Нелегальна міграція – об'єкт міжнародного права. Її існування зумовлює поведінку суб'єкта міжнародного права – держави. Ця поведінка здійснюється в двох площинах: у взаємодії з іншими державами для забезпечення ефективності боротьби з нелегальною міграцією та дотримання міжнародних зобов'язань у межах державної території щодо попередження та запобігання нелегальній міграції. Боротьба з нелегальною міграцією здійснюється шляхом імплементації міжнародних стандартів (незалежно від джерела походження: універсальних, регіональних чи двосторонніх) у національне законодавство. Саме держава в особі інституцій, які виконують її прерогативи, встановлює відповідний режим, визначає засоби та способи його досягнення.

У сучасних умовах криміналізація нелегальної міграції дозволить вирішити декілька завдань одночасно. Перш за все, формування складу злочину забезпечить підвищення загальної та індивідуальної превенції: кримінальна відповідальність за факт незаконного перебування на території країни відверне багато випадків стихійного переміщення – на "непрофесійній" основі, рецидиви тощо. З іншого боку, це дозволить спростити процес опікування нелегальними мігрантами – після виявлення з ними будуть поводитися як із звичайними злочинцями відповідно до норм чинного законодавства.

Видається, найбільш доцільним та ефективним засобом у боротьбі з нелегально міграцією є криміналізація нелегальної міграції як протиправного перебування іноземця на території держави, поведінка індивіда матиме статус злочину міжнародного характеру і на базі цього набере нових форм міжнародне співробітництво.

Список використаної літератури:

1. Нєклєвіч К. Французи чухають потилиці / Пер. Ю. Гудз // Gazeta Wyborcza. – 2006. – 08 трав. – С. 13-14.

2. Про зловживання в галузі міграції і про забезпечення працівникам-мігрантам рівних можливостей і рівного ставлення: Конвенція № 143, прийнята від 24.06.1975 р. [Електронний ресурс] // Режим доступу: http://zakon2.rada.gov.ua/laws/show/993_163.

Надійшла до редакції 04.04.2012

ШКОЛЬНИЙ В.Б., кандидат юридичних наук
(Національна академія внутрішніх справ)

УДК 343.9 : 681:142

ДЕЯКІ ПРИЧИНИ ВИНИКНЕННЯ І РОЗВИТКУ ЗЛОЧИННОСТІ У СФЕРІ ВИКОРИСТАННЯ ЕОМ

Розглянуто основні причини виникнення і розвитку злочинності у сфері використання ЕОМ. Надано класифікацію таких причин за ступенем абстрагування. Зроблено історичний нарис першопричин виникнення зазначеного виду злочинності. Запропоновано низку профілактичних заходів, зокрема криміналізація деяких діянь.

Ключові слова: *комп'ютер, злочин, Інтернет, криміналістика, боротьба зі злочинністю.*

Рассматриваются основные причины возникновения и развития преступности в сфере использования ЭВМ. Осуществляется классификация таких причин по степени абстрагирования. Приводится исторический очерк первопричин возникновения указанного вида преступности. Предлагается ряд профилактических мероприятий, в частности криминализация некоторых деяний.

Ключевые слова: *компьютер, преступление, Интернет, криминалистика, борьба с преступностью.*

The article reviews the main causes of crime and development in the use of computers. Courtesy of the classification of such reasons by the degree of abstraction. Made a historical sketch of the root causes of this type of crime. A series of preventive measures, including criminalization of certain acts.

Keywords: *computer crime, Internet, Forensics, the fight against crime.*

Злочинність – це соціально-правове історично мінливе масове явище, що складається з усієї сукупності скоєних у той чи інший період у державі злочинів, що мають кількісні та якісні показники [1, с. 74]. У повсякденному житті злочинність проявляється як у формі окремого злочину, так і у формі групи злочинів, вчинених певним контингентом осіб.

Н.Ф. Кузнєцова під причинами та умовами злочинності розуміє систему соціально негативних явищ і процесів, які детермінують злочинність як свій наслідок [2]. Проте ми вважаємо, що слід враховувати всю сукупність чинників, яка породжує злочини. Наприклад, розробка ЕОМ і масова комп'ютеризація не є негативним чинником, швидше навпаки, однак в силу ряду умов, застосування комп'ютера може бути як причиною, так і умовою вчинення злочину. Під причинами та умовами злочинності слід розуміти такі явища суспільного життя, які породжують злочинність, підтримують її існування, викликають її зростання або зниження [1, с. 178], тобто зумовлюють криміногенну детермінацію злочинності. Криміногенна детермінація об'єднує в собі як причинність, так і обумовлення злочинності, а також супутні, необхідні і достатні умови.

