2. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991.

3. Вакка Дж. Секреты безопасности в Internet. – К.: “Диалектика”, 1997.

4. Виявлення та розслідування злочинів, що вчиняються за допомогою комп`ютерних технологій. Посібник /Романюк Б.В. Камлик М.І., Гавловський В.Д., Хахановський В.Г. Цимбалюк В.С. /За ред. Я.Ю.Кондратьєва. – К.: НАВСУ, 2000. – 64 с.

5. Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби із злочинами, що вчиняються з використанням комп’ютерних технологій // Боротьба з контрабандою: проблеми та шляхи їх вирішення. - К.: НДІ "Проблем людини",1998. – С.148-154.

6. Калюжный Р.А. Научно-технический прогресс в деятельности правоохранительных органов. – К.: “Наукова думка”, 1990.

7. Калюжний Р.А., Цимбалюк В.С. Вдосконалення інформатизації ОВС України - передумова покращення їх діяльності в боротьбі зі злочинністю // Правова система України: теорія і практика. 1993. – С.397-399.

8. Кримінальне право. Особлива частина. Підручник. (Александров Ю.В., Антипов В.І. та інші). Відпов. редактор Шакун В.І. – К.: “Правові джерела”, 1999.

9. Уголовный кодекс Украины: Научно-практический комментарий (Ответ. Редакторы Яценко С.С., Шакун В.И.). – К.: “Правові джерела”, 1998.

10. Ярочкин В.И. Безопасность информационных систем. – М.: “Ось-89”, 1996.

11. Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Международные отношения, 2000. – 400 с.

В.ХАХАНОВСЬКИЙ, *кандидат юридичних наук, доцент*

НАУКОВО-ПЕДАГОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В ІНФОРМАЦІЙНІЙ ТА КОМУНІКАЦІЙНІЙ СФЕРАХ

Людство неминуче вступає в інформаційну епоху. Фахівці вважають, у світі розпочалося сторіччя інформатизації. Не стоїть осторонь цього процесу й наша держава, де останніми роками питанням інформатизації суспільства приділяється особлива увага.

Загальновідомий вислів “Хто володіє інформацією, той володіє світом” у значній мірі стосується правоохоронних органів, де процеси збирання, обробки, аналізу та зберігання інформації, на основі якої приймаються управлінські рішення, відіграють вирішальну роль.

Сьогодні в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій в діяльність правоохоронних органів. Створюються міжвідомчі інформаційні системи правоохоронних органів, які успішно використовуються у боротьбі зі злочинністю. На відомчі навчальні заклади покладено відповідальне завдання – підготовка висококваліфікованих фахівців нового тисячоліття, спроможних орієнтуватися в величезних інформаційних потоках, адекватно протистояти злочинним угрупованням, які сьогодні мають сучасне технічне оснащення та спеціальну підготовку.

Боротьба зі злочинністю в інформаційній та комунікаційній сферах 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. Лише в Баварії за 1999 рік вчинено 4451 злочин цього виду, у 2000 році тільки в м. Мюнхені порушено вже біля 300 кримінальних справ, пов’язаних з такими злочинами.

У зв’язку з різким поширенням цього виду злочинів у всьому світі нині існують чи створюються відповідні підрозділи по боротьбі з ними. Наприклад, у тій же Німеччині функціонують підрозділи з вилучення речових доказів комп’ютерних злочинів. Позитивні зміни у

цьому напрямку можна вже спостерігати і у країнах СНД. Так, у складі МВС РФ з 1998 року функціонує Головне управління по боротьбі зі злочинами у сфері високих технологій. У складі ДСБЕЗ МВС України також створено управління по боротьбі зі злочинністю в сфері високих технологій та інтелектуальної власності.

Боротьба з цим видом злочинності потребує наявності певної законодавчої бази. Так, Кримінальний кодекс Німеччини з 1986 р. містить п'ять статей, що стосуються злочинності в інформаційній і комунікаційній сферах. Відповідне законодавство існує у переважній більшості країн, як це й було рекомендовано це у 1990 році Комітетом у справах законодавства Ради Європи.

Новий кримінальний кодекс України, що вступив у чинність з 2001 р., містить вже три статті щодо цього виду злочинності: ст. ст. 361, 362 та 363.

