

економічних відносинах: Закон України № 327/95-ВР від 15.09.1995р. // ВВР. 1995. №32. Ст.255. 3. Про заходи щодо підвищення відповідальності за розрахунки з бюджетами та державними цільовими фондами: Указ Президента України № 167/98 від 04.03.1998р // Офіційний вісник України. 1998. №17. 4. Про спрощену систему оподаткування, обліку і звітності малого підприємництва: Указ Президента України №727/28 від 03.07.1998р. // Голос України. 1998. 8 липня. 5. Про ознаки фіктивної фірми: Лист Державної податкової адміністрації України від 21.05.1999р. №229/4/25-1210 // Юридичний вісник України. 1999. 19 вересня.

*Надійшла до редколегії 12.10.2000*

*В.І. Антипов, канд. юрид. наук, начальник Науково-дослідного інституту проблем боротьби зі злочинністю НАВСУ*

### **ВИДИ ТРАНСНАЦІОНАЛЬНИХ ЗЛОЧИНІВ ЗА КЛАСИФІКАЦІЄЮ ООН ТА ЇХ ПОШИРЕНІСТЬ В УКРАЇНІ**

Світ став єдиним. Потік авіапасажирів зріс з 26 до 600 млрд людиномиль за 30 років. Світовий імпорт виріс з 330 до 3500 млрд дол. Мільярди доларів щодня обмінюються електронним шляхом, і приблизно половина цього багатства ховається від податків.

Для тих випадків, коли злочинні дії, операції або схеми порушують закони більш ніж однієї країни, кримінологи ввели термін «транснаціональна злочинність».

Аналіз міжнародно-правових документів дозволяє виділити три групи транснаціональних злочинів:

по-перше, це наднаціональні злочини, які посягають на інтереси людства загалом (агресія, геноцид, екоцид, апартеїд);

по-друге, злочини, що посягають на інтереси двох або більше держав (більшість наркозлочинів, контрабанда, транснаціональна торгівля зброєю й інші);

по-третє, злочини, що вчиняються на території однієї країни громадянами іншої країни з використанням її можливостей. Наприклад, злочини (вбивства, шахрайства тощо) замишляються і готуються на території України, а вчиняються в Італії, або навпаки.

ООН розділила всі транснаціональні злочини на 16 груп [Див.: 1]. Як показало вивчення, більшість із них може вчинятися із застосуванням інформаційних технологій.

Деякі взагалі не можливі без цього. Це, перш за все, як її іменує класифікація ООН – комп'ютерна злочинність.

1. *Комп'ютерна злочинність.* До неї доцільно віднести випадки, коли комп'ютер – є предметом злочину.

Справжній «комп'ютерний злочин» передбачає атаку на комп'ютер об'єкт несанкціонованого доступу (НСД) в основному для отримання інформації, що зберігається на ньому, використання даної системи безкоштовно (крадіжка послуги) або її пошкодження. Більшість (хоч не всі) таких порушень передбачають несанкціонований доступ до системи (тобто «злом» системи).

### 1.1. Розкрадання інформації.

Правопорушення, пов'язані з розкраданням інформації, можуть набувати різних форм залежно від характеру системи об'єкта НСД.

Секретна інформація, що зберігається на комп'ютерах правоохоронних і військових органів, є вельми привабливим об'єктом для багатьох, включаючи осіб, стосовно яких ведеться кримінальне розслідування, терористичні організації й агентів іноземних розвідок.

Секрети фірм є метою для хакерів, які атакують неурядові системи. У деяких випадках інтерес виявляється до економічно важливої інформації. Наприклад, в одній справі хакер отримав доступ до системи бронювання номерів у готелі для того, щоб викрасти номери кредитних карток. В іншій справі хакер викрав виробничу інформацію, що була власністю фірми, на суму більш ніж за один мільярд доларів, яка дозволила б йому створити систему стільникового телефонного зв'язку. Останній випадок підпадає під категорію розкрадання інтелектуальної власності. Вона включає не тільки крадіжку засекреченої технології, але також і набагато простіші злочини, пов'язані з несанкціонованим розмноженням матеріалів, захищених авторським правом, особливо комп'ютерні програми (наприклад, попередні випуски комерційних програм), які недоступні в іншому вигляді.

