УДК 341.46:343.97:681.142.1

В.Д. ГАВЛОВСЬКИЙ, *кандидат юридичних наук,* начальник відділу
Міжвідомчого науково-дослідного центру з проблем боротьби
з організованою злочинністю при РНБО України
В.М. БУТУЗОВ, *кандидат юридичних наук,* головний науковий співробітник
Міжвідомчого науково-дослідного центру з проблем боротьби
з організованою злочинністю при РНБО України
К.В. ТІТУНІНА, науковий співробітник Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю при РНБО України

КОМП’ЮТЕРНА ЗЛОЧИННІСТЬ: МІЖНАРОДНИЙ ДОСВІД БОРОТЬБИ І ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

Анотація. *Щодо досвіду організаційної та функціональної структури зарубіжних правоохоронних органів з протидії комп’ютерній злочинності, тероризму та організаційно-правових проблем протидії боротьбі з комп’ютерною злочинністю в Україні.*

Поступове покращення якості обслуговування у сфері інформаційно-телекомунікаційних технологій (далі – ІТ-технологій) спричинило різкий сплеск комп’ютерної злочинності. Такий стан справ становить серйозну загрозу демократичним перетворенням та безпеці всім країнам світу, що примушує правоохоронні органи активно удосконалювати правові інструментарії, пристосовуючи їх до сучасних реалій.

За останні роки відмічається тенденція до створення та подальшої реорганізації у складі правоохоронних органів (поліції, органів сектору безпеки) держав світу спеціалізованих підрозділів з протидії комп’ютерній злочинності. Все частіше держави виходять з ініціативами щодо протидії комп’ютерній злочинності та комп’ютерному тероризму.

У **Сполучених Штатах Америки** інтенсивний контроль за кримінальною діяльністю в Інтернеті здійснює ФБР. У її складі в 1996 році створено Кіберпідрозділ (Cyber Division FBI), який функціонує на правах окремого управління та складається з чотирьох відділів: протидії незаконним втручанням у роботу комп’ютерних мереж (Network Intrusion Unit), протидії дитячій порнографії (Combating Child On Line Exploit), протидії шахрайствам (Fraud), протидії порушенням у сфері інтелектуальної власності (Intellectual Properties Rights). Відновлення, копіювання комп’ютерної інформації та віддалений доступ до вилученої інформації через комп’ютерну інформаційну мережу для ФБР забезпечує підрозділ Технологічного забезпечення розслідувань, у складі якого працює підрозділ по технічному забезпеченню роботи з вилученою комп’ютерною інформацією (CART). Для контролю за діяльністю провайдерів та користувачів Інтернету ФБР має систему Carnivore [1].

Секретна служба США (US Secret Service), яка входить до складу Міністерства фінансів США, проводить розслідування фінансових злочинів за трьома категоріями:

− злочини проти фінансової системи (фінансових установ (банків), шахрайство з використанням електронних засобів доступу (кредитних карток), відмивання грошей);

− злочини з використанням електронної апаратури (комп’ютерне шахрайство, шахрайство проти телефонних компаній);

− шахрайства проти державних фінансових програм (щодо казначейства США, махінації з електронним переказом грошових коштів, з продовольчими купонами) [2].

У 2003 році у США опубліковано “Національну стратегію захисту кіберпростору” [3],

в якій запропоновано послідовний та комплексний підхід до захисту важливих ІТ-технологій американської нації. Згідно із задекларованою інформацією стратегія розроблена після кількох років консультацій, до яких було залучено велику кількість осіб, у т. ч. працівників органів управління та організацій приватного сектору.

У **Російської Федерації** досвід правоохоронних органів щодо організації боротьби зі злочинами у сфері ІТ-технологій вказує на позитивний приклад взаємодії правоохоронних органів та держави. Починаючи з 1997 року правоохоронними органами було зроблено низку важливих кроків для забезпечення на законодавчому рівні протидії новим видам злочинів, насамперед, пов’язаним з комп’ютерними злочинами. У 1998 році було створено Управління по боротьбі зі злочинами у сфері високих ІТ-технологій (“УБПСВТ МВД России”), а вже до кінця 2000 року було сформовано 81 територіальний підрозділ. У 2001 році на зазначеній базі було створено Управління “К” МВС Росії [4].

