ФП 2008-2
ISSN 1995-6134

УДК 343.851:004.7

Л.В. БОРИСОВА, канд. юрид. наук, Харківський національний університет внутрішніх справ

ПРОФІЛАКТИКА Й ПРОГНОЗУВАННЯ ВЧИНЕННЯ ТРАНСНАЦІОНАЛЬНИХ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Ключові слова: *профілактика, прогнозування, транснаціональні комп'ютерні злочини*

Мета статті полягає в аналізі й прогнозуванні вчинення транснаціональних комп'ютерних злочинів у зв'язку із тим, що інформаційно-комунікаційні технології є одними з найважливіших чинників, які впливають на формування пріоритетних напрямів розвитку двадцять першого століття: надаються безпрецедентні можливості доступу до інформації, колективного її використання і взаємного обміну, а також для розвитку економіки. Науково-технічний прогрес поставив перед людством серйозні проблеми і встановив колосальну відповідальність за використання отриманої могутності: "розвиток техніки несе необмежені можливості для добра і зла" [1, с.76]. Кібернетика стала фактором кризи, сприяючи другій промисловій революції.

Нові можливості, що створюються телекомунікаційними[1] мережами, змусили по-новому поглянути на більшість традиційних передумов правових систем. Поступове покращення якості обслуговування телекомунікаційних мереж спричинило різкий сплеск комп'ютерної злочинності, яка примусила правоохоронні органи розробити відповідні правові інструментарії, пристосовуючи їх до нових технологій.

Комп'ютерна злочинність стає одним з найбільш небезпечних видів злочинних посягань: злочинці дуже швидко усвідомили масштаби можливостей Інтернет і телекомунікацій. За даними ООН збитки, що спричиняються комп'ютерними злочинами, зіставлені з прибутками від незаконного обігу наркотиків і зброї. Серед комп'ютерних злочинів, вчинених у світі, все більше стає "міжнародних", таких, які в якості засобів або жертв використовують телекомунікаційні системи різних держав: через відкриті телекомунікаційні мережі можливий доступ до національних, у тому числі й спеціально захищених інформаційних ресурсів.

Здатність злочинних груп розповсюджувати свій вплив за межі національних кордонів і діяти сумісно з правопорушниками у рамках юрисдикції інших держав, дозволяє їм використовувати існуючі в світі диспропорції в пропозиціях, попиті й вартості товарів, обіг яких обмежений з політичних міркувань. Стан охорони національних кордонів і рамки юрисдикції вивчаються зловмисниками з ціллю укривання доказів та уникнення від розслідування та судового переслідування.

Відповідно, можна говорити про транснаціональну злочинність[2], що відображено в документах ООН. Найбільш небезпечною на сьогоднішній день є транснаціональна організо-

[1] Телекомунікації – будь-яка передача знаків, сигналів, записів, образів, звуків, інформації чи свідчень будь-якого характеру, що передаються повністю або частково за допомогою телефонного зв'язку, радіо, електромагнітної, фотоелектронної чи фотооптичної системи [2, с.17].

[2] Транснаціональні злочини (злочини міжнародного характеру) – це діяння, які передбачені міжнародними угодами, не відносяться до злочинів проти людства, миру і безпеки, але роблять замах на нормальні стабільні відношення між державами, наносять збитки мирному співробітництву в різних областях відношень (економічній, соціально-культурній, майновій тощо), а також організаціям і громадянам, що караються згідно нормам, встановленим в міжнародних угодах, або згідно нормам національного кримінального законодавства у відповідності з цими угодами. До них відносяться: діяння проти стабільності міжнародних відносин (тероризм, захоплення заручників, захоплення і крадіжку повітряних судів, ін.); діяння, що наносять втрати економічному, соціальному і культурному розвитку держав (виготовлення фальшивих грошей, незаконний обіг наркотиків, легалізація злочинних доходів, др.); злочини, вчинені у відкритому морі; злочинні посягання на особисті права людини (работоргівля, др.) і ряд інших [4, с.116].

ISSN 1995-6134

вана злочинність.

У тих державах світу, де діє принцип верховенства права і поважають законність, Інтернет – тільки функція глобальної телекомунікаційної революції. Поки існують великі об'єми даних, які пов'язані з використанням можливостей Інтернет, то ця мережа без сумніву є однією найбільш важливою інформаційною і впливовою мережею світу.