Іноді спроба НСД пояснюється бажанням отримати інформацію особистого характеру про іншу особу, або як засіб для досягнення мети (наприклад, із метою вимагательства або щоб скомпрометувати свою жертву внаслідок розголошення цієї інформації). Серед предметів впливу в даній категорії справ – системи, що зберігають історію хвороби, телефони клієнтів (наприклад, номери, не включені в телефонний довідник) або інформація про кредитні картки покупців.

### 1.2. Розкрадання послуг.

До другої групи правопорушень належить отримання несанкціонованого доступу до якоїсь системи, щоб безкоштовно скористатися послугами, що надаються нею. Наприклад, злочинець може використати свій комп'ютер, щоб проникнути в комутаційну телефонну систему (включаючи приватні системи, такі як приватні АТС з виходом в загальну мережу) із тим, щоб незаконно скористатися послугами по наданню міжміського телефонного зв'язку. (Такого роду маніпуляції з телефонним зв'язком називають «фоун-фрейкинг» або просто «фрейкинг» ). У деяких випадках хакери використали ресурси систем НСД для рішення задач, що вимагають складних розрахунків, наприклад, для визначення закодованих паролів, які вони викрадали з інших вузлів. Злочини, пов'язані з крадіжкою послуг, відбуваються в процесі «заплутування слідів» («уивинг» ), коли хакер проходить через численні системи (і можливо численні телекомунікаційний мережі, такі як Інтернет або системи стільникового і наземного телефонного зв'язку), щоб приховати своє справжнє ім'я й місцезнаходження. При такій ситуації єдиною причиною для проникнення в даний комп'ютер може бути бажання використати його як засіб для атаки на інші системи.

### 1.3. Пошкодження системи.

Навіть якщо зломщик не збирається отримати інформацію з даного комп'ютера або використати його, він може переслідувати ряд інших цілей. Мабуть, найбільш очевидним є той випадок, коли зловмисник намагається зруйнувати або змінити дані, що є важливими для власника або одного чи багатьох користувачів системи – об'єкта НСД. Зловмисні дії такого роду часто вчиняються незадоволеними колишніми співробітниками, які хочуть помститися за несправедливе, на їх думку, ставлення до себе. Дивіться, наприклад, справа «Сейлан проти Сполучених Штатів», 92 F. 3d 865 (9-й округ, 1996) (незабаром після звільнення колишня співробітниця банку змінила або стерла файли в комп'ютерній системі).

У тих випадках, коли порушник здійснює НСД у систему для досягнення більш глобальних цілей, пошкодження можуть бути не такими явними. Найбільш відомі приклади таких порушень пов'язані з комп'ютерами телефонних мереж. Був випадок, коли хакер маніпулював комутаційним телефонним обладнанням, щоб забезпечити собі перемогу в конкурсі слухачів, що дзвонили на місцеву радіостанцію; нагородою за його зусилля повинні були стати два автомобілі Порше і 30 тис. доларів готівкою.

Комп'ютери, сполучені з Інтернетом, також можуть бути об'єктом таких атак. Маршрутизатори комп'ютера, що визначають шлях, по якому пакети інформації переміщуються в Інтернеті, аналогічні телефонним комутаторам і тому є припадними об'єктами для досвідчених хакерів, які хочуть порушити або навіть змінити маршрут «трафіка» в мережі.

У декількох випадках хакери встановлювали програми – «шукачі», що таємно перехоплюють паролі користувачів під час їх реєстрації. Оскільки користувачі часто оперують одним і тим же паролем в більш ніж одній комп'ютерній системі (ігноруючи розсудливість, що диктується правилами безпеки), оволодіння паролем користувача часто дає хакеру можливість легкого доступу в інші комп'ютерні системи, в яких цей користувач має рахунки. Такий доступ у свою чергу дуже полегшує хакеру задачу пошкодження цих інших систем.

Усі інші транснаціональні злочини можуть вчинятися як без застосування комп'ютерів, так і з їх використанням. Зрозуміло, що в останньому випадку більш важко розкрити й розслідувати ці злочини.

Зараз розглянемо більш традиційні транснаціональні злочини, які однак все частіше вчиняються із застосуванням інформаційних технологій. При цьому комп'ютер виступає вже не як предмет, а як знаряддя злочину.