Постійно вдосконалюючи структуру відповідно до сучасних вимог, 19 жовтня 2002 року було створено “БСТМ МВД РФ” – Бюро спеціальних технічних заходів МВС Росії, до структури якого увійшло Управління “К”. Сьогодні діяльність цього підрозділу направлена на припинення найрізноманітніших видів протиправних діянь, і в першу чергу злочинів у сфері ІТ-технологій – таких як злочини у сфері комп’ютерної інформації, електронне шахрайство, розповсюдження в мережі Інтернет “дитячої порнографії”, порушення авторських і суміжних прав та інших.

Враховуючи транснаціональний характер злочинів, що вчиняються з використанням засобів Інтернету, правоохоронними органами Росії в рамках ініціатив “Чисте з’єднання” (“Clean connecting”, форум 2006) в “БСТМ МВД РФ” (Управління “К”) з 1998 року створено та функціонує Національний контактний пункт (НКП), що діє у форматі 24/7 та призначений забезпечувати взаємодію з правоохоронними органами ближнього та далекого зарубіжжя [5]. У рамках проекту “Чисте з’єднання” МВС Росії пропонує державам-членам мережі національних контактних пунктів:

– сприяти розширенню міжнародної мережі національних контактних пунктів за рахунок приєднання до неї нових держав-членів;

– вживати заходів по формуванню національних правових механізмів, які забезпечували б обмін оперативною інформацією з правоохоронними органами інших держав.

У **Німеччині** у 1994 році у складі поліцейського управління м. Мюнхена було створено спеціальну групу по боротьбі зі злочинами у сфері ІТ-технологій (AG EDV). Пізніше у структурі федеральної поліції Німеччини створено групу “Технології”, до складу якої входять працівники кримінальної поліції, техніки, інженери та вчені різних спеціальностей. Їх задачею є як самостійне розслідування високотехнічних злочинів (електронного саботажу, шахрайств, грабежів тощо), так і сприяння роботі інших підрозділів, проведення досліджень і створення нових програмно-апаратних засобів для поліції, міжнародне співробітництво.

Корисним є досвід Німеччини щодо створення національних систем по контролю за діяльністю Інтернет-сайтів, що використовуються в терористичних цілях. Так, з метою інформаційного забезпечення та координації всіх спеціальних та правоохоронних органів Німеччини, задіяних у боротьбі з тероризмом, для пошуку, аналізу та контролю за вищевказаними веб-сайтами на початку 2007 року розпочав свою роботу “Інтернет-центр ФРН” (GIZ) [6]. Центр використовується в інтересах розвідки (BND), служби захисту Конституції (BfV), військової розвідки (MAD), Федерального агентства кримінальних розслідувань (BKA), Генеральної прокуратури (GBA), які відряджають (делегують) до GIZ своїх представників.

GIZ здійснює:

– пошук і дослідження відкритих веб-сайтів (призначених для роботи з широкою аудиторією, не призначених для зв’язку між терористами, фінансування терористичної діяльності тощо);

– інформування спеціальних і правоохоронних органів з наданням висновків та прогнозів щодо реальних та потенційних загроз;

– підтримку і координацію оперативних заходів спеціальних і правоохоронних органів, пов’язаних з використанням терористичними організаціями Інтернету.

Для вирішення термінових завдань в GIZ із залученням представників спеціальних і правоохоронних органів створюються тимчасові робочі групи, результати діяльності яких відображаються в інформаційному бюлетені окремим розділом.

У **Франції** у 1994 році було створено Службу з протидії зловживанням у сфері інформаційних технологій (SEFTI). Даний підрозділ підпорядковується Управлінню паризької кримінальної поліції, його компетенцією є боротьба з “інтелектуальним” піратством та “хакінгом”. Моніторингом мережі Інтернет займається спеціальний відділ у складі Бригади по захисту неповнолітніх, основним завданням якого є боротьба з Інтернет-порнографією. Розкриттям економічних злочинів у мережі Інтернет займається Відділ економічних та фінансових справ кримінальної поліції (SDAEF), а також спеціальна бригада по платіжним шахрайствам (BFMP), головним завданням яких є виявлення злочинів пов’язаних з використанням платіжних карток.

