8. Красиков А.Н. Уголовно-правовая охрана прав и свобод человека в России / А.Н. Красіков. – Саратов, 1996. – 46 с.

9. Новосёлов Г.П. Учение об объекте преступления. Методологические аспекты / Г.П. Новосёлов. – М., 2001. – 560 с.

10. Плаксина Т.А. Общие вопросы уголовной ответственности за убийство /Т.А. Плаксина. – Барнаул. – 2002. – 171 с.

11. Разгильдяев Б.Т. Уголовно-правовая охрана жизни человека и ее оптимизация / Б.Т.Разгильдяев // Уголовно-правовая охрана личности и ее оптимизация. Материалы научно-практической конференции, посвященной памяти профессора А.Н. Красикова (20-21 марта 2003 года).– Саратов, 2003. – 325 с.

12. Анощенко С.В. Учение о потерпевшем в российском уголовном праве / С.В. Анощенко / Автореф. дисс. канд. юр. наук. – Саратов. – 2004. – 31 с.

13. Уголовный кодекс Франции / Под ред. Л.В. Головко, Н.Е. Крыловой. Перевод с французского Н.Е. Крыловой. – СПб.: Юридический центр Пресс, 2001. – 648 с.

УДК 343.451: 004 (477)

КОМП'ЮТЕРНІ ЗЛОЧИНИ: РЕАЛІЇ СУЧАСНОСТІ, ПРОБЛЕМИ БОРОТЬБИ З НИМИ ТА ЙМОВІРНІ ШЛЯХИ ЇХ ВИРІШЕННЯ

Кирбят'єв О.О., ст. оперуповноважений

ГУМВС України в Дніпропетровській області

У статті розглядається сучасний склад комп'ютерного злочину, визначаються та описуються його нові складові, а також його проблематика в сучасних умовах розвитку мережі Internet та віртуальних технологій, формулюються джерела здійснення даного виду злочинів. Також автором пропонуються загальні напрямки з метою підвищення ефективності боротьби з даним видом злочинів.

Ключові слова: комп'ютерний злочин, кіберзлочинність, склад комп'ютерного злочину, автоматизовані електронно-обчислювальні системи, комп'ютер, шахрайство.

Кирбятьев О.А. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ: РЕАЛИИ СОВРЕМЕННОСТИ, ПРОБЛЕМЫ БОРЬБЫ С НИМИ И ПУТИ ИХ РЕШЕНИЯ / ГУМВД Украины в Днепропетровской области, Украина

В статье рассматривается современный состав компьютерного преступления, определяются и описываются его новые составляющие, а также его проблематика в современных условиях развития сети Internet и виртуальных технологий, формулируются источники осуществления данного вида преступлений. Также автором предлагаются общие направления с целью повышения эффективности борьбы с данным видом преступлений.

Ключевые слова: компьютерное преступление, киберпреступность, состав компьютерного преступления, автоматизированные электронно-вычислительные системы, компьютер, мошенничество.

Kirbyatyev O.A. COMPUTER CRIMES: REALITIES OF CONTEMPORANEITY, PROBLEMS OF FIGHT AGAINST THEM AND WAY OF THEIR DECISION / Main administration of ministry of internal affairs of Ukraine in the Dnepropetrovsk region, Ukraine

A modern computer's corpus delict is examined in the article, determined and described his new constituents, and also his problems in the modern terms of development of network of Internet and virtual technologies, the sources of realization of this type of crimes are formulated. Also an author is offer directions of commons with the purpose of increase of efficiency of fight against this type of crimes.

Key words: computer crime, kibercriminality, computer corpus delict, automated electronic-computer systems, computer, swindle.

З того часу коли в 1988 році вірус-черв'як (Morris Worm) паралізував половину комп'ютерів, що працювали в мережі Internet [5], Internet залишається не тільки засобом передачі інформації в науковій, оборонній та інших сферах, але й став глобальною електронною мережею, яка

втілена в усі аспекти нашого життя як вдома, так і на роботі. Атаки в мережі, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, корпоративне шпигунство та поширення дитячої порнографії – ось тільки деякі зі злочинів, що вчиняються в мережі Internet.

Такі протиправні діяння вже сьогодні складають для нашої держави, як і для багатьох інших країн світу, певну суспільну небезпеку, реально загрожуючи інформаційній безпеці – складовій національної безпеки. Національна інфраструктура держави вже сьогодні щільно пов'язана з використанням сучасних комп'ютерних технологій. Щоденна діяльність банківських та енергетичних систем, керування повітряним рухом, транспортна мережа, навіть швидка медична допомога перебувають у майже повній залежності від надійної і безпечної роботи автоматизованих електронно-обчислювальних систем.