Прийнято виділяти три рівні причин за ступенем абстрагування:

- психологічний (індивідуальний) – причини вчинення злочинів конкретною людиною;
- соціологічний (суспільної системи) – соціальні, економічні, політичні та духовні недоліки суспільної системи, що викликають злочинність, їх взаємозв'язок;
- філософський (суспільства в цілому) – негативні явища в людському суспільстві в цілому. По виду відносин, які породжують причини злочинності, виділяють юридичні, економічні, соціальні та моральний стан суспільства.

Злочинність у сфері використання ЕОМ є складовою частиною загальної злочинності й невіддільна від неї, а значить, породжується ы специфічними причинами, і загальними, такими як соціальні.

На початок 90-х років припадає різке зростання злочинності, що зазначається і науковцями, і статистичними даними. Цей період характеризується факторами розвалу СРСР з усією його системою соціального контролю. Крім того, початок 90-х років є своєрідною відправною точкою, з якою дослідники пов'язують появу кваліфікованих злочинів у сфері інформаційних технологій і зростання ступеня їх загрози інформаційній безпеці України.

Інформаційний розвиток суспільства та запровадження на державному рівні в Україні використання мережі Internet та інших комп'ютерних систем в усіх сферах суспільного життя поряд із позитивними здобутками супроводжується і негативними явищами. Особливу занепокоєність викликає збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж як у світі, так і в Україні, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоди суспільству, державі, суб'єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам.

Велику небезпеку являє собою поява нових форм злочинної діяльності, пов'язаних з використанням високих технологій, які раніше не були відомі. З такими проявами поки що досить складно вести ефективну боротьбу як з точки зору кримінального переслідування, так і застосування організаційно-управлінських і кримінологічних заходів з метою їх попередження. До таких злочинних посягань слід віднести умисне втручання в роботу автоматизованих систем, що призвело до перекручування чи знищення комп'ютерної інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручування або знищення інформації чи то носіїв інформації, кримінальна відповідальність за які в Україні була встановлена Законом України "Про внесення змін та доповнень до Кримінального кодексу України" від 20 жовтня 1994 р., яким КК України 1960 р. було доповнено статтею 1981 "Порушення роботи автоматизованих систем". Чинний КК України також передбачив відповідальність за вчинення таких суспільно-небезпечних діянь у статті 361 "Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж", в ч. 1 якої передбачена відповідальність за "незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручування чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для

незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручування або знищення комп'ютерної інформації чи носіїв такої інформації".

Основні причини злочинності у сфері використання ЕОМ, на наш погляд, найбільш доцільним буде розглядати комплексами причин залежно від відносин, що їх породжують.

Перш за все це правові причини. Такими можна вважати:

- відсутність або недостатнє правове регулювання суспільних відносин у сфері інформаційних технологій, як тих, що формуються, так і тих що сформувалися;

- недостатня правова урегульованість інших суспільних відносин, що є одним з основних факторів існування соціально-економічних причин злочинності у сфері використання ЕОМ;

- інформаційні відносини в Україні знаходяться в стадії формування, законодавство про інформаційні відносини регулює в основному загальні питання, лише деякі галузі врегульовані в достатній мірі (захист державної і інших видів таємниць). Між тим, інформаційний обмін може здійснюватися на таких рівнях: міжособистісний; громадський; державний.

За ступенем урегульованості законодавством інформаційні процеси можна розділити на законні, протизаконні та не врегульовані законодавством.

Аналіз вітчизняного законодавства показує відсутність предмета правового регулювання в питаннях індивідуальної, групової і суспільної свідомості і, як наслідок, відсутність правових актів, що встановлюють відповідальність за дані діяння.

Недостатньо врегульована законодавством діяльність засобів масової інформації. Закон України від 16 листопада 1992 р. № 2782-XII "Про друковані засоби масової інформації (пресу) в Україні" [3] вимагає ретельної переробки і змін. Наразі фактично відсутнє визначення місця і ролі засобів масової інформації в життєдіяльності суспільства і держави.

Розвиток інформаційних технологій також вимагає внесення коректив у правові акти. Під засобами масової інформації, згідно з чинним Законом, розуміються періодичні і такі, що продовжуються, видання, які виходять під постійною назвою, з періодичністю один і більше номерів (випусків) протягом року на підставі свідоцтва про державну реєстрацію. Додатки до друкованих засобів масової інформації у вигляді видань газетного та журнального типу є окремими періодичними і такими, що продовжуються, друкованими виданнями і підлягають реєстрації на загальних підставах.