У лютому 2008 року Міністром внутрішніх справ Франції була оприлюднена французька Стратегія з питань боротьби з кіберзлочинністю. Мета Стратегії – співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) та правоохоронними органами з метою обміну інформацією та об’єднання зусиль у боротьбі з кіберзлочинністю [7]. У Стратегії визначено наступні основні напрями:

− модернізація методів розслідування за рахунок удосконалення технічних, нормативно-правових актів для ідентифікації користувачів Інтернету та розробка механізму перехоплення цифрових даних на відстані;

− розробка та встановлення правил співробітництва суб’єктів, що надають послуги з мережі Інтернет, зі службами, зацікавленими у боротьбі з кіберзлочинністю;

− створення нових форм інкримінування провини (визначення злочинного характеру діяння);

− зміцнення міжнародного співробітництва за рахунок укладання міжнародних угод, що дозволяють проводити віддалений обшук інформаційних ресурсів, без одержання попереднього дозволу країни, де розміщений сервер;

− приведення у відповідність до сучасних вимог зміцнення дій представників поліції та жандармерії за рахунок створення групи, що буде займатися боротьбою з шахрайствами в мережі Інтернет;

− підвищення кваліфікаційного рівня фахівців. Пропонується підготувати удвічі більше слідчих, які спеціалізуються на боротьбі зі злочинністю в інформаційних системах, що будуть працювати в Головному управлінні судової поліції, і слідчих у галузі цифрових технологій для жандармерії. Підготовка має здійснюватися завдяки партнерським стосункам із громадськими організаціями, а також французькою промисловістю;

− за погодженням з усіма міністерствами, зацікавленими в боротьбі з кіберзлочинністю, створення Міжвідомчого комітету з розслідування справ, пов’язаних з IT-технологіями й комунікаціями.

У **Республіці Білорусь** у лютому 2001 року у складі кримінальної міліції МВС було створено Управління оперативно-організаційної роботи, до якого увійшли: оперативно-контрольне відділення, відділення інформаційно-аналітичного супроводження розкриття злочинів та відділення по розкриттю злочинів у сфері IT-технологій [8].

Оперативно-розшукова діяльність у зазначеній сфері здійснюється вказаним управлінням МВС Республіки Білорусь та аналогічними низовими структурними підрозділами кримінальної міліції ГУВС Мінськміськвиконкому, УВС облвиконкомів та на транспорті, яким воно надає організаційну та методичну допомогу. Робота Управління здійснюється у тісній взаємодії з іншими підрозділами кримінальної міліції та управлінням інформаційних технологій МВС Республіки Білорусь.

Основними задачами спеціалізованих підрозділів органів внутрішніх справ Республіки Білорусь по розкриттю злочинів у сфері IT-технологій є:

− виявлення та розкриття злочинів у сфері телекомунікацій;

− боротьба з незаконним обігом радіоелектронних та спеціальних технічних засобів, припинення виготовлення, розповсюдження та використання на території Білорусі несертифікованої (забороненої для використання) радіотехніки та апаратури;

− боротьба зі злочинними посяганнями на конституційні права громадян щодо недоторканності приватного життя, таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, організацією незаконних міжміських та міжнародних переговорних пунктів, а також радіопіратством;

− захист від несанкціонованого доступу до службової інформації в інтересах власної безпеки органів та підрозділів внутрішніх справ Республіки Білорусь;

− участь у розробці та реалізації міжнародних зобов’язань Республіки Білорусь щодо ефективного співробітництва із зарубіжними правоохоронними органами з координації боротьби зі злочинами у сфері IT-технологій.

