інтернет – у групах новин, на Web-сторінках і серверах, володіти основними методами подолання систем захисту комп’ютерних мереж, знати особливості зняття інформації з технічних каналів зв’язку в локальних і глобальних комп’ютерних мережах.

Особа, що досліджує комп’ютер, також повинна володіти методикою оперативно-технічного супроводження розкриття злочинів у сфері комп’ютерної інформації, знати уразливі місця комп’ютерної системи, методи і засоби несанкціонованого доступу, проблеми розслідування і розкриття злочинів у сфері комп’ютерної інформації, ознаки і засоби виявлення фактів несанкціонованого проникнення в систему, засоби і методи моніторингу та систем оповіщення про факти вторгнення, тактичні прийоми застосування програмних і апаратних пасток, відслідковування і документування дій правопорушника, тактичні прийоми утримання мережного з’єднання з правопорушником, методику застосування спеціальної техніки для документування фактів учинення злочинів у сфері комп’ютерної інформації.

Для викладання окремих тем вказаних дисциплін (у разі потреби) можна залучати професорсько-викладацький склад кафедр НАВСУ та фахівців з інших вузів (Академія СБУ, Національний технічний університет та ін.).

При організації навчання можна використовувати позитивний досвід окремих вузів. Так, у навчальний процес НАВСУ впроваджена дисципліна “Комп’ютеризовані інформаційні системи правоохоронних органів та інформаційна безпека”, де вивчаються проблеми попередження комп’ютерних злочинів. Крім того, в рамках дисципліни “Криміналістична інформатика”, що викладається в НАВСУ вже декілька років, вивчаються окремі питання виявлення та розслідування злочинів, пов’язаних з використанням комп’ютерних технологій.

Вивчення передового досвіду діяльності поліції країн, які через об’єктивні причини сьогодні випереджають нашу країну в цій галузі, є надто корисним. Треба також організувати підготовку та випуск достатньої кількості навчально-методичної літератури з цієї тематики.

Крім того, вкрай необхідні наукові дослідження у цій сфері, в тому числі на дисертаційному рівні. Треба, за можливістю, ширше залучати науковців до розкриття та розслідування таких злочинів, що вчиняються в Україні.