2. *Відмивання грошей* націлене на те, щоб нелегально отримані капітали представити як законні. Значна частина грошових коштів добувається нечесним шляхом за рахунок хабарництва, корупції, діяльності на «чорному» ринку, порушень податкового законодавства, особливо за рахунок контрабанди зброї, збуту краденого, предметів мистецтва й наркотиків. Установлено, що щорічно на світовому ринку нелегально продається наркотиків на суму 300-500 млрд дол. Що ж наркобарони роблять із таким колосальним багатством? Безпосередньо з ними – нічого, тому що це «брудні» гроші. Але якщо їх «відмити» за кордоном, то вони могли б повернутися

до наркоділів і на них можна купити цілі галузі промисловості, нерухо- мість і політичний вплив.

Стандартним способом відмивання грошей залишається переміщення готівки за межі країни (літаком, пароплавом або у вантажівці з подвійним дном), вкладення готівки на банківські рахунки за кордоном за допомогою багаторазових міжнародних переказів, внаслідок чого джерело походження грошей уже неможливо відстежити. А ці транзакції здійснюються саме за допомогою електронних платежів. Зовсім не треба їхати до Швейцарії, щоб зробити переказ із Швейцарського банку до банку Нью-Йорка. У результаті гроші здаються «чистими» і легально вкладаються в економіку, хоч і знаходяться під контролем організованої злочинності. Істинні масштаби відмивання грошей невідомі.

3. *Терористичні акти* продовжуються. За допомогою сучасних засобів пересування й зв'язку вчиняти їх полегшало набагато. При цьому ті країни, чий уряди займають тверду позицію стосовно терористів, повинні бути готові до їх несподіваних відповідей. Поки ще тільки створюється міжнародний механізм, що забезпечує арешт або підсудність міжнародних терористів. Кримінологи ще тільки намагаються дослідити цю проблему, що не залежить від державних кордонів. При цьому слід враховувати – для того, щоб організувати катастрофу на залізниці, зовсім не обов'язково скручувати рейки. Хакер може перехопити управління світлофорами чи засобами переведення стрілок і катастрофа гарантована. Кібертероризм – так пропонують іменувати такі злочини деякі дослідники.

4. *Угон або захоплення літаків* – це мабуть різновид тероризму. Авіація особливо страждала від угонів літаків і в 70-ті та 80-ті роки.

Тільки у окремих випадках діяли одинаки, що вимагали викупу, в більшості ж інцидентів злочинці висували політичні вимоги, типові для терористів. Вони прагнули демонструвати силу, заявити про свої організації і пропагувати свою ідеологію.

Реакція на захоплення літаків повсюдно була швидкою і результативною. Можливість захоплення літаків існує і сьогодні, хоч частота цих акцій поменшала. Але зараз створюються умови для так званого віртуального угону.

5. *Крадіжка інтелектуальної власності*. Поняття «крадіжка інтелектуальної власності» включає порушення прав авторів і виконавців, а також незаконне використання знаків охорони авторського права і торгових марок. Спокусу незаконно відтворити захищені твори і продати їх дешевше або за ту ж ціну велике, особливо в країнах із нерозвиненою економікою. Масштаби збитку країн-виробників важко піддаються вимірюванню в грошовому вираженні. Тільки від нелегального використання програмного забезпечення, як підрахувала Асоціація американських видавців програмного забезпечення, збиток становить 7,5 млрд дол. в рік. Підробку знаків охорони авторського права не можуть здійснити дрібні підприємства або підприємці-одинаки. Тут необхідні координація і налагоджена система збуту часто на транснаціональному рівні.

## 6. Транснаціональні фінансові оборудки. Віртуальні казино.

Попри наявність серйозних проблем у нормативному регулюванні та практиці контролю за гральним бізнесом у його традиційних формах (казино, букмерські контори, тоталізатори на іподромах, ставки на результати більярдних змагань тощо) він усе ж не залишається поза увагою законодавця та органів виконавчої влади, в т. ч. правоохоронних органів. Цього, на жаль, не можна сказати про так звані «віртуальні казино».