У **Великій Британії** у листопаді 2000 року уряд країни виділив 25 млн фунтів стерлінгів на створення спеціального поліцейського загону по боротьбі з кіберзлочинністю – Національного підрозділу по боротьбі зі злочинами у сфері високих технологій (National Hi-Tech Crime Unit, NHTCU), який складався з чотирьох відділів: відділу збору оперативної та загальної інформації, до функцій якого входить, зокрема, розвідка та аналітика; відділу здійснення операцій, що займається розслідуваннями; відділу технічного та інформаційного забезпечення; відділу застосування спеціальної техніки, який, зокрема, проводить відновлення й вивчення електронних доказів та експертні дослідження [9]. У квітні 2006 року NHTCU було розформоване, його функції та матеріали передані Агентству по боротьбі з організованою злочинністю (Serious Organised Crime Agency) [10].

У **Японії** у 1998 році Національним поліцейським управлінням було створено 13 спеціальних груп по боротьбі з комп’ютерними злочинами у восьми префектурах Японії, у тому числі декілька – у Токіо та Осаці. З 2002 року у структурі Національного поліцейського управління функціонує центр по боротьбі з хакерами, завданням якого є цілодобове стеження за несанкціонованими вторгненнями до японського сегменту мережі Інтернет та розвідка комп’ютерних атак, що готуються [11].

В **Індії** активну боротьбу з електронною злочинністю здійснює Центральне бюро розслідувань (Central Bureau of Investigation, CBI), у структурі якого з 2000 року функціонують сектор розслідування електронних злочинів та відділ по дослідженню кіберзлочинності (Cyber Crime Research & Development Unit, CCRDU). Відділ CCRDU займається збиранням, накопиченням та аналізом інформації про комп’ютерні злочини [12].

Зміни у цьому напрямі можна спостерігати і **в Україні**. Боротьба з цим видом злочинності визнана одним з головних завдань органів внутрішніх справ. У 2001 році у складі ДСБЕЗ МВС України створено і функціонує Управління (в даний час відділ) по боротьбі зі злочинами у сфері інтелектуальної власності та високих технологій, а в обласних апаратах у складі У(В)ДСБЕЗ – відділи (відділення, групи) [13, с.189].

У 2006 році з метою удосконалення організації діяльності підрозділів внутрішніх справ і розподілу їх компетенції з питань протидії правопорушенням у сфері інтелектуальної власності та ІТ-технологій, запровадження комплексного підходу до боротьби з даними видами злочинів було прийнято: Типове положення про підрозділи ДСБЕЗ по боротьбі з правопорушеннями у сфері інтелектуальної власності та ІТ-технологій; Інструкцію щодо організації діяльності підрозділів внутрішніх справ з протидії правопорушенням у сфері інтелектуальної власності та ІТ-технологій. Проте, аналіз даної Інструкції свідчить, що:

− у структурі органів внутрішніх справ не визначено службу, що відповідає за організацію та координацію діяльності по боротьбі зі злочинами у сфері ІТ-технологій;

− боротьбу зі злочинами у сфері ІТ-технологій в межах компетенції визначено завданням усіх оперативних служб ОВС, хоча тільки ДСБЕЗ має відповідні підрозділи.

Узагальнюючи вищенаведене, можна зробити **висновки**, що підрозділи ДСБЕЗ по боротьбі з правопорушеннями у сфері інтелектуальної власності та ІТ-технологій на сьогодні:

– є єдиними спеціалізованими підрозділами у системі ОВС, завданням яких є боротьба зі злочинами у сфері ІТ-технологій;

− у своїй діяльності зорієнтовані в основному на боротьбу зі злочинами економічної спрямованості (злочинами у сфері інтелектуальної власності, службовими злочинами на об’єктах галузі зв’язку та інформатизації);

− не мають повноважень, передбачених Конвенцією Ради Європи про кіберзлочинність.

Згідно з анкетуванням, проведеним науковцями Центру, 37,11 % опитаних працівників правоохоронних органів пропонують утворити нові спеціалізовані підрозділи з правами, передбаченими Конвенцією Ради Європи про кіберзлочинність, а 20,7% − вважають за доцільне проведення реорганізації існуючих підрозділів по боротьбі зі злочинами у сфері ІТ-технологій.