Закон "Про друковані засоби масової інформації (пресу) в Україні" залишає відкритим питання про віднесення до засобів масової інформації так званих "електронних засобів масової інформації" (тобто засобів масової інформації, які розміщуються в мережі Інтернет) саме як додатків до друкованих засобів масової інформації, адже вони наділені більшістю ознак ЗМІ.

Уявляється доцільним згадати електронні засоби масової інформації в Законі України "Про друковані засоби масової інформації (пресу) в Україні", внісши необхідні зміни до цього закону, як таку, що щільно увійшла у повсякденне життя форму подання інформації.

Одним з напрямків урегулювання інформаційних процесів є криміналізація суспільно небезпечних діянь, яка здійснюється на основі таких чинників:

- існування самих фактів вчинення подібного діяння;
- визначення ступеня суспільної небезпеки діяння;
- відносна поширеність діяння;
- визначення громадської думки відносно даних діянь.

При вирішенні питання про криміналізацію діяння необхідно також визначити можливості виявлення, запобігання, фіксації діяння, закріплення доказів його вчинення - оцінка наукових, технічних, матеріальних, кадрових та інших можливостей.

Як підкреслюють вчені-криміналісти П.Д. Біленчук, М.А. Зубань та В.О. Голубєв, сьогодні у вітчизняній криміналістичній науці все ще не існує чіткого визначення поняття комп'ютерного злочину, дискутуються різні точки зору з питань їх класифікації. Складність у формулюваннях цих понять існує як внаслідок неможливості виділення єдиного об'єкта злочинного посягання, так і через множинність предметів злочинного посягання в аспекті їх кримінально-правового значення [4, с. 19].

Більшість фахівців розподілило комп'ютерні злочини на два типи.

Перший – злочини, в яких об'єктом їх здійснення є ЕОМ. До таких можна віднести і:

- знешкодження або заміну даних, програмного забезпечення та обладнання;
- розкрадання вхідних, вихідних даних, програмного забезпечення та обладнання;
- економічне шпигунство та розголошення відомостей, які складають державну чи комерційну таємницю;
- інші злочинні діяння цього виду.

Другий тип таких злочинів об'єднує протизаконні акції, для здійснення яких ЕОМ використовується як знаряддя в досягненні злочинної мети. Такими є:

- комп'ютерний саботаж;
- вимагання та шантаж;
- розтрата;
- розкрадання коштів;
- обман споживачів, інвесторів чи користувачів;
- інші злочини.

До категорії "інші злочинні діяння" віднесено несанкціоноване використання комп'ютера в особистих цілях.

На наш погляд, під комп'ютерною злочинністю слід розуміти суспільно небезпечну діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинення збитків майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським формуванням і громадянам, а також правам особи.

Розповсюдження загальних комп'ютерних знань, постійне підвищення технічних характеристик та супутнє зниження цін на обладнання, застосування комп'ютерів, мабуть, чи не в усіх професіях, розвиток машинних мов високого рівня, які легко засвоюються будь-якою зацікавленою особою, і, як наслідок, постійне зростання кількості користувачів, зумовило зростання масштабів протизаконних дій, пов'язаних з використанням ЕОМ. Збільшення кількості кримінальних справ, пов'язаних з комп'ютерними злочинами, спостерігається практично у всіх промислово розвинутих країнах.

Основні причини вчинення злочинів у сфері використання ЕОМ, як і багатьох інших видів злочинності, слід шукати в економічних відносинах, в їх суперечливості. За деякими оцінками дослідників, нині економічний характер разом з корисливою мотивацією злочинної поведінки мають 4/5 криміногенних детермінант.

Наявність великої кількості безробітних, у тому числі й осіб, що володіють достатніми професійними навичками, здатних здійснювати кваліфіковані злочини у сфері використання комп'ютерів, є загальною проблемою для країн колишнього СРСР, де рівень фізико-математичної освіти завжди був високим, а рівень безробіття після розпаду СРСР значно підвищився.

Формування нової галузі суспільних відносин вимагає, у свою чергу, аналізу та доповнення діяльності щодо протидії вчиненню правопорушень і злочинів.