Бурхливий розвиток глобальної мережі Інтернет і пов'язаних з нею технологій несе (як і усякий прояв прогресу) не лише позитивні наслідки, а й усілякі збочення й негаразди. Одним із них є розповсюдження азартних ігор, які повністю опинилися за межами будь-якого регулювання й контролю. Відсутність останніх визначається самою природою вільного доступу до ресурсів Інтернету й свободи розміщення на сторінках його сайтів будь-яких ресурсів. Першими антисоціальними проявами в Інтернеті стали порно-сайти. Потім пішла хвиля віртуальних казино. Спочатку, як і все, що стосується Інтернету, ця хвиля «накрила» США. Реакція не забарилася.

23 липня 1998 р. Сенат США переважною більшістю голосів (90 проти 10) затвердив білль, що забороняє азартну гру в Інтернеті.

Цей білль розповсюджує на Інтернет й інші сучасні засоби зв'язку діючий закон, який забороняє використання для організації азартної гри телефонного зв'язку. Сенатори визнали, що гральний бізнес в Інтернеті практично не піддається контролю й регулюванню і представляє велику небезпеку для дітей, які зможуть грати, використовуючи кредитні картки батьків. У той же час білль дозволяє використання Інтернету для проведення державних лотерей і гри, в якій учасники укладають парі між собою (звичайно – із приводу результатів майбутніх спортивних змагань) – «pari-mutuel betting». Згідно з біллем, провайдери Інтернету зобов'язані класти край розміщенню гральних сайтів у своїх мережах. Організаторам віртуальних казино загрожує чотири роки ув'язнення й штраф в 20000 доларів, а гравцям – 3 місяці ув'язнення і 500 доларів штрафу.

Оскільки для доступу до Інтернету звичайно використовуються телефонні лінії, законність організації азартної гри в мережі й до прийняття білля викликала сумнів. До того ж у деяких штатах азартна гра заборонена взагалі. Тому велика частка фірм, що працюють у цій сфері, розташовується за межами США, звичайно на території маленьких острівних держав. Їх бізнес розвивається вельми успішно: за оцінками Міністерства юстиції, в минулому році американці поставили 600 млн. доларів тільки на спортивні тоталізатори, що функціонують у мережі.

Індустрія починає самоорганізовуватися: так, Рада по інтерактивній грі (Interactive Gaming Council, IGC) об'єднує вже 55 фірм. Реакція цього співтовариства на рішення американських законодавців не примусила себе чекати: представник IGC Сю Шнайдер (Sue Schneider) у своєму коментарі сказала, що інші країни знайшли розв'язання проблеми контролю, а заборона призведе не до зникнення віртуального казино, а до захоплення цього бізнесу кримінальними структурами. Приблизно в такому ж дусі витрима-

ний великий за обсягом прес-реліз компанії PlayStar Corporation, що займається розробкою гральних систем. У цьому документі заборона порівнюється з сумно звісним «сухим законом», прогнозується прихід в індустрію мафіозі («Е-Капоне», із слів президента PlayStar) і висловлюється надія на те, що Палата представників поставиться до законопроекту більш уважено. Представники грального бізнесу вважають також, що побоювання про можливе залучення до гри дітей не мають під собою досить вагомих підстав.

А тим часом Верховний суд Каліфорнії розглядає курйозний позов Синтії Хейнс (Cynthia Haines), що програла в Інтернеті біля 70 тис. доларів. Тепер вона хоче отримати ці гроші з платіжних систем Visa і MasterCard: на її думку, ці компанії, по-перше, не повинні були відкривати рахунки власникам ігрових сайтів, а, по-друге, блокувати перекази грошей з її рахунку до віртуального казино, оскільки азартні ігри в штаті Каліфорнія, де вона живе, заборонені.

З'являються також повідомлення про нову азартну гру. Компанія GTECH, яка займається організацією лотерей у США й інших країнах, готується запустити онлайніві лотереї. Доступ до них, за запевненнями GT, буде відкритий тільки для користувачів, що проживають за межами США. А британське відділення Microsoft хоче надати жителям Великобританії онлайнівий доступ до добродійної лотереї Червоного Хреста «Millions2000».