Крім того, слід зазначити, що ефективна протидія комп’ютерним злочинам може здійснюватися лише на основі високопрофесійної роботи спеціалізованих підрозділів у структурі компетентного державного органу з функцією координації боротьби з комп’ютерною злочинністю, який до цього часу в Україні відсутній. З метою виявлення та усунення або нейтралізації негативних соціальних процесів і явищ, що породжують комп’ютерну злочинність, є необхідність в утворенні організаційних структур у межах певного державного органу, а саме:

• ***по-перше***, створити спеціалізований підрозділ по боротьбі з комп’ютерними злочинами. Серед його завдань, з урахуванням положень Конвенції Ради Європи про кіберзлочинність, необхідно визначити наступні:

– організація та координація боротьби зі злочинами у зазначеній сфері (весь спектр злочинів, віднесених міжнародними та національними нормативними актами до комп’ютерних, а також злочини у сфері телекомунікацій);

– здійснення оперативно-розшукової діяльності в інформаційно-телекомунікаційних системах, у тому числі проведення оперативно-технічних заходів із збирання та перехоплення комп’ютерної інформації у масштабі реального часу;

– проведення аналізу оперативної обстановки у сфері ІТ-технологій. Подання аналітичних матеріалів та прогнозу щодо тенденцій та наслідків від проявів комп’ютерної злочинності на розгляд визначеному державному органу та органам державної влади;

– розроблення та впровадження в практичну діяльність органів внутрішніх справ ефективних методик документування комп’ютерних злочинів, а також традиційних злочинів, учинених із використанням ІТ-технологій;

– надання допомоги галузевим службам з питань розкриття злочинів, учинених із використанням ІТ-технологій;

– забезпечення засобами термінової комунікації взаємодії з компетентними підрозділами інших країн при документуванні та розкритті злочинів даного виду;

• ***по-друге***, створити єдиний орган (Контактний національний пункт), який відповідно до внутрішньодержавного законодавства і практики (з урахуванням міжнародних норм права) повинен забезпечувати надання технічних порад, збереження даних, збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних. Визначений орган для здійснення контактів у цілодобовій мережі повинен мати можливість термінового встановлення контакту з органом іншої країни.

Використана література

1. Cyber Investigations. – Режим доступу : http://www.fbi.gov/cyberinvest/cyberhome.htm

2. United States Secret Service: Mission Statement. – Режим доступу : http://www.ustreas.gov/usss/mission.shtml>

3. Гавловський В.Д. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії й практики / В.Д. Гавловський, М.В. Гуцалюк, Р.А. Калюжний та ін. – Запоріжжя: Просвіта, 2002. – С. 38.

4. История создания и развития “киберполиции” в России. – Режим доступу : http://www.cyb erpol. ru/cybercops.shtml#p_01

5. Материалы Международной прак. конференции по вопросам борьбы с киберпреступностью и кибертерроризмом (19-20 апреля 2006 года г. Москва). – М., 2006.

6. Немецкие спецслужбы создали “Совместный центр по наблюдению за Интернетом”. – Режим доступу : http://www.agentura.ru/equipment/?id=1176700740

7. Бутузов В.М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп’ютерній злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 19.

8. Лист Посольства Республіки Білорусь від 05.06.01 р. № 53.

9. Шеломенцев В.П. Боротьба з організованими злочинними угрупованнями у сфері використання банківських платіжних карток. – Режим доступу : http://mndc.naiau.kiev.ua/Gurnal/10text/g10_24.htm

10. The “National High-Tech Computer Crime Unit” is now “The Serious Organized Crime Agency”. – Режим доступу : http://www.nhtcu.org

11. Японская полиция создает специальный центр по компьютерным преступлениям. – Режим доступу : http://sp.sz.ru/99_04_23_02_.html

12. Rajkumar Dubey. India: Cyber Crimes “an unlawful act where in the computer is either a tool or a target or both” – In Indian Legal Perspective. – Режим доступу : http://www.crime-research.org/articles/Dubey/2>

13. Хахановський В.Г. Організаційні та методичні проблеми підготовки кадрів у сфері протидії комп’ютерній злочинності : матеріали науково-практичної конференції [“Міжнародне співробітництво в боротьбі з комп’ютерною злочинністю: проблеми та шляхи вирішення”]. – Донецьк: ДЮІ ЛГУВД, 2007. – С. 188-192.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~