На сучасному етапі розвитку нашого суспільства прогнозується подальше зростання залежності життєдіяльності національної інфраструктури від процесів інформатизації та входження України в єдиний інформаційний простір, поширення криміногенних процесів, пов'язаних з протиправним використанням комп'ютерних технологій.

Вітчизняна та світова практика свідчить, що число клієнтів Internet продовжує бурхливо зростати, а разом із цим зростає і кількість атак, яких щодня зазнають комп'ютерні системи із зовнішнього середовища. За статистикою Американського Інституту Комп'ютерної Безпеки (Computer Security Institute), збитки від злочинів, що вчиняються за допомогою комп'ютерних технологій, з кожним роком збільшуються.

Разом із поширенням впровадження сучасних інформаційних технологій в Україні постійно зростає загроза як для державних комп'ютерних систем, так і для приватних організацій та окремих громадян. Особливої актуальності проблема кіберзлочинності набула в наш час.

Термін "кіберзлочин" молодий і утворений сполученням двох слів: кіберпростір і злочин. Термін кіберпростір (у вітчизняній літературі частіше зустрічаються терміни "віртуальний простір" або "віртуальний світ") позначає інформаційний простір, що моделюється за допомогою комп'ютера, у якому існують визначеного роду об'єкти або символьне уявлення інформації – місце, де діють комп'ютерні програми і переміщуються дані. Використання цього терміна поширене у світовій науковій літературі та вживається автором не як юридична категорія, а як визначення соціального та технічного феномена. Термін "кіберзлочини" в подальшому використовуватиметься і як синонім термінів "транснаціональні комп'ютерні злочини", "злочини, що вчиняються за допомогою мережі Internet". Під терміном "кіберзлочини" будемо розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Internet на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян.

Соціологічні опитування в різних країнах, і насамперед, у високорозвинених, показують, що кіберзлочинність посідає одне з чільних місць серед тих проблем, які турбують людей.

Більше того, на думку фахівців, сьогодні це явище становить значно серйознішу небезпеку, ніж 5 років тому внаслідок використання зі злочинною метою новітніх інформаційних технологій, а також зростаючої уразливості сучасного індустріального суспільства. Незважаючи на зусилля держав, які спрямовані на боротьбу з кіберзлочинами, їх кількість у світі не зменшується, а, навпаки, постійно зростає.

Жодна держава сьогодні не здатна протистояти цьому злу самостійно. Нагальною є потреба активізації міжнародного співробітництва в цій сфері. Вагоме місце в такому співробітництві належить, безумовно, міжнародно-правовим механізмам регулювання. Але, зважаючи на те, що в сучасних умовах значна частка засобів боротьби з кіберзлочинами, як і з іншими злочинами міжнародного характеру, належить до внутрішньої компетенції кожної окремої держави, необхідно паралельно розвивати й національне законодавство спрямоване на боротьбу з комп'ютерними злочинами, узгоджуючи його з нормами міжнародного права та спираючись на існуючий світовий позитивний досвід.

Відсутність ефективних механізмів боротьби з кіберзлочинами визначається сьогодні як одна із загроз національній безпеці нашої країни. За таких обставин Україна, як незалежна демократична держава, не може стояти осторонь від проблем протидії комп'ютерної злочинності і, зокрема, його транснаціональних форм.

Зараз триває процес реформування правової системи України. Саме цим, у першу чергу, обумовлюється актуальність питань, які розглядаються в цій статті, оскільки аналіз основних проблем боротьби з кіберзлочинами сприятиме формуванню та реалізації на практиці концепції нового Українського інформаційного законодавства, а також розробки та впровадженню термінових, ефективних заходів протидії негативним процесам інформатизації, пов'язаних із комп'ютерною злочинністю.

Кіберзлочинність – це явище міжнародного значення, рівень якого знаходиться в прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій, мереж їх загального користування та доступу до них. Таким чином, стрімкий розвиток інформатизації в Україні несе за собою потенційну можливість використання комп'ютерних технологій із корисливих мотивів, що певною мірою ставить під загрозу національну безпеку держави.