Питання про азартну гру в Інтернеті розглядається і Європейською комісією, яка, однак, досі вивчає стан проблеми і розробляє заходи з регулювання. Заборони на гру в Інтернеті в Європі, очевидно, не буде, а це позбавляє значення й американську заборону, якщо вона все ж таки буде прийнята Конгресом. Зараз азартна гра в Інтернеті офіційно дозволена (крім дрібних країн Карибського басейну, Австралії й Швеції).

Що стосується країн СНД, неабиякий інтерес становить інформація з Калмикії (Російська Федерація), де прийнятий закон, що дозволяє створення Інтернет-казино і заохочує гральний бізнес. 10 березня 1999 р. парламентом Республіки Калмикія був прийнятий закон «Про розвиток грального бізнесу в Республіці Калмикія». Як повідомляє Міністерство інвестиційної політики Калмикії, законом передбачені ліберальні вимоги для організації грального бізнесу. Також закон допускає створення Інтернету-казино. У повідомленні підкреслюється, що такого роду закон у Росії приймається вперше.

Тим часом, в Україні такі ж процеси розгортаються без особливої реклами й дискусій щодо доцільності чи небажаності дозволу на відкриття віртуальних казино. Вони вже є й успішно працюють. Показово, що за деякими з них стоять іноземні організації та підприємці. Ретельна перевірка, можливо, дозволить стверджувати, що всіма віртуальними казино в Україні володіють іноземці, що призводить, серед іншого, до безконтрольного вивозу капіталу. Розглянемо механізм функціонування віртуального ігрового закладу на прикладі казино «Адмірал».

Користувач мережі Інтернет набрав адресу <http://admiral.mediana.net.ua> (адресу цього закладу, як і адреси інших віртуальних казино, легко знайти за

допомогою стандартних пошукових систем Інтернету), опиняється на першій (як ще кажуть – початковій, домашній) сторінці віртуального казино «Адмірал». Натиснувши кнопку з бажаною мовою спілкування – російська або англійська, відвідувач отримує доступ до таких сторінок цього сайту, як: «Засновники», «Правила ігор», «Відкриття рахунку», «Реєстрація» та інші.

На сторінці «Засновники» ми не знайдемо офіційних даних про власників казино. Повідомляється лише, що правами на програмний продукт (мабуть, той, що дозволяє грати з персонального комп'ютера в ігри віртуального казино) володіє якась «Асоціація грального бізнесу й казино Східної Європи». Указується її адреса – Литва, Вільнюс, вул. Вітяніса, 3.

Вивчення інших сторінок сайту казино «Адмірал» дозволяє зрозуміти умови та порядок гри в ньому.

Спочатку слід завантажити з цього сайту на свій комп'ютер величезну за обсягом комп'ютерну програму казино «Адмірал». Оскільки вона сягає 2,5 мегабайт у запакованому вигляді, її завантаження займе чимало часу. Як результат, потенціальний гравець, що не став повноправним членом казино, вже починає витрачати гроші (у даному випадку – це оплата телефонного часу та оплати послуг провайдера).

Після того як програма буде на жорсткому диску гравця, він повинен її інстальювати, тобто привести у робочий стан. Потім за допомогою цієї програми треба через Інтернет з'єднатися із сервером (сайтом) казино «Адмірал», де новому гравцю буде повідомлено його умовне ім'я (так званий Login), пароль (Password), який треба використовувати, щоб отримати доступ до гри, та ключове слово (KeyWord), яке потрібно, щоб перерахувати гроші на рахунок казино і, якщо повезе, отримувати виграш. Ця процедура йменується реєстрацією.

Наступним кроком є заповнення платіжного доручення, форма якого люб'язно розміщена на сусідній сторінці сайту, і перерахування певної суми грошей до одного з обраних банків. Список банків з усіма необхідними реквізитами знаходиться тут же.

Як обіцяє віртуальний адміністратор, протягом 1 години після надходження засобів гравцю буде видана відповідна кількість ігрових фішок. Це слід розуміти так, що при черговому відвідуванні казино «Адмірал» новий гравець побачить на екрані свого монітора зображення своїх фішок, які він має право використовувати, щоб робити ставки в рулетку, карти тощо. Тобто, тільки отримавши віртуальні фішки за реальні гроші, можна починати гру. Щоправда, власники казино обіцяють викупити фішки у гравців за першою їх вимогою.