Транснаціональний характер злочинності з використанням телекомунікаційних мереж дає змогу вважати, що розробка загальної політики з ключових питань повинна бути частиною будь-якої стратегії в боротьбі зі злочинністю. Така концепція має важливе значення для запобігання виникнення "інформаційних сховищ", у тому числі й в рамках тих правових систем, де комп'ютерні злочини не є кримінально карними. Разом із тим, принцип державного суверенітету залишається нездоланною перешкодою, так як потенційно будь-яка держава може надати притулок екстремістам, злочинцям, фальшивомонетникам або терористам.

Розробка загальної політики по протидії транснаціональній комп'ютерній злочинності стала одним із напрямів діяльності Програми ООН. Метою керівного документу із запобігання злочинам, пов'язаних із використанням комп'ютерів і боротьбою з правопорушеннями в сфері інформаційних технологій, опублікованого Організацією Об'єднаних Націй, є узгодження як матеріального, так і процесуального права, а також міжнародне співробітництво в боротьбі зі злочинністю, пов'язаною з використанням комп'ютерів. У зв'язку з цим привертається увага світової спільноти на такі аспекти [3, с.18]:

- сприяння розробці правотворчими органами стандартів для забезпечення надійності та безпеки телекомунікацій та технологій обробки даних;

- розробка інформаційних і телекомунікаційних систем, здатних виявляти зловживання в мережах, відслідковувати осіб, які вчиняють такі зловживання й збирати відповідні докази.

Вітчизняні та зарубіжні дослідники з проблем транснаціональної комп'ютерної злочинності звертають увагу на те, що одним із пріоритетних напрямів вирішення завдання ефективної протидії сучасній злочинній діяльності в інформаційному просторі є активне використання правоохоронними органами різноманітних заходів правового і профілактичного характеру [5-7].

М.П. Яблоков вважає, що "успішна криміналістична діяльність у боротьбі з різними видами злочинів неможлива без використання в ній чітко продуманої системи криміналістичних засобів профілактичного характеру, в сукупності складаючи криміналістичну профілактичну діяльність" [8, с.119] і покликана "розробляти рекомендації по встановленню обставин, що сприяли вчиненню певного виду злочинів, які зумовили слідоутворення, а також застосуванню запобіжних заходів криміналістичними методами, прийомами і засобами" [9, с.35].

Подальший розвиток усіх складових науки криміналістики, вдосконалення існуючих і розробка нових криміналістичних заходів, прийомів, методів та рекомендацій розслідування й запобігання злочинам у процесі наукового пошуку неможлива без широкого і продуманого використання методів наукового і практичного прогнозування[3]. Результатом прогностичних досліджень є прогнози як носії інформації про можливі напрями і тенденції розвитку будь-якого об'єкта, альтернативні шляхи та терміни настання його певних характеристик (стану, структури та ін.). При цьому прогноз не є простою сумою зібрання інформації про відповідний об'єкт, його минуле і теперішнє. Він містить в собі нову інформацію, яка зменшує невизначеність судження відносно майбутнього стану даного об'єкта [10, с.154]. Відповідно, без цього неможлива ефективна пізнавальна і тактико-методична діяльність слідчого, експерта-криміналіста і оперативно-розшукового працівника на прак-

[3] Б.М. Шавер уперше висловив ідею необхідності застосування пізнавального апарату прогностики в практичній діяльності органів розслідування ще в кінці 30-х років [11, с.68].

ISSN 1995-6134

тиці [8, с.126].

Прогнозування – невід'ємна передумова мотивованої діяльності, частина психічного стану його суб'єкта. Прогноз робиться не на основі самої тенденції розвитку процесу, а на основі нашого знання про цю тенденцію. Причому це знання, завжди залишаючись приблизним, орієнтованим, деколи може бути досить точним для даного прогнозу.

Використання поняття "криміналістичне прогнозування" обґрунтоване специфікою його цілей (оптимізація діяльності розкриття, розслідування й запобігання злочинам криміналістичними засобами) і отриманими прогнозами (в аспекті, що розглядається, гіпотетичні багатофакторні моделі можливого стану або розвитку злочинної діяльності в майбутньому), а за висловом М.В. Салтевського "розуміння криміналістичної моделі дозволяє заздалегідь будувати типову прогностичну модель розслідуваного злочину, визначаючи ймовірні співвідношення між її елементами та обставинами реальної події, намічати шляхи розшуку людей і речей [12, с.423].