Перші спеціальні закони по боротьбі з комп'ютерною злочинністю було прийнято в 1973 р. в Швеції і в 1976 р. у США на федеральному рівні. Склади злочинів у сфері інформаційних технологій (комп'ютерних злочинів) було сформовано в 1979 р. на Конференції американської асоціації адвокатів у Далласі, до яких увійшли: використання або спроба використання комп'ютера, обчислювальної системи або мереж комп'ютерів з метою отримання грошей, власності або послуг шляхом прикриття фальшивими кодами або видання себе за іншу особу; умисна несанкціонована дія, що має за мету зміну, пошкодження, знищення або викрадення комп'ютера, обчислювальної системи, комп'ютерної мережі або систем математичного забезпечення, що містяться в них, програм або даних; умисне незаконне порушення зв'язку між комп'ютерами, обчислювальними системами або комп'ютерними мережами [5, с. 60]. Згодом поступово в багатьох країнах світу затверджено законодавчі акти стосовно цієї категорії злочинів.

У лютому 1986 р. Бундестагом Німеччини було прийнято Другий Закон по боротьбі з економічною злочинністю. Завдяки цьому було закладено правову базу для ефективного кримінально-правового переслідування економічних правопорушень нового типу, перш за все злочинів, об'єктом або знаряддям яких є ЕОМ. Ряд нових статей, які введено цим законом, вміщують спеціально сформульовані склади комп'ютерних злочинів. Закон було введено в дію 1 серпня 1986 р.

В Італії законодавчими актами введені основні положення відносно найбільш важливих комп'ютерних злочинів:

Декрет № 518 від 29.12.92 р. "Використання положень Європейського Економічного співтовариства за № 91/250 стосовно офіційного захисту комп'ютерних програм":

Закон № 547 від 23.12.93 "Зміна та внесення нових статей стосовно комп'ютерних злочинів у Кримінальний Кодекс".

Комп'ютерний злочин, згідно з кримінальним законодавством Італії, – це злочин, скоєний з використанням комп'ютерних технологій, від персонального комп'ютера до портативних телефонних пристроїв, які створені на базі мікрочіпів.

Законодавство Італії забезпечує захист урядових організацій, військових об'єктів, банків, компаній, фірм від несанкціонованого доступу в комп'ютерні мережі, протиправного використання захищених банків даних, незаконного копіювання топографій напівпровідників (чіпів), які злочинці використовують для встановлення кодів кредитних і телефонних карток, банківських рахунків тощо.

Щорічні втрати в Італії від комп'ютерних злочинів складають сотні мільйонів лір. Характерним для поведінки комп'ютерних злочинців є використання програмного забезпечення, яке може автоматично набирати всі алфавітно-цифрові комбінації на основі принципу генератора випадкових чисел. Завдяки цій процедурі вони здатні встановити пароль, що дозволить увійти до системи [5, с. 109].

Франція володіє повним юридичним арсеналом для боротьби з такою категорією злочинності. У 1994 р. було сформовано Бригаду поліції з компетентного персоналу, яка спеціалізується на виявленні та розслідуванні комп'ютерних злочинів при тісному співробітництві із службами безпеки та цивільними організаціями.

З 1 березня 1994 р. було введено в дію нову версію Кримінального Кодексу, який докорінно змінив внутрішні закони про комп'ютерну злочинність.

До Кримінального Кодексу були внесені статті з санкціями проти правопорушень, які пов'язані з обробкою інформації та із злочинами стосовно фальсифікації даних.

Прийнятий 5 січня 1994 р. Закон "Godfrran", який було названо на честь автора, вніс ясність та уточнив питання юриспруденції і практики стосовно несанкціонованого доступу та протидії функціонуванню систем, які приносять щорічних збитків, наприклад, страховим компаніям в розмірі 5 мільярдів франків.

Єдиний закон, який передбачає покарання за комп'ютерні злочини - Кримінальний Кодекс Іспанії. Диспозиції статей Кодексу сформульовано відповідно до норм Державного Закону № 5/92 від 2 жовтня 1992 р., який регулює процеси персональної автоматизованої обробки даних і передбачає утворення органу захисту даних для контролю за виконанням цих норм.

Специфічні комп'ютерні злочини вміщують правопорушення, в яких комп'ютерна система є об'єктом вчинення злочину. Прикладом цього виду злочинів може бути протизаконний доступ до комп'ютерної системи.

До злочинів, які пов'язані з комп'ютерами, належать правопорушення, в яких комп'ютер виступає в ролі предмета або інструмента здійснення правопорушення. Одним з прикладів цієї категорії злочинів є крадіжка грошей з банку з використанням комп'ютера як інструмента вчинення злочину.