Якщо ж фішки купувалися не для того, щоб їх відразу продати назад (при цьому, навіть якщо ціна купівлі й продажу буде однакова, відбудуться втрати засобів у вигляді сплати банку за трансферт), можна розпочати гру. У казино «Адмірал» пропонуються три азартні гри: «Американська рулетка», «Карибський покер» і «Блек Джек». У випадку програшу поставлених на кон фішок, із рахунку гравця адміністрацією казино знімаються відповідні гроші. При виграші – відповідні суми на цей рахунок перераховуються, що відображається у вигляді збільшення кількості віртуальних фішок. За

вимогою гравця, як обіцяють власники казино, його виграш може бути перерахований на інший рахунок, тобто не рахунок віртуального казино «Адмірал».

Аналіз викладеної схеми відразу показує її, м'яко кажучи, невігідність для гравців.

По-перше, як вступний внесок, так і можливий виграш перераховуються на рахунок, власником і безконтрольним користувачем якого є не гравець, а власники казино.

По-друге, на відміну від реального казино, гравці віртуального казино ніяк не можуть проконтролювати, що колесо рулетки обертається вільно, що зображення карт гравців не бачить круп'є тощо. Оскільки відсутнє законодавство, яке б регулювало умови роботи віртуального казино, гравці не можуть сподіватися й на те, що хтось (якась наглядова інстанція) – контролює додержання власниками казино правил гри.

По-третє, відсутність вірогідних офіційних даних про засновників (власників) казино робить примарними шанси гравців отримати свої гроші у випадку, якщо одного разу вони не знайдуть в Інтернеті сайту «Казино «Адмірал».

Дуже показовою в цьому виглядає така обставина. На одній зі сторінок, де роз'яснюються правила гри, є попередження, що у випадку зникнення телефонного зв'язку після роздачі карт або після запуску рулетки, усі поточні ставки вважаються програшними. З урахуванням якості вітчизняних телефонних мереж українські гравці віртуальних казино відразу повинні значну суму грошей виділити на оплату ставок, які будуть програні через обриви зв'язку.

Викладене дозволяє зробити висновок про те, що в існуючому вигляді азартні (на реальні гроші) ігри через мережу Інтернет ніяк і ніким не контролюються, українські гравці віртуальних казино приречені на програш, з огляду на іноземне походження казино коштів «спливають» за кордон, прибутки власників казино в Україні не оподатковуються.

*7. Шахрайство зі страховкою* – різновид фінансових обмудок. Страхова індустрія стала міжнародною, тому шахрайство в будь-якій країні тепер зачіпає всіх. Глобальний збиток від цього виду злочинів не підрахований. Однак відомо, наприклад, що втрати Австралії від страхових шахрайств щорічно досягають 1,7 млрд австралійських дол., в США щорічні збитки дорівнюють 100 млрд дол.

Організована злочинність прагне до участі в страховому шахрайстві шляхом об'єднання дрібних підприємців в окремих галузях (наприклад, страхування морських перевезень) або ж проникаючи в саму страхову індустрію.

В Україні проблема криміногенності страхового бізнесу виникла в середині 90-х років у зв'язку з масовим обманом індивідуальних страхувальників – громадян. Це було шахрайство за зразком і подібністю до трастових компаній. Зараз, на наш погляд, потрібно звернути увагу на попередження шахрайських операцій страхових компаній стосовно інтересів держави.



Поки що є види транснаціональних злочинів, безпосереднє вчинення яких відбувається без використання комп'ютерів. Але і вони не можуть бути вільними від новітніх технологій на стадіях готування.

Електронна пошта і сеанси спілкування можуть бути використані злочинцями для планування або координації практично будь-яких незаконних дій або навіть для того, щоб загрозувати своїм жертвам і займатися вимагательством. У міру того, як набувають все більшого розповсюдження надійні методи кодування інформації, можна чекати, що злочинці будуть використовувати таку технологію, щоб уникнути виявлення при плануванні і здійсненні своєї незаконної діяльності.