Виходячи із конкретних задач і рівнів дослідження в практичному прогнозуванні В.Я. Колдін пропонує виділити [13, с.103-105]:

- оперативне прогнозування, метою якого є підвищення якості методів запобігання і припинення злочинів, створення сприятливих умов для їхнього розкриття "по гарячим слідам";

- індивідуальне прогнозування, яке орієнтує слідство на можливість учинення особою нових злочинів, визначення їхнього характеру, місця, часу, способу (підготовка, вчинення, приховування, посягання, ухилення від відповідальності), жертви, безпосереднього предмета посягання, співучасників, найбільш імовірних каналів збиту. Цей вид прогнозування перемежовується з кримінологічним прогнозуванням індивідуальної злочинної поведінки;

- науково-прикладне прогнозування неминуче виникаючих принципово нових видів посягань, а також суттєвих змін у способах вчинення "традиційних" злочинів.

Одним з найбільш перспективних підходів до вирішення проблеми криміналістичної профілактики транснаціональних комп'ютерних злочинів є формування прогнозу про ймовірний злочин і розробка моделей, алгоритмів відповідних рекомендацій. За висловом В.А. Журавля "вчених та практиків не можуть не цікавити питання про динаміку розвитку і трансформації названих злочинів з виділенням та аналізом прогнозованого фону, про ймовірність появу нових ще більш соціально небезпечних злочинів, про необхідність і доцільність впровадження в судово-слідчу і експертну практику певних криміналістичних нововведень як засобів недопущення передбачуваного перебігу змін у досліджуваній злочинній діяльності та ін. [10, с.181].

Як відомо, інформаційна модель – маломірне уявлення про багатомірний простір. У той же час інформаційна модель злочинності – це портрет злочинності як системи, як сукупності окремих видів злочинів. Коли мова йде про транснаціональні комп'ютерні злочини, то під цим терміном розуміється цілий спектр протиправних дій, що і визначає комплексний підхід до питань криміналістичної профілактики даного виду злочинів.

Особливість і природа транснаціональних комп'ютерних злочинів така, що існує ймовірність розробки моделей достатньо точних прогнозів збільшення кількості злочинів, вчинених з використанням глобальних телекомунікаційних мереж.

З урахуванням специфічності та новизни транснаціональних комп'ютерних злочинів серед заходів їхньої профілактики виділяють не тільки криміналістичні аспекти їхнього запобігання, а також правові та організаційно-технічні. Ключовим елементом, на наш погляд, є відмова від точки зору на необхідність захисту лише таємної й конфіденційної інформації та перехід до розуміння необхідності захисту будь-якого інформаційного ресурсу, важливого для його власника.

Організаційні заходи представляють собою ефективний спосіб захисту інформації й реальний фундамент, на якому будується вся система захисту. Основними організаційно-

ISSN 1995-6134

технічними задачами захисту інформації, що охороняється, у телекомунікаційних мережах є наступні:

- запобігання витоку інформації за рахунок побічних електромагнітних випромінювань, що створюються функціонуючими технічними засобами, наприклад, застосовування TEMPEST-подібного захисту;
- запобігання атакам шкідливих програм;
- запобігання перехопленню інформації, що передається каналами зв'язку, технічними засобами.

Засобами й умовами забезпечення інформаційної безпеки є:

- розробка моделей злочинного посягання на інформаційні масиви шляхом пошуку та узагальнення інформації про наміри та можливості зловмисників;
- визначення та систематизація переліку відомостей, які складають об'єкт захисту інтересів держави або організації в окремих галузях їхньої діяльності;
- розробка на основі експертних оцінок систем захисту та побудова комплексів захисту таємної та конфіденційної інформації;
- удосконалення тактики керування та взаємодії між різними організаціями – власниками інформаційних масивів, які підлягають обов'язковому захисту;
- поєднання правових, організаційно-технічних та адміністративних заходів захисту таємної і конфіденційної інформації різних за ступенем важливості;
- удосконалення та підсилення законодавства про авторські права на програмні продукти, пропаганду переваг ліцензійного використання програмних продуктів.

Із матеріалів збірника Datapro за 1991 рік бачимо, що 71 % респондентів працювали в компаніях, які мають опубліковану політику організації безпеки, лише 77 % мали спеціаліста або підрозділ, які відповідають за безпеку ЕОМ. У банківсько-фінансовій сфері цей коефіцієнт досягає 86 %. Зростає кількість членів професійних організацій: кількість членів Асоціації по забезпеченню безпеки інформаційних систем (ISSA) з 1985 року до 1987 збільшилася з 100 до 400, а до кінця 1990 року – перевищила 2000 членів [14, с.9-10].