Боротьба зі злочинністю у сфері використання автоматизованих електронно-обчислювальних систем (далі – комп'ютерні злочини), вже сьогодні є одним із важливіших державних завдань. Для того, щоб ця боротьба була максимально ефективною, безумовно, необхідно дослідження цієї ще нової для нашого суспільства форми злочинності, її складових, виявлення відповідних закономірностей і тенденцій, а також глибоке вивчення організаційно-правових та інших можливих заходів, що перешкоджають її поширенню, розробка заходів попередження і розслідування таких видів злочину.

При недостатній практиці розслідування комп'ютерних злочинів (далі – КЗ) і судового розгляду таких справ, необхідних для розробки їхньої криміналістичної характеристики, можливе застосування порівняльного аналітичного і прогностичного підходів. Джерелами їх здійснення є:

- стан, структура, характеристика КЗ в країнах, де поширені ці діяння і розроблено засоби боротьби з ними;
- досвід правового регулювання боротьби з цим видом злочинів;
- практика виявлення, розслідування і профілактики;
- діяльність правоохоронних структур щодо збору, накопичування та аналізу інформації, що стосується КЗ.

Стан КЗ характеризується наявністю діянь, предметом зазіхання яких є комп'ютерна інформація, її носії, або протиправними діями, для здійснення яких комп'ютер використовується як знаряддя.

У багатьох публікаціях зазначається значне зростання КЗ на Заході. Це підтверджують документи міжнародних організацій (Європейський комітет з проблем злочинності Ради Європи, Інтерпол), що дають підставу розглядати КЗ як транснаціональну проблему.

На такій небезпечній тенденції наголошувалося і у виступах учасників X конгресу ООН щодо попередження злочинності і поводження з правопорушниками, який відбувся у Відні (Австрія) 10-17 квітня 2000 р. [3].

Уперше склад КЗ було сформульовано в 1979 р. на Конференції американської асоціації адвокатів в м. Далласі (США), де було запропоновано наступні формулювання:

- використання або спроба використання комп'ютера, обчислювальної системи або мережі комп'ютерів з метою отримання грошей, власності або послуг, прикриваючись фальшивими приводами, помилковими обіцянками або видаючи себе за іншу особу;
- навмисна несанкціонована дія, що має на меті зміну, пошкодження, знищення або викрадення комп'ютера, обчислювальної системи, мережі комп'ютерів або систем математичного забезпечення, що містяться в них, програм або інформації;
- навмисне несанкціоноване порушення зв'язку між комп'ютерами, обчислювальними системами або мережами комп'ютерів.

Однак ці пропозиції знайшли відображення в американському законодавстві лише через декілька років.

До сучасного складу КЗ включаються все нові види протиправних діянь, хоч і не скрізь досить оформлені в правовому відношенні. Так, на сьогодні до цього переліку вже відносять:

- несанкціоноване проникнення в автоматизовані електронно-обчислювальні системи;
- розкрадання системного і прикладного програмного забезпечення;
- несанкціоноване копіювання, модифікацію або знищення комп'ютерної інформації;
- блокування комп'ютерної інформації, шантаж та інші методи комп'ютерного тероризму;
- комп'ютерне шпигунство;
- підробку і фальсифікацію комп'ютерної інформації;
- розробку і поширення комп'ютерних вірусів і програмних закладок;
- несанкціонований перегляд або розкрадання інформації з банків даних і баз знань;
- халатну недбалість при розробці, створенні автоматизованих електронно-обчислювальних систем і програмного забезпечення, що призводить до тяжких наслідків і втрати інформації;
- механічні, електричні, електромагнітні та інші види впливу на автоматизовані електронно-обчислювальні системи;
- мережеве шахрайство;
- шахрайство з використанням пластикових платіжних карток;
- використання глобальної інформаційної мережі Internet для вчинення віддалених атак проти електронно-обчислювальних систем.

Мабуть, цей перелік не є повним, а буде з часом поповнюватися, але щодо структури КЗ в узагальненому вигляді можна дотримуватися рекомендацій, що були надані ще в 1990 р. Європейським комітетом з проблем злочинності Ради Європи для включення в законодавство європейських країн списку протиправних діянь у сфері комп'ютерної інформації:

1) комп'ютерне шахрайство;

2) комп'ютерна підробка;

3) пошкодження комп'ютерної інформації або комп'ютерних програм;

4) комп'ютерний саботаж;

5) несанкціонований доступ до комп'ютерних систем;

6) несанкціоноване перехоплення інформації;

7) несанкціоноване копіювання захищених комп'ютерних програм;

8) незаконне виробництво копій напівпровідникової продукції.