8. *Крадіжки творів мистецтва й предметів культури.* Ці злочини потенційно загрожують культурній спадщині всіх народів. Гробниці й пам'ятники розорилися ще з часів єгипетських фараонів. Але вдосконалення зброя злочини і високий попит на предмети культури, а також простота їх транспортування дозволили міжнародним злодіям і грабіжникам розробити систему, яка дає можливість позбавити цілий регіон і навіть країну культурної спадщини. Установлено, що щорічно викрадається творів мистецтва на суму 4,5 млрд дол. для продажу їх на світовому ринку. Зараз у розшуку знаходяться 45 тис. творів мистецтва, причому щомісяця цей список поповнюють 2 тис. нових предметів.

В Україні від злочинних посягань культура несе суттєві матеріальні, а частково й духовні втрати. Лише в галузі археології від незаконних «диких» розкопок такі втрати досягають астрономічних розмірів. Тільки у Бахчисарайському районі (Крим) пограбовано 90 відсотків могильників. На думку директора Кримської філії Інституту археології Національної академії наук України В. Міща, у результаті таких розкопок тільки з Кримського півострова протягом року за кордон вивозиться раритетів щонайменше на 60 млн доларів [Див.: 2].

Облік об'єктів культурн є однією з умов їх виявлення, збереження й охорони. Однак на сьогодні в Україні досі не існує єдиної системи державного управління справою охорони пам'яток, яка розпорощена між кількома відомствами.

Постановою Кабінету Міністрів України від 12 серпня 1992 р. № 466 започатковано ведення Державного реєстру національного культурного надбання, до якого заносяться об'єкти матеріальної й духовної культури: виняткової історичної, художньої, наукової чи іншої культурної цінності, у т.ч. пам'ятки історії, археології, містобудування й архітектури, мистецтва, документальні пам'ятки та інші об'єкти, що становлять виняткову цінність для історії, культури, етнології чи науки взагалі. З 1992 р. такий реєстр не створено, що обумовлює неможливість використання можливостей Інтерполу у розшуку викрадених предметів.

9. *Незаконна торгівля зброєю.* Збройні конфлікти в різних точках земної кулі неможливо уявити без міжнародної мережі виробників і постачальників зброї. Масштаби їх діяльності – поза статистичними оцінками. Точна інформація про незаконну торгівлю зброєю відсутня, незважаючи на те, що поводження зброї і військового спорядження піддається відстежен-

ню. Але численні повідомлення у пресі вказують на те, що ця проблема не обминула Україну [3, с. 6].

Найнебезпечнішим аспектом цих злочинів стало нелегальне перекидання радіоактивних матеріалів. Поки що жодна з подібних спроб не увінчалася успіхом, радіоактивні матеріали не дійшли до адресата. У ряді випадків самі викрадачі, перевізники і оточуючі їх люди зазнавали впливу радіації. За рекомендацією міжнародних організацій багато країн вже вжили заходів у відповідь, встановивши міжурядовий контроль за джерелами радіоактивних матеріалів.

10. *Піратство*. Це давно забуте явище відродилося в середині 70-х років і проявляється при перевезенні наркотиків з Південної й Центральної Америки в США на яхтах або риболовецьких судах, які злочинці захоплюють у відкритому морі або в порту, знищуючи їх власників і екіпажі. Постраждало вже декілька тисяч суден.

Піратство також поширене у вузьких судноплавних каналах. Тисячі видів з Африки, Південно-Східної Азії і Латинської Америки не пропускають можливості поживитися цінностями і вантажами, що знаходяться на борту кораблів, користуючись тим, що судна стоять на якорі або йдуть на малій швидкості. Є версія, що піратство в Південно-Східній Азії контролюється організованими злочинними групами, пов'язаними зі збройними силами. Кримінологи схиляються до висновку, що одночасні піратські напади в різних частинах світу зовсім не випадкові, їх сліди тягнуться до одного центру.

Україна – морська держава. Крім того, розпочинає відроджуватися річкове судноплавство. Не можна виключати потенційної небезпеки появи морських і річкових піратів у зоні юрисдикції України.