Третій вид злочинів – правопорушення, в яких інформаційна технологія використовується як допоміжна у його вчиненні. Як приклад – використання синдикатами, які займаються розповсюдженням наркотиків, спеціальних комп'ютерів або комунікаційних засобів для безпечного зв'язку між собою.

Сьогодні Україна стоїть перед проблемою подальшого розвитку сучасних біо- та інформаційних технологій, телекомунікаційних систем, інформатизації суспільства. Головним завданням інформатизації суспільства є створення правових, економічних, технологічних, соціальних та освітніх першооснов для забезпечення будь-якому потенційному користувачеві в будь-який час у будь-якому місті країни доступу до інформації, яка необхідна для вирішення відповідних господарських, технічних, наукових, соціальних та особистих проблем.

Розвиток мережі комерційних банків з великими обсягами банківських фінансових операцій щодо переказів значних сум грошей між державними і комерційними структурами як у межах країни, так і за кордон, поставив питання про спрощення розрахунків шляхом впрова-

дження в банківську систему комп'ютерної мережі та інших технічних засобів.

Інформаційна технологія стала промисловим фактором. Сьогодні вона займає позицію, яка прирівнюється до таких факторів, як праця та капітал. Це означає, що той, хто вміє користуватися інформаційною технологією, одержує змогу впливати на економічні процеси, а, відтак, на політику і взагалі на суспільство.

Протягом останнього десятиріччя значно розширилися масштаби протизаконного використання ЕОМ саме при вчиненні економічних злочинів.

Організація інформаційно-технологічних систем на світовому рівні поряд з поліпшенням взаємодії ставить багато проблем. Організовані злочинні формування намагаються проникнути у виробництво програмного забезпечення і впливати на безпеку комп'ютерних мереж. Ці проблеми не можна не враховувати.

Просте управління комп'ютерами та водночас недостатня захищеність комп'ютерних мереж від несанкціонованого доступу стає причиною розкрадання великої кількості коштів шляхом їх електронного переказу за вигадані послуги з міжнародних банків усього світу на поточні рахунки до тих країн, де уряди не особливо турбують себе запитами та іншими формами перевірки. Випадки крадіжок грошей за допомогою комп'ютерної техніки стають такими ж небезпечними злочинами, як викрадення дітей, вимагання, тероризм, торгівля наркотиками.

Головною проблемою у вирішенні глобальної задачі профілактики злочинності у сфері використання ЕОМ є формування в Україні єдиного інформаційно-правового простору, що забезпечує правову інформованість всіх структур суспільства і кожного громадянина окремо. Дана проблема висувається на перший план якісним оновленням суспільства, становленням ринкової економіки, побудовою демократичної правової держави і багатьма іншими чинниками, тому що правова освіченість необхідна, щоб рости в умовах демократії.

Список використаної літератури:

1. Криминология: Учебник / Под. ред. В.Н. Кудрявцева и В.Е. Эминова. – М., 2009.
2. Кузнецова Н.Ф. Проблемы криминологической детерминации. – М., 1984.
3. ВВР. – 1993. – № 1. – Ст. 1.
4. Голубєв В.О. Комп'ютерні злочини в банківській діяльності. – Запоріжжя, 1997.
5. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навч. посібник. – К., 2002.
6. Пашнєв Д.В., Рудик М.В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом // Ученые записки Таврического национального университета им. В. И. Вернадского. – Серия «Юридические науки». – 2009. – Т. 22 (61). – № 1.– С. 229-235.

Надійшла до редакції 11.04.2012

ГУМЕНЮК Ю.С., аспірант
(Львівський національний університет імені Івана Франка)

УДК 343 (477) + 343.241 (477)

ПРИЗНАЧЕННЯ ПОКАРАННЯ ЗА НЕЗАКІНЧЕНИЙ ЗЛОЧИН: ІСТОРИЧНО-ПРАВОВИЙ ДОСВІД

Проаналізовано історичний розвиток регламентації призначення покарання за незакінчений злочин та його прототипів у джерелах права, які діяли на території України починаючи із X ст. по сьогодення.

Ключові слова: *незакінчений злочин, замах на злочин, готування до злочину, призначення покарання*

Анализируется историческое развитие регламентации назначения наказания за неоконченное преступление и его прототипов в источниках права, которые действовали на территории Украины с X в. по настоящее время.

Ключевые слова: *неоконченное преступление, покушение на преступление, подготовка к преступлению, назначение наказания*