Робоча група Інтерполу, що була створена з січня 1991 р., теж прагне знайти шляхи розв'язання цієї проблем, які вже виникають не тільки на національному але й на міжнародному рівнях. Зарубіжними фахівцями було розроблено різні класифікації засобів здійснення КЗ. Однією з подібних класифікацій є кодифікатор робочої групи Інтерполу, що в 1991 р. був інтегрований в автоматизовану систему пошуку інформації і в цей час є доступним більш ніж для 100 країн.

Особливе значення має той факт, що відповідно до рекомендацій Європейського комітету з проблем злочинності Ради Європи на базі Національного центрального бюро Інтерполу в Україні створено Національний центральний консультативний пункт (НЦКП) з пробем КЗ, який здійснює збір і накопичення інформації стосовно КЗ, скоєних на території країни, і узагальнює практику їх розслідування; взаємодіє з НЦКП інших країн; здійснює інформаційне супроводження конкретних кримінальних справ, що мають транснаціональний характер.

Соціальна небезпека КЗ визначається негативними тенденціями, що мають відношення до КЗ на сучасному етапі. До них, на наш погляд, необхідно віднести:

- високий ступінь їх розповсюдження;
- дуже високий рівень суспільної небезпеки (збитки від них часто не піддаються обчисленню);
- ступінь латентності (чи не самий великий порівняно з іншими видами злочинів);
- велика кількість професійної або "білокоміркової" злочинності;
- транснаціональний характер їх окремих видів.

Певне уявлення масштабу КЗ дають експертні дані, і, насамперед, дані про злочини.

Відповідно до офіційної статистики в США з 90% опитаних, чиї комп'ютерні системи піддалися в 1999 році атакам у Internet, 74% стверджували, що проникнення в їхню систему було пов'язане з розкраданням конфіденційної інформації через фінансове шахрайство (розкрадання інформації і фінансове шахрайство завдало шкоди на 68 млн дол. і 56 млн дол. відповідно). Фінансові втрати у 273 опитаних склали понад в 265 млн дол. Збитки від атаки типу "відмовлення в обслуговуванні" тільки у 1998 році склали 77 тис. дол., а у 1999 р. зросли до 116 тис. дол [4]. У лютому 2000 р. були атаковані відомі в усьому світі Web-сайти Yahoo. com, Amazon. com, CNN. com, eBay. com та ін., збиток від трьох днів атаки на ці сайти склав понад 1,2 млрд дол. США [7].

Постійне зростання КЗ свідчить, що боротьба з нею ще не достатньо ефективна і не приносить позитивних наслідків.

Ця тенденція має відношення не тільки до України, але й стосується всього світу.

Причинами недостатньої ефективності боротьби, на наш погляд, є:

- відсутність комплексного підходу до розробки заходів попередження і обмеження КЗ;
- недосконаліть українського законодавства;
- використання виключно іноземного програмно-технічного забезпечення;
- відсутність необхідних методик розслідування КЗ;
- відсутність програм підготовки високоякісних фахівців-практиків в галузі боротьби з КЗ;
- відсутність міжнародної взаємодії, міжвідомче розмежування діяльності правоохоронних органів з питань попередження і розслідування КЗ.

Ще однією, дуже важливою проблемою, залишається і неузгодженість зусиль правоохоронних органів на міжнародному рівні щодо попередження та розслідування транснаціональних КЗ, що отримали на Заході назву "кіберзлочини" (cyber crime).

Одним із серйозних кроків, спрямованих на врегулювання цієї проблеми, є прийняття Радою Європи (Council of Europe) 24 квітня 2000 р. проекту Конвенції щодо попередження кіберзлочинів [6]. З огляду на складність проблеми, Рада Європи підготувала і опублікувала проект Конвенції щодо боротьби зі злочинами у кіберпросторі, який планується остаточно прийняти у вересні 2001 року. Реалізуючи положення цього документа, на національному рівні необхідна гармонізація кримінального законодавства з урахуванням рекомендацій Ради Європи і норм міжнародного права. Така необхідність викликана тим, що часто при вчиненні таких видів злочинів об'єкт і суб'єкт знаходяться в різній юрисдикції, існує дуже великий ризик того, що злочинці будуть здійснювати свої протиправні дії з території держав, де такі діяння не віднесено до кримінальних. Тому, підписання і прийняття Україною запропонованої Конвенції щодо попередження кіберзлочинів сприятиме зміцненню міжнародного співробітництва в боротьбі з цими видами злочинів.