11. *Захоплення наземного транспорту*. Включення цього виду злочинів у класифікацію ООН може викликати здивування. У рамках однієї країни угон вантажівки визначається як крадіжка. Але світова економіка мінляється, і проходження вантажівок на величезні відстані з Східної Європи в Західну або з республік Середньої Азії у країни Балтії стало повсякденною реальністю. На жаль, число випадків зникнення вантажівок зростає пропорційно зростанню товарообігу. Точні масштаби цього виду злочинів невідомі. Тільки чотири держави відповіли на анкету ООН на цю тему. У майбутньому ця проблема стане ще більш зловідомою через зростаючу прозорість кордонів і зростання організованої злочинності, особливо в країнах Східної Європи.

Думається, дана проблема для України, на відміну від проблеми піратства, перестала носити абстрактний характер. Було б вельми цікаво провести спеціальне вивчення щодо наявності випадків зникнення (назавжди або тимчасово) вантажівок з товарами й масштабів цього явища.

12. *Екологічна злочинність*. Жертвою екологічних злочинів стає населення всього світу. Переважно як злочинці виступають підприємства, що ігнорують екологічні норми і вступають у зговір із творцями системи контролю за виробництвом. Це стало особливо очевидним, коли виробництво розпочали переносити в країни, що розвиваються. Тут механізм контролю

практично відсутній або діє так, як зручно іноземним виробникам, які шедро витрачаються на хабарі й підкуп чиновників. Бідні нації віддають перевагу індустріалізації, що забезпечує їм зайнятість і зростання національного продукту. Організована злочинність вже знайшла свою нішу в цій сфері, особливо в перевезенні і похованні небезпечних продуктів [4].

13. *Торгівля людьми* набирає сили і включає в себе перевезення емігрантів-нелегалів, жінок для заняття проституцією, наймані сили для роботи в рабських умовах, домашньої прислуги з країн, що розвиваються, дітей для незаконного усиновлення за величезні суми [5].

Правова база для припинення цього виду злочинів цілком достатня. В умовах усе більшої прозорості кордонів ці закони стають більш жорсткими. Але проблема виходить на новий виток, оскільки жителі третього світу прагнуть до переселення в щодо благополучні країни. Потік нелегалів переважно контролюється організованою злочинністю. Ті, хто прибуває до розвинених країн, як правило, не мають роботи і вливаються в маргінальну верству, що експлуатується бере участь у злочинах.

14. *Торгівля людськими органами*. Відомо, що перша пересадка нирки була зроблена в 1954 р., легені – в 1963 р., серця – в 1967 р. На сьогодні проведено майже півмільйона операцій по пересадці нирок. Трансплантологія стала галуззю медицини і породила індустрію по постачанню донорськими органами. Для цих цілей в США створено 69 спеціалізованих агентств. Нелегальний бізнес по поставці органів для пересадок приносить величезні гроші і перемістився в країни третього світу. «Донорів» часто вбивають ради органів, або ж ними стають діти бідняків, що продають цей товар за жадливо низьку плату. Після публікацій в світовій пресі перших викриттів нелегальної торгівлі людськими органами в ряді країн були створені спеціальні комісії з розробки законодавчих актів, що регулюють цей процес. В Україні цього поки що не зроблено. Є немало доказів того, що нелегальна поставка органів із країн третього світу контролюється організованою злочинністю країн Західної Європи.

15. *Незаконна торгівля наркотиками*. Її оборот у світовому масштабі оцінюється в 300-500 млрд дол. Такі важливі документи, як Загальна конвенція про наркотики 1961 р., Конвенція про психотропні речовини 1971 р. й Конвенція ООН проти нелегальної торгівлі наркотиками і психотропними речовинами 1988 р., створили базу для міжнародного контролю.

16. *Фіктивне банкрутство*. Інтернаціоналізація торгівлі перетворила фіктивні банкрутства з локальних злочинів у міжнародні. Реальний розмах цього явища не піддається обліку. Вибіркові аналізи показують: мафія, скупивши підприємство, доводить його до банкрутства, хоч прибутки великі. У цій сфері необхідно об'єднати міжнародні зусилля по співпраці.

#### Список літератури:

1. Distr. GENERAL E/CN. 15/1993/3 11 January 1993.
2. Голос України. 08.05.1997 р.
3. «Чорний ринок»? зброя на будь який смак // Україна. Європа. Світ. 1994. №12.
4. Голос України. – 1995. – 21 сичн.
5. Голос України. – 1995. – 21 берез.

Надійшла до редакції 20.03.2000