Боротьба з цим видом злочинності в Україні сьогодні визнана одним з пріоритетних напрямків діяльності органів внутрішніх справ. Ця проблема розглядалася на колегіях та нарадах керівництва МВС України, про актуальність проблеми свідчять також дані спеціальних підрозділів МВС України за останні роки. Так, лише по одній з порушених кримінальних справ в Україні матеріальний збиток становив 249 млн. грн.

Національна академія внутрішніх справ України надавала свої пропозиції щодо вдосконалення боротьби з цим видом злочинів. Зокрема, висловлювалися пропозиції щодо вдосконалення законодавства України щодо цього виду злочинності; доцільності створення відповідного міжвідомчого координаційного центру, підрозділів МВС України в областях (містах), завданням яких повинно бути розкриття, розслідування та попередження таких злочинів.

Для узагальнення передового досвіду з цієї проблеми було запропоновано виявити та зібрати для проведення 1-2 тижневого семінару в НАВСУ працівників слідчих та оперативних підрозділів, які брали участь у розкритті та розслідуванні подібних злочинів, зобов'язавши їх зробити копії відповідних кримінальних справ та підготувати реферати з цієї тематики.

Щодо підготовки та перепідготовки кадрів в цій галузі. На декількох засіданнях Вченої ради НАВСУ у 2000-2003 р.р. розглядалися питання про можливості організації підготовки фахівців з боротьби зі злочинністю в комп'ютерній сфері. Спеціально створена робоча група, до складу якої увійшли науковці та практичні працівники правоохоронних органів, з урахуванням досвіду інших навчальних закладів, розробила пропозиції щодо організації підготовки та перепідготовки фахівців з боротьби з організованою злочинністю в цій сфері. Думається, що ці питання потребують спільного обговорення фахівцями Національної академії внутрішніх справ України та Національного університету внутрішніх справ України.

На нашу думку, в Україні подібних фахівців треба готувати за спеціальною програмою на базі профілюючої вищої технічної та економічної освіти. Крім вивчення основних юридичних дисциплін, профілюючі знання, вміння та навички можуть бути надані шляхом впровадження нових спеціалізованих дисциплін з такими орієнтовними назвами: "Методика розкриття, розслідування та попередження злочинів в інформаційній та комунікаційній сфері", "Комп'ютерні технології в оперативній та інформаційно-аналітичній роботі" та ін. До проведення таких навчальних занять в НАВСУ, крім штатного професорсько-викладацького складу, пропонується залучити також фахівців з інших вузів.

Для ефективного дослідження проблем боротьби із злочинністю в комп'ютерній сфері треба скористатися зарубіжним позитивним досвідом, зокрема, шляхом поширення участі у міжнародних конференціях, семінарах, підвищення кваліфікації за кордоном науковців та професорсько-викладацького складу навчальних закладів.

Треба також поширювати наукові дослідження у цій сфері, в тому числі - й на дисертаційному рівні, організувати випуск достатньої кількості наукової та навчально-методичної літератури з цієї тематики. Так, у 2000 році випущено посібник "Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій", підготовлений співробітниками МНДЦ з проблем боротьби з організованою злочинністю та НАВСУ, але тиражем лише 100 прим., чого явно замало. Працівниками тих самих підрозділів за участю НЦБ Інтерполу підготовлено посібник "За-

хист інформації в автоматизованих системах". Треба поширювати таку практику та, по можливості, залучати науковців до розслідування злочинів в комп'ютерній сфері.

На нашу думку, настав час для поєднання зусиль та створення певного міжвідомчого підрозділу, яке б сприяло підготовці кадрів з боротьби з організованою злочинністю в інформаційній та комунікаційній сферах для правоохоронних органів України.

Слід зазначити, що широке розповсюдження комп'ютерних технологій та їхнє масове використання у всіх галузях життя сучасного суспільства, в тому числі – й із злочинними намірами, створює об'єктивну основу для отримання цінної оперативної інформації, документування злочинних дій певних осіб шляхом контролю комп'ютерних масивів інформації, повідомлень, що передаються комп'ютерними мережами.

Отримання, дослідження і використання комп'ютерної інформації в оперативно-розшуковій діяльності стає достатньо перспективним і актуальним напрямом. Однак, з урахуванням специфіки об'єктів, засобів і методів дослідження, – це досить складний інструмент ОРД, який вимагає спеціальної підготовки оперативних працівників.

Так, вони повинні знати правові та організаційні основи проведення вказаних дій в рамках оперативно-розшукових та оперативно-технічних заходів, свої права щодо зміни чи знищення при цьому комп'ютерної інформації, 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.