Протягом останніх чотирьох років представники країн Європи і США працювали над проектом угоди такого міжнародного співробітництва, яке в разі прийняття більшістю держав світу забезпечило б необхідний правовий мінімум у законодавчих базах держав-учасниць і утвердило "чорний список" злочинів, відповідальність за які повинна передбачатися в окремих національних законодавствах. Сьогодні лише двадцять країн мають національне законодавство стосовно використання глобального інформаційного простору. Наприклад, на розгляд конгресу США представлені наступні законопроекти: Закон про захист Інтернет, Закон про захист персональної інформації в Інтернет, Закон про безпеку і свободу через шифрування, Закон про сімейний доступ в Інтернет, Законопроект "Про заборону на азартні ігри".

Аналіз основних міжнародних документів правового регулювання інформаційних технологій дозволив зробити висновок, що для ефективної боротьби з транснаціональною комп'ютерною злочинністю необхідно здійснити уніфікацію кримінального й кримінально-процесуального законодавств кожної держави за вчинення комп'ютерних злочинів, усунути норми "подвійного права". Разом із тим, вважаємо:

- основними методами дослідження є кваліфіковане спостереження, системний аналіз, математичне моделювання, інструментальний аналіз із застосуванням ЕОМ, статистичний та соціальний експеримент, метод експертних оцінок, спеціальні методи предметних наук;
- забезпечити абсолютну безпеку комп'ютерної інформації в телекомунікаційній мережі неможливо, так як абсолютно захищена система непридатна для її використання, крім того не всі шляхи подолання безпеки реально відомі;
- задача розшуку зловмисників ускладнюється значною кількістю офіційно зареєстрованих користувачів терміналами автоматизованих систем, вузлами мереж, окремими

ISSN 1995-6134

ПЕОМ тощо.

ЛІТЕРАТУРА

1. Винер Н. Кибернетика или управление и связь в животном и машине. –М.: Советское радио, 1968. –326 с.
2. Офіційний переклад нормативних актів Євросоюзу в сфері інформаційно-комунікаційних технологій /Громадська організація ІНТЕРНЬЮЗ-УКРАЇНА. –Київ, 2000. –219 с.
3. Преступления, связанные с использованием компьютерной сети. Справочный документ для семинара-практикума по использованию компьютерной сети /Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. –Документ ООН A/CONF/187/10.
4. Международное право: Учебник /Игнатенко Г.В., Суворова В.Я., Туинов И.О. и др., Под ред. Г.В. Игнатенко. –М.: Высш. шк., 1995. –399 с.
5. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями. –М.: Мир, 1999. –351 с.
6. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. –М.: Юрид.лит., 1991. –160 с.
7. Цимбалюк В. Організація та координація боротьби з організованою транскордонною кіберзлочинністю // Право України. –2003. –№ 2. –С.26–30.
8. Криминалистика: Учебное пособие /Герасимов В.Н., Колдин В.Я., Крылов В.В. и др.; Отв. ред. Н.П. Яблоков. –М.: БЕК, 1995. –689 с.
9. Криміналістика: Підручник /Шепітько В.Ю., Глібко В.М., Дудніков А.Л., Журавель В.А. та ін.; За ред. В.Ю. Шепітька. –К.: Вид. дім "Ін Юре", 2001. –682 с.
10. Журавель В.А. Проблеми теорії та методології криміналістичного прогнозування. –Харків: Право, 1999. –304 с.
11. Шавер Б.М. Предмет и метод советской криминалистики // Соц. законность. -1938. –№ 6. –С.56-82.
12. Салтевський М.В. Криміналістика (у сучасному викладі): Підручник. –К.: Кондор, 2005. –588 с.
13. Типовые модели и алгоритмы криминалистического исследования: Учеб. пособие /Под ред. В.Я. Колдина. -М.: Изд-во Моск. ун-та, 1989. –184 с.
14. Вус М.А. Аттестация специалистов по безопасности в США // Защита информации. Конфидент. -1994. –№ 2. –С.9-10.

Борисова Л.В. Профілактика й прогнозування вчинення транснаціональних комп'ютерних злочинів // Форум права. -2008. -№ 2. –С.27-31 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2008-2/08blvtkz.pdf

Розглянуті сучасні проблеми профілактики й прогнозування транснаціональних комп'ютерних злочинів.

***

Борисова Л.В. Профилактика и прогнозирование совершения транснациональных компьютерных преступлений

Рассмотрены современные проблемы профилактики и прогнозирования транснациональных компьютерных преступлений.

***

Borisova L.V. Preventive maintenance and forecasting of fulfillment of transnational computer crimes

Modern problems of preventive maintenance and forecasting of transnational computer crimes are considered.