Криміногенна ситуація у сфері використання автоматизованих електронно-обчислювальних систем потребує комплексного підходу стосовно вирішення проблем попередження і розслідування КЗ. Застосування системи заходів завжди є більш ефективним, ніж вплив на злочинність окремими діями. Коли при розробці заходів дотримується комплексний системний підхід, що включає в себе різні рівні, тоді отримання позитивних результатів стає реальним.

Іншою проблемою є відсутність фахівців-практиків у галузі попередження і боротьби з КЗ. Суб'єктами КЗ, як вже зазначалося раніше, виступають фахівці дуже високого рівня, злочинці-інтелектуали. Треба невідкладно, на рівні вузівської освіти готувати вузьких фахівців щодо боротьби з КЗ. Програма підготовки таких спеціалістів повинна включати в себе поглиблене вивчення інформатики та обчислювальної техніки і отримання практичних навичок щодо попередження і розслідування КЗ.

Таким чином, для вирішення цієї проблеми необхідно ввести курс з попередження і розслідування злочинів у сфері використання автоматизованих електронно-обчислювальних систем. Метою цієї дисципліни має бути ознайомлення студентів з поняттям і сутністю комп'ютерної інформації, основними засобами її зберігання та захисту, з кримінально-правовою і криміналістичною характеристикою таких видів злочину, особливостями розкриття

і розслідування злочинів у сфері використання автоматизованих електронно-обчислювальних систем. У зазначеному курсі повинна також вивчатися тема стосовно попередження КЗ, у якій розглядаються питання безпеки автоматизованих електронно-обчислювальних систем і попередження КЗ при використанні глобальної інформаційної мережі Internet.

У рамках вирішення цієї проблеми необхідна не тільки вузівська підготовка таких фахівців, але й реалізація програм щодо підвищення кваліфікації практичних співробітників правоохоронних органів, які спеціалізуються у боротьбі з КЗ.

Всебічний аналіз вітчизняного законодавства, яке регулює суспільні інформаційні відносини в Україні, дозволяє стверджувати, що наша держава, поряд із заходами стимулювання розвитку інфраструктури на основі новітніх технологій, вживає необхідні заходи щодо протидії комп'ютерної злочинності. Прикладом цьому може служити Указ Президента України від 31 липня 2000 року Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в України [2], а також Розділ 16. "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж" прийнятого нового Кримінального кодексу України [1, 105].

Разом з тим, є ще багато неврегульованих проблем, які не дають можливості ефективно протидіяти правопорушенням, що вчиняються у сфері використання комп'ютерних технологій.

Для ефективної боротьби з кіберзлочинами треба дати оцінку, чи відповідають зміни процесуальних норм ведення розслідування і переслідування в судовому порядку вимогам часу. Рівень злочинності в мережі Internet зростає настільки й з такою швидкістю, що законодавство просто не встигає за розвитком технологій.

Комплекс заходів щодо боротьби з КЗ повинен спиратися на єдину державну політику в цій галузі. Для цього повинна бути розроблена науково обгрунтована програма, яка включатиме заходи державного, політичного, економічного, соціального, правового та іншого характеру.

ЛІТЕРАТУРА

1. Кримінальний кодекс України (прийнятий сьомою сесією Верховної Ради України 5 квітня 2001 р.). – К., Офіційний вісник України, 2001. – 256 с.
2. Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 року. – Официальный сайт Центра Исследования Компьютерного Преступления // [Електронний ресурс]. – Режим доступу: http://www.crime-research.org/library/Ukaz_Inter.htm.
3. Іванов Д.Ю. Про X конгрес ООН щодо попередження злочинності і поводження з правопорушниками / Д.Ю. Іванов // Computerword. - Київ., 2000. – 16 лютого. – С. 29.
4. Golubev V Creating conditions for constructive international cooperation in combating the transnational computer crime – is the demand of the time // The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, to be held in Vienna, Austria, from 15 April 2000 // [Електронний ресурс]. – Режим доступу: http://www. networkremotemonitor. com/articles/vienna. html.
5. Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism and Government Information Washington, D.C. – 2000. – March 28.
6. Convention is in relation to warning of computercrimes. United States vs. Morris // [Електронний ресурс]. – Режим доступу: http://www.jmls.edu/cyber/cases/morris.txt.
7. Раскевич О.Ю. Атаки на глобальні сайти та їх наслідки / Офіційний сайт Інституту вивчення комп'ютерної злочинності // [Електронний ресурс]. – Режим доступу: http://www. fbi/gov/nipc/compcrime. html.