Комп'ютерні носії інформації можуть розглядатися як об'єкт дослідження, а також як речові докази чи документи. Вони можуть містити, зокрема, інформацію, що має орієнтовне чи доказове значення. Зрозуміло, що особа, яка здійснює дослідження комп'ютерних носіїв інформації, повинна бути обізнана з фізичними принципами збереження даних, логічною їх організацією на носіях, з методами і засобами пошуку комп'ютерної інформації, що має оперативний інтерес, з можливостями відновлення видаленої інформації та дослідження пошкоджених носіїв.

Потребують окремого розгляду також питання, що пов'язані із засобами і тактикою отримання інформації із захищених комп'ютерних систем, уразливими місцями та методикою подолання типових механізмів захисту, з порядком оформлення результатів проведення оперативно-технічних заходів.

Крім того, треба знати архітектуру і функціонування локальних і глобальних комп'ютерних мереж, види мережних протоколів, операційних систем, особливості мережних захисних механізмів, засоби і прийоми дослідження топології і логічної структури мережі: сканування мережних адрес і портів, моніторингу інформаційних потоків, а також вміти виявляти інформаційні ресурси, що являють оперативний інтерес у відкритих джерелах глобальної мережі Інтернет: у групах новин, на сторінках Веб і серверах, володіти основними методами подолання систем захисту комп'ютерних мереж, знати особливості зняття інформації з технічних каналів зв'язку в 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 такого виду, 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, викриття та документування дій правопорушника, тактичні прийоми утримання мережного з'єднання з правопорушником, методику застосування спеціальної техніки для документування фактів вчинення злочинів у сфері комп'ютерної інформації.

Напевно, настав час для розгляду питання про впровадження у навчальний процес спеціалізованої дисципліни для певних категорій слухачів та курсантів, де б вивчалися пробле-

ми, що розглянуті вище. На нашу думку, ця дисципліна повинна бути комплексною та викладатися декількома кафедрами.

Використана література

1. Закон України "Про захист інформації в автоматизованих системах" від 5.07.94, № 81/94-ВР.
2. Биленчук П.Д., Хахановский В.Г. Компьютерная безопасность // Бюл. по обм. опытом работы ОВД. – 1994. – №115. – С. 48-49.
3. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій: Посібник / За ред. Я.Ю. Кондратьєва. – К.: НАВСУ, МНДЦ. 2000.
4. Система інформаційного забезпечення ОВС України / Під ред. Л.В.Бородича. – К., РВВ МВС України, 2000.

М. ГУЦАЛЮК, *кандидат юридичних наук*

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Нині всі економічно розвинені країни перейшли на широке використання нових інформаційних технологій у виробничій, комерційній, банківській сферах. Технологічний прогрес надає можливість по-новому організувати процеси обробки, зберігання, пошуку та передавання інформації в будь-якій потрібній формі: усній, письмовій або візуальній – незалежно від відстані, часу та обсягу [1].

Найбільш активно розвиваються технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як е-торгівля, е-бізнес, е-уряд тощо. Це яскраво демонструє графік зростання кількості користувачів Мережі (табл. 1).

Електронна комерція охопила увесь світ, хоча насиченість електронних засобів у різних країнах є вкрай нерівномірною. Так, за даними Nua Ltd., у США та Європі – по 200 млн користувачів Інтернет, у Латинській Америці – 30 млн, Африці – 6 млн. Цей процес не минув і Україну, фінансові установи якої отримали доступ до міжнародних платіжних систем. Темпи зростання кількості користувачів Інтернет у нашій державі продовжують залишатися високими, на відміну від західних країн. Сьогодні їх приблизно 2 млн. Проте, це тільки 4 зі 100 громадян.

Разом з тим, в інформаційному суспільстві, виникли нові загрози, що стали серйозною перешкодою для інформаційного суспільства. Нові інформаційні технології почали активно використовуватися злочинним світом.

Наприклад, за даними Computer Emergency Response Team (CERT) – міжнародного авторитета в галузі безпеки Internet, заснованого Інститутом розробки програмного забезпечення Пітсбургського університету Карнегі-Мелона (Carnegie Mellon University Pittsburgh), останнім часом стрімко зросла кількість несанкціонованих проникнень до інформаційних систем (див. табл. 2).

Таблиця 1

Кількість користувачів у глобальній мережі Internet, млн